kaspersky

Kaspersky Security Center 17 Linux

© 2026 AO Kaspersky Lab

Índice

Ajuda do Kaspersky Security Center Linux

O que há de novo

Problemas corrigidos

Sobre os certificados do Kaspersky Security Center Linux

- Kit de distribuição
- Requisitos de hardware e software
  - Requisitos do Servidor de Administração
  - Requisitos do Web Console
  - Requisitos do Agente de Rede
- Aplicativos e soluções da Kaspersky compatíveis
- Sobre a compatibilidade dos componentes do Kaspersky Security Center Linux
- Comparativo do Kaspersky Security Center: baseado em Windows X baseado em Linux
- Sobre o Kaspersky Next Expert View

Arquitetura e conceitos básicos

- Arquitetura
- Diagrama de implementação do Servidor de Administração do Kaspersky Security Center Linux e do Kaspersky Security Center Web Console
- Portas usadas pelo Kaspersky Security Center Linux
- Portas usadas pelo Kaspersky Security Center Web Console
- Conceitos básicos
  - Servidor de Administração
  - Hierarquia de Servidores de Administração
  - Servidor de Administração virtual
  - Servidor Web
  - Servidor Web do Kaspersky Security Center Linux
  - Agente de Rede
  - Grupos de administração
  - Dispositivo gerenciado
  - Dispositivo não atribuído
  - Estação de trabalho do administrador
  - Plug-in da Web de gerenciamento
  - Políticas
  - Perfis da política
  - Tarefas
  - Escopo da tarefa
  - Como as configurações do aplicativo local se relacionam com as políticas
  - Ponto de distribuição
  - Gateway de conexão
  - Servidores de Administração virtual

Esquemas para o tráfego de dados e uso de porta

- Servidor de Administração e dispositivos gerenciados em uma rede de área local (LAN)
- Servidor de Administração principal dentro da rede de área local e dois Servidores de Administração secundários
- Servidor de Administração na LAN, dispositivos gerenciados na Internet, proxy reverso em uso

Servidor de Administração dentro da LAN, dispositivos gerenciados na Internet, e o gateway de conexão em uso
Servidor de Administração dentro do DMZ, dispositivos gerenciados na Internet
Interação dos componentes e aplicativos de segurança do Kaspersky Security Center Linux: mais informações
Convenções usadas em esquemas de interação
Servidor de Administração e DBMS
Servidor de Administração e dispositivo cliente: Gerenciar o aplicativo de segurança
Atualizar o software em um dispositivo cliente através de uma ponto de distribuição
Hierarquia de Servidores de Administração: Servidor de Administração principal e Servidor de Administração secundário
Hierarquia de Servidores de Administração com um Servidor de Administração secundário na DMZ
Servidor de Administração, um gateway de conexão em um segmento da rede e um dispositivo cliente
Servidor de Administração e dois dispositivos na DMZ: um gateway de conexão e um dispositivo cliente
Servidor de Administração e Kaspersky Security Center Web Console
Guia de Introdução
Guia de Proteção
Lista de verificação de proteção
Implementação do Servidor de Administração
Segurança de conexão
Contas e autenticação
Gerenciamento da proteção do Servidor de Administração
Gerenciar a proteção do Agente de Rede
Gerenciamento de proteção dos dispositivos cliente
Configuração da proteção para aplicativos gerenciados
Manutenção do Servidor de Administração
Transferência de eventos para sistemas de terceiros
Recomendações de segurança para sistemas de informações de terceiros
Recomendações para usar aplicativos de segurança da Kaspersky
Cenário: Autenticação do MySQL Server
Cenário: Autenticação TLS bidirecional do PostgreSQL para o banco de dados do Servidor de Administração e o banco de dados do IAM
Preparação para implementação
Selecionar a configuração do Kaspersky Security Center Linux
Configuração padrão: escritório único
Configuração padrão: Alguns escritórios de larga escala executam por si seus próprios administradores
Configuração padrão: múltiplos pequenos escritórios remotos
Selecionar uma estrutura para a proteção de uma empresa
Esquemas típicos para implementação do sistema de proteção
Selecionar um DBMS
Fornecer acesso à Internet ao Servidor de Administração
Acesso à Internet: Servidor de Administração em uma rede local
Acesso à Internet: Servidor de Administração em DMZ
Instalação
Configuração do servidor MariaDB x64 para trabalhar com o Kaspersky Security Center Linux
Configuração do servidor de DBMS baseado em PostgreSQL para trabalhar com o Kaspersky Security Center Linux
Configuração do servidor MySQL x64 para trabalhar com o Kaspersky Security Center Linux
Preparar um cluster DBMS de alta disponibilidade para funcionar com o Kaspersky Security Center Linux

Instalação do Kaspersky Security Center Linux
- Instalação do Kaspersky Security Center Linux no modo silencioso
- Instalação do Kaspersky Security Center Linux no Astra Linux no modo de ambiente de software fechado

Instalar o Kaspersky Security Center Web Console
- Parâmetros de instalação do Kaspersky Security Center Web Console
- Instalação do Kaspersky Security Center Web Console no Astra Linux no modo de ambiente de software fechado

Instalação do Kaspersky Security Center Linux com um script

Implementação do cluster de failover do Kaspersky Security Center Linux
- Cluster de failover do Kaspersky Security Center Linux. Esquemas de implementação
- Cluster de failover do Kaspersky Security Center Linux
  - Cenário: implantação de um cluster de failover do Kaspersky Security Center Linux
  - Cluster de failover da Kaspersky Security Center Linux. Requisitos de hardware e software
  - Preparação de um servidor de arquivos para um cluster de failover do Kaspersky Security Center Linux
  - Preparação de nós para um cluster de failover do Kaspersky Security Center Linux
  - Instalação do Kaspersky Security Center Linux nos nós do cluster de failover do Kaspersky Security Center Linux
  - Como iniciar e interromper nós de cluster manualmente
  - Reinstalar um nó de cluster de failover
  - Instalação do Kaspersky Security Center Web Console conectado com o Servidor de Administração instalado nos nós do cluster de failover do Kaspersky Security Center Linux
- Cluster de failover da Kaspersky Security Center Linux distribuído geograficamente
  - Cluster distribuído geograficamente que executa o Ubuntu com o DBMS do PostgreSQL
    - Preparação de um sistema de arquivos de nós de cluster
    - Configurar um sistema de arquivos de cluster replicado
    - Instalação e configuração do Corosync e o Pacemaker nos nós de cluster
    - Instalação e configuração do DBMS do PostgreSQL
    - Instalação da Kaspersky Security Center Linux nos nós de cluster de failover distribuídos geograficamente
  - Cluster distribuído geograficamente que executa o SberLinux com o DBMS do Platform V Pangolin
    - Preparação de um sistema de arquivos de nós de cluster
    - Configurar um sistema de arquivos de cluster replicado
    - Instalação e configuração do Corosync e o Pacemaker nos nós de cluster
    - Instalação e configuração do DBMS do Platform V Pangolin
    - Instalação da Kaspersky Security Center Linux nos nós de cluster de failover distribuídos geograficamente
  - Instalação do Kaspersky Security Center Web Console em nós de cluster de failover distribuídos geograficamente

Contas para uso com o DBMS
- Criação de bancos de dados MySQL e MariaDB e contas de usuário
- Criar bancos de dados baseados em PostgreSQL e contas de usuário
- Mover dados de um espaço de tabela compartilhado para um espaço de tabela individual nos DBMSs MySQL e MariaDB

Certificados para trabalhar com o Kaspersky Security Center Linux
- Sobre os certificados do Kaspersky Security Center
- Requisitos para certificados personalizados usados no Kaspersky Security Center Linux
- Reemissão dos certificados internos do Kaspersky Security Center Web Console
- Substituir o certificado do Kaspersky Security Center Web Console
- Converter um certificado PFX para o formato PEM
- Cenário: especificação do certificado personalizado do Servidor de Administração
- Substituição do certificado do Servidor de Administração usando o utilitário klsetsrvcert
- Conexão dos Agentes de Rede ao Servidor de Administração usando o utilitário klmover
- Reemissão do certificado do Servidor Web

Alterar o certificado IAM padrão para um certificado personalizado

Adicionar o endereço do Servidor de Administração à configuração do Servidor IAM

Definir uma pasta compartilhada

Login no Kaspersky Security Center Web Console e logout

Interface do Kaspersky Security Center Web Console

Alteração do idioma da interface do Kaspersky Security Center Web Console

Alteração da página inicial do Kaspersky Security Center Web Console

Adicionar e remover favoritos

Instale o Kaspersky Security Center Web Console.

Assistente de início rápido

Etapa 1. Especificando as configurações de conexão da Internet

Etapa 2. Download das atualizações necessárias

Etapa 3. Seleção dos ativos a serem protegidos

Etapa 4. Selecionar a criptografia em soluções

Etapa 5. Configurar a instalação dos plugins para os aplicativos gerenciados

Etapa 6. Baixando os pacote de distribuição e criando pacotes de instalação

Etapa 7. Configurar a Kaspersky Security Network

Etapa 8. Selecionando o método de ativação do aplicativo

Etapa 9. Especificar as configurações de gerenciamento de atualização de terceiros

Etapa 10. Criar uma configuração básica de proteção de rede

Etapa 11. Configurar notificações por e-mail

Etapa 12. Fechar o Assistente de início rápido

Assistente de implementação da proteção

Etapa 1. Iniciar o assistente de implementação da proteção

Etapa 2. Seleção do pacote de instalação

Etapa 3. Seleção de um método de distribuição de arquivo de chave ou código de ativação

Etapa 4. Seleção de versão do Agente de Rede

Etapa 5. Seleção de dispositivos

Etapa 6. Especificação das configurações de tarefa de instalação remota

Etapa 7. Gerenciamento de reinício

Etapa 8. Remoção de aplicativos incompatíveis antes de instalação

Etapa 9. Movimentação de dispositivos para dispositivos gerenciados

Etapa 10. Seleção de contas para acessar dispositivos

Etapa 11. Início da instalação

Atualização do Kaspersky Security Center Linux

Atualização da Kaspersky Security Center Linux da versão 16 ou posterior

Atualização do Kaspersky Security Center Linux da versão 16 ou posterior usando o arquivo de instalação

Atualização da Kaspersky Security Center Linux da versão 16 ou posterior por meio do backup

Atualização da Kaspersky Security Center Linux versão 16 ou posterior nos nós de cluster de failover da Kaspersky Security Center Linux

Atualização da Kaspersky Security Center Linux da versão 15.4 ou anterior

Atualização da Kaspersky Security Center Linux da versão 15.4 ou anterior usando o arquivo de instalação

Atualização da Kaspersky Security Center Linux da versão 15.4 ou anterior por meio do backup

Atualização da Kaspersky Security Center Linux da versão 15.4 ou anterior nos nós de cluster de failover da Kaspersky Security Center Linux

Atualizar o Kaspersky Security Center Web Console

Atualização do Kaspersky Security Center Web Console no Astra Linux no modo de ambiente de software fechado

Migração para o Kaspersky Security Center Linux
Guia geral para migração para um novo servidor do Kaspersky Security Center Linux
Tutorial em vídeo: Migração para o Kaspersky Security Center Linux utilizando o backup de dados do Servidor de Administração
Migração para o Kaspersky Security Center usando o Assistente de migração
Exportação de objetos de grupo a partir do Kaspersky Security Center Windows
Importação do arquivo de exportação no Kaspersky Security Center Linux
Alternância entre dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux
Configurando o Servidor de Administração
Configuração do endereço de conexão do Servidor de Administração
Configuração da conexão do Kaspersky Security Center Web Console ao Servidor de Administração
Configuração de uma lista de permissão de endereços IP para conexão com o Kaspersky Security Center Linux
Definição das configurações de acesso à Internet para o Servidor de Administração
Hierarquia de Servidores de Administração
Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário
Visualizar a lista de Servidores de administração secundários
Gerenciar Servidores de Administração virtuais
Criar um Servidor de Administração virtual
Ativando ou desativando um Servidor de Administração virtual
Atribuição de um administrador para um Servidor de Administração virtual
Alterar o Servidor de Administração para dispositivos cliente
Excluindo um Servidor de Administração virtual
Configuração do registro em log de eventos de conexão do Servidor de Administração
Configuração do número máximo de eventos no repositório de eventos
Mover Servidor de Administração para outro dispositivo
Alteração do nome do Servidor de Administração
Preservação das conexões pela adição de um novo registro DNS
Preservação das conexões pela mudança para a conectividade baseada em endereço IP
Restauração de conexões interrompidas após a alteração do nome do servidor
Alterando credenciais de DBMS
Cópia backup e restauração dos dados do Servidor de Administração
Criando uma tarefa de backup de dados do Servidor de Administração
Usando o utilitário klbackup para fazer backup e recuperar dados
Uso do utilitário klbackup para alterar dispositivos gerenciados sob gerenciamento de outro Servidor de Administração
Backup e restauração de dados do Servidor de Administração ao usar MySQL ou MariaDB
Manutenção do Servidor de Administração
Excluir uma hierarquia de Servidores de Administração
Acesso a servidores DNS públicos
Configurar interface
Conexão criptografado a um Servidor de Administração
Criptografar comunicação com TLS
Configurações de rede para interação com serviços externos
Lista de sub-redes globais
Verificar a integridade dos módulos usando os utilitários klscmodchk e integrity_checker
Localizar dispositivos na rede
Cenário: Localizar dispositivos na rede
Sondagem da rede do Windows

- Sondagem do conjunto de IPs
- Adição e modificação de um conjunto de IPs
- Sondagem Zeroconf
- Sondagem do controlador de domínio
- Autenticação e conexão com um controlador de domínio
- Configuração de um controlador de domínio Samba
- Inventário de equipamentos
  - Adição de informações dobre novos dispositivos
  - Configuração de critérios usados para definir dispositivos corporativos
- Usar o modo dinâmico VDI nos dispositivos cliente
  - Ativar o modo dinâmico VDI nas propriedades de um pacote de instalação para o Agente de Rede
  - Mover os dispositivos da VDI para um grupo de administração

Gerenciamento de dispositivos cliente

- Configurações de um dispositivo gerenciado
- Verificar a conexão entre um dispositivo cliente e o Servidor de Administração. Utilitário klnagchk
- Regras de migração de dispositivos
  - Criar regras para mover dispositivos
  - Copiar as regras para mover dispositivos
  - Condições para migrar uma regra de um dispositivo
- Adicionar dispositivos manualmente a um grupo de administração
- Migrando dispositivos ou clusters manualmente para um grupo de administração
- Sobre clusters e matrizes de servidores
- Propriedades de um cluster ou matriz de servidores
- Ajuste de pontos de distribuição e gateways de conexão
  - Sobre os pontos de distribuição
  - Configuração padrão de pontos de distribuição: escritório único
  - Configuração padrão de pontos de distribuição: múltiplos pequenos escritórios remotos
  - Calcular o número e a configuração de pontos de distribuição
  - Atribuir os pontos de distribuição automaticamente
  - Atribuir os pontos de distribuição manualmente
  - Adicionando um gateway de conexão na DMZ como um ponto de distribuição
  - Modificar a lista de pontos de distribuição para um grupo de administração
  - Ativando um servidor push
  - Aumento do limite de descritores de arquivo para o serviço klnagent
- Sobre os status do dispositivo
- Configurar a alternância dos status do dispositivo
- Seleções de dispositivos
  - Visualização da lista de dispositivos a partir de uma seleção de dispositivos
  - Criar uma seleção de dispositivos
  - Configurar uma seleção de dispositivos
  - Exportação da lista de dispositivos a partir de uma seleção de dispositivos
  - Remover os dispositivos de grupos de administração em uma seleção
- Tags de dispositivo
  - Criando uma tag de dispositivo
  - Renomeando uma tag de dispositivo
  - Excluindo uma tag de dispositivo
  - Visualizando dispositivos aos quais uma tag está atribuída

Visualizando as tags atribuídas a um dispositivo

Identificação de um dispositivo manualmente

Removendo uma tag atribuído de um dispositivo

Visualização de regras para identificar dispositivos automaticamente

Edição de uma regra para identificar dispositivos automaticamente

Criação de uma regra para identificar dispositivos automaticamente

Execução de regras para identificar dispositivos automaticamente

Exclusão de uma regra para identificar dispositivos automaticamente

Gerenciamento de tags de dispositivo usando o utilitário klscflag

Criptografia e proteção de dados

Visualização da lista de unidades criptografadas

Visualização da lista de eventos de criptografia

Criação e visualização de relatórios de criptografia

Concessão de acesso a uma unidade criptografada no modo offline

Transmitindo as chave de criptografia entre Servidores de Administração

Alterar o Servidor de Administração para dispositivos cliente

Evitar conflitos entre vários Servidores de Administração

Migração de dispositivos conectados com o Servidor de Administração por meio de gateways de conexão para outro Servidor de Administração

Exibir e configurar as ações quando os dispositivos mostram inatividade

Enviar mensagens aos usuários de dispositivos

Ativar, desativar e reiniciar remotamente dispositivos clientes

Acesso remoto aos dispositivos gerenciados

Acesso remoto de um dispositivo baseado em Linux com o Kaspersky Security Center Web Console para um dispositivo gerenciado baseado em Linux

Acesso remoto de um dispositivo baseado em Linux com o Kaspersky Security Center Web Console para um dispositivo gerenciado baseado em Windows

Acesso remoto de um dispositivo baseado em Windows com o Kaspersky Security Center Web Console para um dispositivo gerenciado baseado em Linux

Acesso remoto de um dispositivo baseado em Windows com o Kaspersky Security Center Web Console para um dispositivo gerenciado baseado em Windows

Gerenciamento de Dispositivos Móveis

Usar o Firebase Cloud Messaging

Integração com a infraestrutura de chaves públicas

Gerenciamento de grupos de administração

Criação de grupos de administração

Instalação automática de aplicativos nos dispositivos em um grupo de administração

Mover grupos de administração

Exclusão de grupos de administração

Implementação de aplicativos Kaspersky

Cenário: Verificando a implementação dos aplicativos Kaspersky

Adicionando plugins de gerenciamento para aplicativos Kaspersky

Pacotes

Download e criação de pacotes de instalação para aplicativos Kaspersky

Criando pacotes de instalação a partir de um arquivo

Criar pacote de instalação autônomo

Configurações do pacote de instalação do Agente de Rede

Execução de pacotes independentes criados pelo Kaspersky Security Center Linux

- Instalação de aplicativos usando pacotes independentes
- Adequabilidade da atualização dos bancos de dados em um pacote de instalação de um aplicativo de segurança
- Alteração do limite de tamanho dos dados de pacotes de instalação personalizada
- Distribuindo pacotes de instalação para Servidores de Administração secundários
- Visualizar a lista de pacotes de instalação independente

Instalação do Agente de Rede para Linux

- Preparação de um dispositivo Linux para a instalação do Agente de Rede
- Preparo de um dispositivo executando o SUSE Linux Enterprise Server 15 para instalação do agente de rede
- Preparar um dispositivo executando o Astra Linux no modo de ambiente de software fechado para a instalação do Agente de Rede
- Preparação para a instalação do Agente de Rede em um sistema operacional Linux com glibc 2.5 (SO herdado)
- Preparativos para a instalação do Agente de Rede em um sistema operacional Linux com OpenSSH versão 6.4 (SO herdado)
- Instalação remota do Agente de Rede em um dispositivo Linux
- Instalar o Agente de Rede para Linux no modo silencioso (com um arquivo de resposta)
- Instalação do Agente de Rede para Linux no modo interativo
- O suporte do sistema de arquivos reverte para dispositivos com o Agente de Rede

Instalação do Agente de Rede para Windows

- Instalando o Agente de Rede para Windows no modo interativo
- Instalar o Agente de Rede para Windows no modo silencioso
- Implementação ao capturar e copiar a imagem de um dispositivo
- Modo de clonagem do disco do Agente de Rede
- Parâmetros de instalação do Agente de Rede

Instalação de aplicativos usando a tarefa de instalação remota

- Sobre as tarefas de instalação remotas no Kaspersky Security Center Linux
- Instalar um aplicativo remotamente
- Instalação remota de aplicativos em dispositivos macOS
- Instalando aplicativos nos Servidores de Administração secundários
- Instalação remota de aplicativos em dispositivos com o Agente de Rede instalado
- O gerenciamento do dispositivo reinicia na tarefa de instalação remota
- Implementação forçada usando a tarefa de instalação remota do Kaspersky Security Center Linux
- Instalando aplicativos no modo silencioso

Preparar um dispositivo macOS para a instalação remota do Agente de Rede

Infraestrutura virtual

- Dicas sobre como reduzir a carga em máquinas virtuais
- Suporte de máquinas virtuais dinâmicas
- Suporte para copiar máquinas virtuais

Especificando configurações para instalação remota em dispositivos Unix

Monitorar a implementação

Início e interrupção de aplicativos da Kaspersky

Substituição de aplicativos de segurança de terceiros

Remover aplicativos ou atualizações de software remotamente

Preparação de um dispositivo Windows para instalação remota

Criar a tarefa Executar scripts remotamente

- Criar um pacote de instalação com base em um arquivo de manifesto
- Preparar um arquivo para a tarefa Executar scripts remotamente

Instalar aplicativos remotamente em dispositivos usando a tarefa Executar scripts remotamente
Configurar notificações e monitoramento para a tarefa Executar scripts remotamente
Licenciamento
Licenciamento da Kaspersky Security Center Linux
Sobre o Contrato de Licença do Usuário Final
Sobre a licença
Sobre o certificado de licença
Sobre a chave de licença
Visualizar a Política de Privacidade
Opções de licença do Kaspersky Security Center
Sobre o arquivo de chave
Sobre a coleta de dados
Sobre a assinatura
Ativação do Kaspersky Security Center Linux
Licenciamento de aplicativos gerenciados da Kaspersky
Licenciamento de aplicativos gerenciados
Adição de uma chave de licença ao repositório do Servidor de Administração
Implementando uma chave de licença para dispositivos cliente
Distribuição automática de uma chave de licença
Visualizando de informações sobre chaves de licença em uso
Eventos do limite da licença excedidos
Excluindo uma chave de licença do repositório
Revogando o consentimento com um Contrato de Licença do Usuário Final
Renovando licenças para aplicativos da Kaspersky
Usando o Kaspersky Marketplace para escolher as soluções comerciais Kaspersky de sua preferência
Configuração de aplicativos da Kaspersky
Cenário: Configurar a proteção da rede
Sobre as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário
Configuração e propagação de políticas: abordagem centrada no dispositivo
Configuração e propagação de políticas: abordagem centrada no usuário
Políticas e perfis da política
Sobre as políticas e perfis de política
Sobre as configurações de bloqueio e bloqueadas
Herança de políticas e perfis de política
Hierarquia de políticas
Perfis de política em uma hierarquia de políticas
Como as configurações são implementadas em um dispositivo gerenciado
Gerenciamento de políticas
Visualização da lista de políticas
Criação de uma nova política
Configurações da política gerais
Modificar uma política
Ativando o desativando uma opção de herança de política
Cópia de uma política
Mover uma política
Exportação de uma política
Importação de uma política

Sincronização forçada
Visualizar o gráfico de status de distribuição da política
Ativação automática de uma política no evento Ataque de vírus
Exclusão de uma política
Gerenciando perfis de política
Visualização dos perfis de uma política
Alteração de uma prioridade de perfil da política
Criar um perfil da política
Copiar um perfil de política
Criar uma regra de ativação do perfil da política
Excluir um perfil de política
Exportar e importar um perfil de política
Configurações de política do Agente de Rede
Uso do Agente de Rede para Windows, Linux e macOS: comparativo
Comparativo entre configurações de Agente de Rede por sistemas operacionais
Ativar e desativar o modo de baixo consumo de recursos para o Agente de Rede
Definir as configurações de proteção de aplicativos gerenciados
Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security
Configuração manual da tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security
Kaspersky Security Network (KSN)
Sobre a KSN
Configurar o acesso à KSN
Ativação e desativação do uso da KSN
Visualizando a Declaração da KSN aceita
Aceitando uma declaração da KSN atualizada
Verificar se o ponto de distribuição funciona como servidor proxy da KSN
Visualização das estatísticas do servidor proxy da KSN
Tarefas de gerenciamento
Sobre as tarefas
Sobre o escopo de tarefa
Criar uma tarefa
Como iniciar uma tarefa manualmente
Como iniciar uma tarefa para dispositivos selecionados
Visualizando a lista de tarefas
Configurações de tarefa gerais
Exportação de tarefa
Importação de uma tarefa
Iniciar o Assistente para alterar a senha das tarefas
Etapa 1. Especificar as credenciais
Etapa 2. Selecionar uma ação a ser executada
Etapa 3. Visualizar os resultados
Visualização de resultados da execução de tarefas armazenados no Servidor de Administração
Tags de aplicativo
Tags de aplicativo
Criando uma tag de aplicativo
Renomeando uma tag de aplicativo
Atribuindo uma tag de aplicativos

Removendo tags atribuídas de um aplicativo
Excluir uma tag de aplicativos
Usando o utilitário klscflag para abrir a porta 13291
Registrar o aplicativo Kaspersky Industrial CyberSecurity for Networks no Kaspersky Security Center Web Console
Gerenciamento de usuários e funções dos usuários
Sobre as contas de usuário
Sobre as funções dos usuários
Configurar direitos de acesso aos recursos do aplicativo. Controle de acesso baseado em função
Direitos de acesso aos recursos do aplicativo
Funções de usuário predefinidas
Atribuição de direitos de acesso a objetos específicos
Atribuição de direitos de acesso a usuários e grupos de segurança
Adicionar uma conta de usuário interno
Criação de um grupo de segurança
Editar uma conta de usuário interno
Edição de um grupo de segurança
Atribuição de uma função a um usuário ou grupo de segurança
Adição de contas de usuário em um grupo de segurança interno
Atribuir um usuário como um proprietário de dispositivo
Atribuir um usuário como proprietário do dispositivo durante a instalação do Agente de Rede
Atribuir um usuário como proprietário do dispositivo Linux após a instalação do Agente de Rede
Remover um usuário como proprietário do dispositivo
Ativando a proteção da conta contra modificações não autorizadas
Configuração da autenticação de dois fatores
Sobre a autenticação de dois fatores para uma conta
Configuração de uma chave secreta de autenticação de dois fatores ao fazer login no Kaspersky Security Center Web Console
Permitir que os usuários configurem a autenticação de dois fatores
Redefinição e exclusão de uma chave secreta de autenticação de dois fatores
Excluir contas da autenticação de dois fatores
Editando o nome de um emissor do código de segurança
Alterar o número permitido de tentativas de entrada de senha
Excluir um usuário ou um grupo de segurança
Alterar a senha de uma conta de usuário
Criar uma função de usuário
Editar uma função de usuário
Editar o escopo de uma função de usuário
Excluir uma função de usuário
Associação de perfis da política a funções
Propagando funções de usuário aos Servidores de Administração secundários
Alterar a senha da conta
Revogação de direitos de administrador local
Configuração da autenticação do domínio Kerberos
Atualização dos bancos de dados e dos aplicativos da Kaspersky
Cenário: Atualização regular dos bancos de dados e dos aplicativos Kaspersky
Sobre atualização de bancos de dados, módulos de software e aplicativos da Kaspersky
Criação da tarefa baixar atualizações no repositório do Servidor de Administração

Verificação das atualizações baixadas
Criar a tarefa para baixar as atualizações aos repositórios de pontos de distribuição
Adicionando fontes de atualizações para a tarefa Baixar atualizações no repositório do Servidor de Administração
Aprovar e recusar atualizações de software
Instalação automática de atualizações para o Kaspersky Endpoint Security for Windows
Sobre usar os arquivos diff para atualizar bancos de dados e módulos do software Kaspersky
Ativação do recurso Baixar arquivos diff
Baixar atualizações por pontos de distribuição
Atualização de bancos de dados e módulos de software da Kaspersky em dispositivos offline
Monitoramento, relatórios e auditoria
Cenário: Monitoramento e relatórios
Sobre os tipos do monitoramento e relatórios
Acionamento de regras no modo de Treinamento inteligente
Exibir e confirmar detecções executadas usando regras do Controle Adaptativo de Anomalias
Adicionar exclusões a partir das regras do Controle Adaptativo de Anomalias
Painel e widgets
Usar o painel
Adição de widgets ao painel
Ocultação de um widget do painel
Movimentação de um widget no painel
Alteração do tamanho ou da aparência do widget
Alteração das configurações do widget
Sobre o modo somente painel
Configurando o modo somente painel
Relatórios de administração e proteção
Usar os relatórios
Criação de um modelo de relatório
Visualização e edição das propriedades do modelo de relatório
Exportar um relatório para um arquivo
Como gerar e visualizar um relatório
Criação de uma tarefa de entrega de relatório
Excluir os modelos de relatório
Centro de fortalecimento da segurança
Aplicativo de segurança instalado
Política aplicada
Atualização de banco de dados do antivírus configurada
Backup configurado
Manutenção do Servidor de Administração configurada
Criptografia TLS ativada
Todos os dispositivos são gerenciados
Eventos e seleções de eventos
Sobre eventos no Kaspersky Security Center Linux
Eventos dos componentes do Kaspersky Security Center Linux
Estrutura de dados da descrição do tipo de evento
Eventos do Servidor de Administração
Eventos críticos do Servidor de Administração
Eventos de falha funcional do Servidor de Administração

Eventos de aviso do Servidor de Administração
Eventos informativos do Servidor de Administração
Eventos do Agente de Rede
Eventos de falha funcional do Agente de Rede
Eventos de aviso do Agente de Rede
Eventos informativos do Agente de Rede
Usar as seleções de eventos
Criar uma seleção de eventos
Editar uma seleção de eventos
Visualizando uma lista de uma seleção de eventos
Exportar uma seleção de eventos
Importar uma seleção de eventos
Visualização das áreas de detalhes do evento
Exportar eventos para um arquivo
Visualização de um histórico de eventos a partir de um evento
Excluir os eventos
Excluir as seleções de eventos
Configuração do termo de armazenamento de um evento
Bloqueio de eventos frequentes
Sobre o bloqueio de eventos frequentes
Gerenciando o bloqueio de eventos frequentes
Removendo o bloqueio de eventos frequentes
Processamento e armazenamento do evento no Servidor de Administração
Notificações e status do dispositivo
Sobre notificações
Visualizar notificações que exigem atenção
Visualizar notificações do sistema
Visualizar informativos
Desativando o recebimento de Novidades Kaspersky
Configurar a alternância dos status do dispositivo
Configurar a entrega de notificações
Testar as notificações
Sobre os status do dispositivo
Parâmetros e variáveis de ambiente para descrever um evento
Visualizando informações sobre detecção de ameaças
Integrações para responder a alertas
Configurar a integração com o Active Directory para executar ações de resposta
Configurando a integração com a Kaspersky Automated Security Awareness Platform
Configurando a integração com o Kaspersky Threat Intelligence Portal Sandbox
Agrupando alertas por atributos
Cloud Discovery
Como ativar o Cloud Discovery usando o widget
Como adicionar o widget do Cloud Discovery ao painel
Exibir informações sobre o uso de serviços em nuvem
Nível de risco de um serviço de nuvem
Como bloquear o acesso a serviços de nuvem indesejados

Exportação de eventos para os sistemas SIEM
Configuração da exportação de eventos para sistemas SIEM
Pré-requisitos
Sobre a exportação de evento
Sobre a configuração de exportação de eventos em um sistema SIEM
Sobre a exportação de eventos usando formatos CEF e LEEF
Conversão de eventos para o formato CEF ou LEEF
Marcando eventos para exportação para sistemas SIEM em formato Syslog
Marcando eventos de um aplicativo da Kaspersky para exportação em formato Syslog
Marcando eventos gerais para exportação no formato Syslog
Sobre a exportação de eventos usando o formato Syslog
Configurando o Kaspersky Security Center Linux para exportação de eventos para o sistema SIEM
Monitoramento de alterações em políticas e perfis de política
Exportando eventos diretamente do banco de dados
Executar uma consulta SQL usando o utilitário klsql2
Exemplo de uma consulta SQL no utilitário klsql2
Exibir o nome de banco de dados do Kaspersky Security Center Linux
Exibir os resultados da exportação
Gerenciar revisões de objeto
Exibir e salvar uma revisão da política
Comparar as revisões de uma política
Reverter um objeto para uma revisão anterior
Ameaças ativas
Desinfeção de um arquivo não processado
Baixando um arquivo não processado
Exclusão de arquivos da seção Ameaças ativas
Exclusão de objetos
Baixar e excluir arquivos da Quarentena e do Backups de arquivo
Baixar arquivos da Quarentena e dos backups de arquivos
Sobre a remoção de objetos dos repositórios da Quarentena, do Backup de arquivos ou das Ameaças ativas
Gerenciamento do aplicativo pelo SNMP
Configuração do serviço snmpd no sistema operacional
Ativar e desativar as notificações por SNMP
Ativar e desativar o SNMP na Kaspersky Security Center Linux
Valores de identificadores de objetos para SNMP
Trabalhando com o Kaspersky Security Center Linux sob o licenciamento Kaspersky Next XDR Optimum
Integrações para responder a alertas
Configurar a integração com o Active Directory para executar ações de resposta
Configurando a integração com a Kaspersky Automated Security Awareness Platform
Configurando a integração com o Kaspersky Threat Intelligence Portal Sandbox
Agrupando alertas por atributos
Integração entre o Kaspersky Security Center Web Console e outras soluções
Estabelecendo uma conexão em segundo plano
Configuração da conexão do servidor proxy
Diagnóstico remoto de dispositivos cliente
Abertura da janela de diagnóstico remoto
Ativação e desativação do rastreamento para aplicativos

Download de arquivos de rastreamento de um aplicativo
Exclusão de arquivos de rastreamento
Download das configurações do aplicativo
Baixar as informações do sistema a partir de um dispositivo cliente
Download de registros de eventos
Início, interrupção e reinício do aplicativo
Execução do diagnóstico remoto do Agente de Rede do Kaspersky Security Center Linux e download dos resultados
Execução de um aplicativo em um dispositivo cliente
Execução do diagnóstico remoto em um dispositivo cliente baseado em Linux
Gerenciar aplicativos e arquivos executáveis de terceiros em dispositivos clientes
Usar o Controle de Aplicativos para gerenciar arquivos executáveis
Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos clientes
Criar uma categoria de aplicativos com conteúdo adicionado manualmente
Criar uma categoria de aplicativo que inclua arquivos executáveis dos dispositivos selecionados
Criar uma categoria de aplicativo que inclua arquivos executáveis da pasta selecionada
Visualizando a lista de categorias de aplicativo
Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos
Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows
Obter e visualizar uma lista de aplicativos instalados nos dispositivos cliente
Sobre aplicativos de terceiros
Instalar atualizações de software de terceiros
Cenário: Atualizando software de terceiros
Opções de instalação de atualizações de software de terceiros
As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias
Criar a tarefa Encontrar vulnerabilidades e atualizações necessárias
Exibir informações sobre atualizações disponíveis para software de terceiros
Exportando a lista de vulnerabilidades de software para um arquivo
Aprovando e recusando atualizações de software de terceiros
Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades
Adicionar regras para instalação da atualização
Configurações da tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades especificadas após a criação da tarefa
Atualizar aplicativos de terceiros automaticamente
Corrigindo vulnerabilidades de software de terceiros
Sobre como encontrar e corrigir vulnerabilidades de software
Cenário: Encontrar e corrigir vulnerabilidades de software de terceiros
Corrigindo vulnerabilidades de software de terceiros
Criar a tarefa Corrigir vulnerabilidades
Selecionar as correções do usuário para vulnerabilidades em software de terceiros
Visualizar informações sobre vulnerabilidades de software detectadas em todos os dispositivos gerenciados
Visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado
Visualizar as estatísticas de vulnerabilidades em dispositivos gerenciados
Exportar a lista de vulnerabilidades de software para um arquivo
Ignorar as vulnerabilidades de software
Criação de um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky
Ver e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky
Configurações do pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky

Correção de vulnerabilidades em uma rede isolada
Cenário: correção de vulnerabilidades de softwares de terceiros em uma rede isolada
Sobre a correção de vulnerabilidades de softwares de terceiros em uma rede isolada
Configuração do Servidor de Administração com acesso à Internet para corrigir vulnerabilidades em uma rede isolada
Configuração de Servidores de Administração isolados para corrigir vulnerabilidades em uma rede isolada
Transmissão de patches e instalação de atualizações em uma rede isolada
Desativar a transmissão de patches e a instalação de atualizações em uma rede isolada
Guia de referência de API
Práticas recomendadas para Provedores de Serviços
Planejamento da implementação do Kaspersky Security Center Linux
Fornecer acesso à Internet ao Servidor de Administração
Configuração padrão do Kaspersky Security Center Linux
Sobre os pontos de distribuição
Hierarquia de Servidores de Administração
Servidores de Administração virtual
Implementação e configuração inicial
Recomendações sobre a instalação do Servidor de Administração
Criar contas para os serviços do Servidor de Administração em um cluster para falhas
Selecionar um DBMS
Especificar o endereço do Servidor de Administração
Manter conexões ociosas
Implementar o Agente de Rede e os aplicativos de segurança
Configurar a proteção em uma rede da organização cliente
Configuração manual da política do Kaspersky Endpoint Security
Configurar a política na seção Proteção Avançada Contra Ameaças
Configurar a política na seção Proteção Essencial Contra Ameaças
Configurar a política na seção Configurações Gerais
Configurando a política na seção Configuração de eventos
Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security
Configuração manual da tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security
Agendar a tarefa Encontrar vulnerabilidades e atualizações necessárias
Configuração manual da tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades
Criação de uma estrutura de grupos de administração e atribuir pontos de distribuição
Configuração de cliente MSP padrão: escritório único
Configuração de cliente MSP padrão: múltiplos pequenos escritórios remotos
Hierarquia de políticas, usando perfis de política
Hierarquia de políticas
Perfis da política
Tarefas
Regras de migração de dispositivos
Categorização de software
Cópia backup e restauração das configurações do Servidor de Administração
Um dispositivo com o Servidor de Administração está inoperável
As configurações do Servidor de Administração ou o do banco de dados estão corrompidas
Sobre a configuração de perfis de conexão para usuários ausentes
Sobre a mudança do Agente de Rede para outro servidor de Administração
Criando um perfil de conexão para usuários ausentes

- Acesso remoto aos dispositivos gerenciados
  - Uso da opção "Não desconectar do Servidor de Administração" para fornecer conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração
  - Sobre verificar o tempo de conexão entre um dispositivo e o Servidor de Administração
  - Sobre a sincronização forçada
- Guia de dimensionamento
  - Sobre este Guia
  - Limitações do Kaspersky Security Center Linux
  - Cálculos para os Servidores de Administração
    - Cálculo de recursos de hardware para o Servidor de Administração
      - Requisitos de hardware para o DBMS e para o Servidor de Administração
      - Cálculo do espaço do banco de dados
      - Cálculo do espaço em disco
    - Cálculo do número e configuração de Servidores de Administração
    - Recomendações para conectar máquinas virtuais dinâmicas ao Kaspersky Security Center
  - Cálculos para pontos de distribuição e gateways de conexão
    - Requisitos para um ponto de distribuição
    - Calcular o número e a configuração de pontos de distribuição
    - Cálculo do número de gateways de conexão
  - Registro de informações sobre eventos para tarefas e políticas
  - Melhores práticas para um Servidor de Administração que gerencia um grande número de dispositivos
  - Considerações específicas e configurações ótimas de determinadas tarefas
    - Frequência da descoberta de dispositivos
    - Tarefa de backup dos dados do Servidor de Administração e tarefa de manutenção do banco de dados
    - Tarefas de grupo para atualizar o Kaspersky Endpoint Security
    - Tarefa de inventário
  - Detalhes da carga da rede espalhada entre o Servidor de Administração e os dispositivos protegidos
    - Taxa de tráfego sob diversos cenários
    - Uso de tráfego médio durante 24 horas
- Problemas conhecidos e limitações
- Entrar em contato com o Suporte Técnico
  - Como obter suporte técnico
  - Suporte técnico via Kaspersky CompanyAccount
  - Obter arquivos de dump do Servidor de Administração
- Fontes de informação sobre o aplicativo
- Glossário
  - Administrador cliente
  - Administrador do Kaspersky Security Center Linux
  - Administrador do provedor de serviço
  - Agente de atualização
  - Agente de autenticação
  - Agente de Rede
  - Aplicativo incompatível
  - Application settings
  - Arquivo de chave
  - Ataque de vírus
  - Atualização

Atualização disponível

Bancos de dados antivírus

Certificado compartilhado

Certificado do Servidor de Administração

Chave ativa

Chave reserva

Cloud Discovery

Configurações de tarefa

Console de Administração

Cópia de backup de dados do Servidor de Administração

Direitos de administrador

Dispositivo MDM do iOS

Dispositivos gerenciados

Domínio de difusão

Estação de trabalho do administrador

FileTransferBridge

Gateway de conexão

Gerenciamento centralizado de aplicativos

Gerenciamento direto de aplicativos

Gravidade do evento

Grupo de administração

Grupo de funções

HTTPS

Identity and Access Manager (IAM)

Instalação local

Instalação manual

Instalação remota

JavaScript

Lightweight Nagent (LWNGT)

Loja de aplicativos

Nível de importância do patch

Operador do Kaspersky Security Center

Pacote de instalação

Pasta de backup

Perfil

Perfil de configuração

Perfil de provisionamento

Período da licença

Política

Proprietário do dispositivo

Provedor de serviço de proteção antivírus

Reconhecimento de local de rede (NLA)

Repositório de eventos

Restauração

Restauração dos dados do Servidor de Administração

Segurança antivírus da rede

Servidor de Administração

Servidor de Administração cliente (Dispositivo cliente)
Servidor de Administração Principal
Servidor de Administração virtual
Servidor MDM do iOS
Servidor Web do Kaspersky Security Center Linux
Servidores de atualização da Kaspersky
SSL
Status de proteção
Status de proteção da rede
Tarefa
Tarefa de grupo
Tarefa local
Tarefa para dispositivos específicos
Usuários internos
Validador de Integridade do Sistema do Kaspersky Security Center (SHV)
Vulnerabilidade
Zona desmilitarizada (DMZ)
Informação sobre código de terceiros
Avisos de marca registrada

Ajuda do Kaspersky Security Center Linux

Novos recursos

- O que há de novo

Requisitos de hardware e software

- Requisitos do Servidor de Administração
- Requisitos do Web Console
- Requisitos do Agente de Rede

Guia de introdução

- Instalação
- Assistente de início rápido
- Assistente de implementação da proteção

Licenciamento e ativação

- Ativação do Kaspersky Security Center Linux
- Licenciamento de aplicativos gerenciados

Implementação e configuração

- Localizar dispositivos na rede
- Ajustar pontos de distribuição e/ou gateways de conexão
- Substituição de aplicativos de segurança de terceiros
- Implementação do aplicativo Kaspersky Implementação centralizada

- Configuração da proteção da rede
- Implementação do aplicativo Kaspersky Atualização de bancos de dados e módulos de software
- Configuração do endereço de conexão do Servidor de Administração
- Migração para o Kaspersky Security Center Linux
- Sobre a atualização do Kaspersky Security Center Linux

Monitoramento

- Monitoramento e relatórios
- Cloud Discovery

Gerenciamento de dispositivos cliente

- Acesso remoto aos dispositivos gerenciados

Gerenciamento de patches e vulnerabilidades

- Encontrar e corrigir vulnerabilidades de software de terceiros

Recursos adicionais

- Exportação de eventos para os sistemas SIEM
- Visualização das estatísticas do servidor proxy da KSN
- Guia de dimensionamento (apenas Ajuda on-line)

O que há de novo

Kaspersky Security Center 17 Linux

O Kaspersky Security Center 17 Linux inclui vários novos recursos e aprimoramentos:

- Os certificados do Web Console, do IAM e do Servidor de Administração agora podem ser adicionados manualmente e substituídos automaticamente sem reinstalar o Web Console.
- Ao visualizar o conteúdo de uma revisão ou comparar revisões de políticas, os dados dos perfis de política agora estão disponíveis.
- Agora, depois de executar uma tarefa para um dispositivo ou dispositivos específicos, você pode acessar as propriedades da tarefa para visualizar os resultados.
- Um novo indicador de nível de proteção foi adicionado ao Centro de fortalecimento, permitindo identificar dispositivos sobre os quais o controle pode ter sido perdido.
- As seguintes informações sobre dispositivos cliente foram adicionadas aos eventos publicados pelo Servidor de Administração para dispositivos gerenciados: nome DNS (FQDN), nome NetBIOS, endereço IP e DisplayName.
- Os recursos de auditoria foram ampliados:
  - Quando o Agente de Rede muda para outro Servidor de Administração, um evento agora é registrado no Log de Eventos Kaspersky. O evento indica o endereço do novo Servidor de Administração e o endereço do gateway, se houver.
  - Agora, os eventos estendidos são enviados ao importar e copiar políticas, bem como ao reverter uma política para uma revisão selecionada.
- Melhorias na experiência do usuário:
  - A seção **Tags** foi renomeada para **Tags de dispositivos**.
  - A seção **Tags de dispositivos**, com suas subseções, foi movida da seção **Gerenciamento de ativos** para a seção **Repositórios**.
  - Agora você pode baixar, em um arquivo, todos os eventos de um dispositivo ou uma seleção de eventos da lista de eventos.
- O script de instalação rápida do Kaspersky Security Center Linux agora oferece suporte a opções adicionais de implantação:
  - MySQL 8.4.10 com Ubuntu Server 26.04 LTS
  - MariaDB 10.11.18 com CentOS Stream 10
  - MariaDB 10.11.18 com RED OS 8
  - MariaDB 10.11.13 com Astra Linux 1.8.5

- O Servidor de Administração agora oferece suporte a novas versões de SGBD:
  - MariaDB 11.4
  - MariaDB 11.8
  - MariaDB 12.3
  - Platform V Pangolin 7.2.0.
  - Platform V Pangolin 7.2.0 (cluster de alta disponibilidade integrado)
- O Servidor de Administração e o Web Console agora oferecem suporte às seguintes novas versões de sistemas operacionais:
  - ALT Server 11
  - MosOS 15.6
- Agora, o Agente de Rede é compatível com as seguintes novas versões do sistema operacional:
  - Microsoft Windows 11 26H2 Home/Pro/Pro for Workstations/Enterprise/Education
  - Microsoft Windows 10 IoT Enterprise versão 1507
  - Debian GNU/Linux versões 12.10, 12.11 e 12.14 (Bookworm) ARM
  - Astra Linux Special Edition RUSB.10015-16 (versão 2) (atualização operacional 8.1) E2K
  - Astra Linux Special Edition RUSB.10265-01 (atualização operacional 8.1) E2K
  - Elbrus 9.3.6 E2K
  - ALT Workstation 11.2 ARM
  - ALT Server 11.1 ARM
  - ALT SP Workstation 10 E2K
  - ALT SP Server 10 E2K
  - ALT 8 SP Workstation E2K
  - ALT SP Server 8 E2K
  - MSVSPHERE 9.5 SERVER
  - MSVSPHERE 9.5 ARM
  - Amazon Linux 2023
  - MosOS 15.6

Kaspersky Security Center 16.3 Linux

O Kaspersky Security Center 16.3 Linux inclui vários novos recursos e aprimoramentos:

- Se você modificar uma política, será criado um evento de auditoria separado para cada parâmetro alterado. Os eventos são exportados para o SIEM.
- Adicionamos compatibilidade com o **Kaspersky SIEM** (KUMA) à funcionalidade de exportação de eventos para sistemas SIEM.
- O Kaspersky Security Center Linux agora é compatível com a solução Kaspersky Vulnerability Management.
- Para estar em conformidade com o Guia de proteção, elaboramos uma configuração otimizada do Kaspersky Endpoint Security for Linux para instalação nos dispositivos com Servidor de Administração, Web Console e DBMS, bem como para implementação do cluster de failover da Kaspersky Security Center Linux.
- Agora você pode especificar o esquema de banco de dados personalizado ao instalar o Kaspersky Security Center Linux.
- Em **Monitoramento** → **Painel**, o indicador de nível de proteção ajuda a avaliar a segurança do Servidor de Administração e dos pontos de distribuição. Se o indicador estiver amarelo ou vermelho, execute ações para resolver os problemas e alterar o estado do indicador para verde.
- Está disponível um método simplificado de implementação do Kaspersky Security Center Linux. Agora você pode usar um script de instalação.
- Está disponível um pacote de distribuição especial para o Kaspersky Network Agent for Linux Legacy com glibc versão 2.5 para dar suporte aos seguintes sistemas operacionais desatualizados:
  - CentOS 5.2
  - CentOS 5.4
  - CentOS 6.4
  - CentOS 6.6
  - Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.4) 64 bits
- Agora, o Agente de Rede é compatível com as seguintes novas versões do sistema operacional:
  - Microsoft Windows 11 IoT Enterprise version 25H2 64 bits
  - SberOS 3.6.1
  - Ubuntu Server 26.04 LTS
- Os seguintes DBMSs não são mais compatíveis:
  - Aurora MySQL 5.7
  - MariaDB 10.1.30

- Melhorias na experiência do usuário:
  - Filtragem aprimorada para as tabelas de **Tarefas** e **Políticas**. Agora você pode adicionar várias condições usando a lógica `OR`, bem como usar um novo operador que permite selecionar vários valores para uma única propriedade e exibir registros correspondentes a pelo menos um dos critérios especificados.
  - No menu principal:
    - Está disponível uma nova seção de **Gerenciamento de software**. Agora, as seguintes seções foram movidas para o **Gerenciamento de software**: **Pacotes de instalação**, **Aplicativos da Kaspersky**, **Aplicativos de terceiros**, **Catálogo de software da Kaspersky** e **Gerenciamento de patches**.
    - Agora, as seções **Dispositivos não atribuídos** e **Hardware** foram movidas para o **Gerenciamento de ativos**.
    - As seções **Tarefas** e **Repositórios** foram movidas para o primeiro nível do menu.
    - A seção **Backups de plug-ins da web** não é mais usada e foi removida do Web Console.

Kaspersky Security Center 16.2 Linux



Visão geral dos novos recursos da versão 16.2. Vídeo

O Kaspersky Security Center 16.2 Linux inclui vários novos recursos e aprimoramentos:

- No Kaspersky Security Center Web Console, agora você pode configurar um gateway de conexão na zona desmilitarizada (DMZ).

  Use a opção **Usar o gateway de conexão DMZ por endereço** para configurar um gateway de conexão.

- O algoritmo para preservar o identificador de dispositivo do Agente de Rede (o parâmetro `Device ID`) nos dispositivos Linux foi aprimorado. Se o número de série do BIOS, o número de série da placa-mãe, os identificadores do disco de armazenamento ou o endereço MAC de um dispositivo corresponderem a valores já conhecidos, o Servidor de Administração identificará corretamente o dispositivo como previamente descoberto após uma atualização do sistema operacional ou uma alteração do endereço MAC.

- Foi adicionado suporte para um cluster de failover da Kaspersky Security Center Linux distribuído geograficamente com nós localizados em diferentes data centers. Na configuração de cluster distribuído geograficamente, todos os componentes são de failover.

- Agora é possível exportar eventos para um sistema SIEM nos formatos CEF ou LEEF.
- Foi adicionado suporte para o cluster PostgreSQL de alta disponibilidade com Patroni para failover automatizado e HAProxy para balanceamento de carga.
- Você pode comparar as revisões da política. A opção está disponível para as políticas do Servidor de Administração, Agente de Rede, Kaspersky Endpoint Security for Windows (a partir da versão 14.0 do plug-in da web) e Kaspersky Endpoint Security for Mac (a partir da versão 12.2.1 Patch A do plug-in da web). A lista de aplicativos da Kaspersky compatíveis com esse recurso será expandida em versões futuras.
- Agora há compatibilidade com SNMP. Você pode fornecer informações, estatísticas e eventos do Servidor de Administração para aplicativos cliente de terceiros usando SNMP.
- A sondagem de rede do Windows agora tem suporte para pontos de distribuição baseados no Windows.
- Já está disponível um pacote de instalação único para o Agente de Rede para Linux. O pacote de instalação inclui versões para diferentes gerenciadores de pacotes e arquiteturas de CPU. O ambiente é automaticamente detectado durante a instalação e o pacote de instalação apropriado do Agente de Rede é instalado.
- Os eventos agora incluem informações sobre o iniciador dos comandos executados em dispositivos móveis.
- O componente NSQ é removido do pacote de distribuição do Kaspersky Security Center Web Console. O serviço KSCWebConsoleMessageQueue.service não é mais usado e será removido após a atualização do Kaspersky Security Center Web Console.
- Se o Servidor de Administração não tiver acesso ao repositório de distribuições de aplicativos para instalação remota, antes de criar pacotes de instalação a partir de um arquivo para aplicativos em dispositivos Windows, será necessário baixar módulos adicionais do site da Kaspersky: Arquivos para instalação remota via Kaspersky Security Center (os arquivos ri_utils_win32.zip e ri_utils_arm64.zip).
- Agora, o Agente de Rede é compatível com a arquitetura Windows ARM de 64 bits. A compatibilidade com aplicativos gerenciados pode ser verificada na documentação de ajuda correspondente.
- O Kaspersky Security Center Linux é compatível com o Kaspersky Sandbox.
- Melhorias na experiência do usuário:
  - Agora você pode excluir todos os eventos de uma seleção de eventos e de uma lista de eventos do dispositivo de uma só vez.

    As opções **Selecionar tudo** e **Selecionar todos na página atual** estão disponíveis na seleção de eventos e na lista de eventos do dispositivo.
  - Agora é possível especificar a prioridade de uma regra de movimentação manualmente.

    O botão **Alterar prioridade** fica disponível quando você seleciona uma regra de movimentação, permitindo que você especifique a nova prioridade.
- O Kaspersky Security Center Linux é compatível com o Platform V SberLinux OS Server (SLO) 9.6.
- O Kaspersky Security Center Linux agora oferece suporte ao trabalho com os seguintes DBMSs:
  - MySQL Standard Edition 8.4
  - MySQL Enterprise Edition 8.4
  - PostgreSQL 18

- Postgres Pro 18 (todas as edições)
- Postgres Pro 18 Enterprise (cluster com alta disponibilidade integrada)

- Agora, o Agente de Rede é compatível com as seguintes novas versões do sistema operacional:
  - Microsoft Windows 11 Home/Pro/Pro para Workstations/Enterprise/Education ARM
  - Platform V SberLinux OS Server (SLO) 9.6

Kaspersky Security Center 16.1 Linux

O Kaspersky Security Center 16.1 Linux inclui vários novos recursos e aprimoramentos:

- Agora, a autenticação de dois fatores está ativada por padrão. A opção global para desativar a autenticação de dois fatores não está mais disponível. Para garantir que os usuários possam fazer login no Kaspersky Security Center Web Console e continuar usando os scripts de automação OpenAPI, ative a autenticação de dois fatores para todos os usuários antes da atualização.
- Você pode salvar um perfil de política em um arquivo KLPROF sem exportá-la e, em seguida, usar esse arquivo para importar o perfil salvo para a política.
- O Agente de Rede agora opera em um dispositivo que executa o SO ALT no modo de ambiente de software fechado.
- Adicionamos a compatibilidade para a autenticação do domínio baseada em Kerberos para usuários do domínio que não utilizam senha por meio do protocolo SCRIL, ativando a conexão única (SSO) baseada em certificado.
- Melhorias na experiência do usuário:
  - A filtragem de dispositivos cliente por meio da versão do sistema operacional e do gerenciador de pacotes agora inclui versões do sistema operacional Linux.
  - Aprimoramento do mecanismo de paginação para tabelas no Kaspersky Security Center Web Console: o número padrão de itens exibidos foi aumentado para 50, e o número personalizado de itens exibidos agora é preservado entre sessões.
  - Comentários para categorias de aplicativos que permitem adicionar descrições de regras para incluir e excluir aplicativos em uma categoria.
  - Por padrão, a lista de pacotes de instalação disponíveis agora exibe somente os pacotes de instalação do aplicativo da Kaspersky no idioma da interface do Kaspersky Security Center Web Console e em inglês.
- O Kaspersky Security Center Linux é compatível com o trabalho com o Kaspersky Endpoint Security for Linux 12.4.
- O Kaspersky Security Center Linux é compatível com o trabalho com as novas versões do sistema operacional:
  - Debian GNU/Linux 13 (Trixie)
  - CentOS Stream 10
  - Red Hat Enterprise Linux Server 10.x

- Agora, o Agente de Rede é compatível com as seguintes novas versões do sistema operacional:
  - ALT Workstation 11
  - ALT Server 11
  - ALT Education 11
  - AlterOS 2025
  - SberOS 3.4.0
  - SberOS 3.5.0
  - OSnova 3.*

Kaspersky Security Center 16 Linux

O Kaspersky Security Center 16 Linux inclui vários novos recursos e aprimoramentos:

- Os controladores de domínio FreeIPA e ALD Pro são compatíveis.
- A autenticação do domínio (conexão única) foi implementada. O recurso de conexão única permite ativar a autenticação segura no Kaspersky Security Center 16 Web Console sem ter que inserir a senha novamente na rede corporativa. Para usar a autenticação do domínio, você deve especificar os parâmetros adicionais no arquivo de resposta durante a instalação do Kaspersky Security Center Web Console.
- O Servidor de Administração Linux do Kaspersky Security Center 16 só é compatível com o Kaspersky Security Center 16 Web Console. As versões anteriores do Kaspersky Security Center Web Console não podem ser usadas.
- Agora você pode usar a funcionalidade Kaspersky Next XDR Optimum sob uma licença de avaliação, desde que tenha adicionado um Servidor de Administração secundário, ativado esse servidor com a licença de avaliação e aplicado a chave de licença nos dispositivos gerenciados pelo Servidor de Administração secundário.
- Melhorias na experiência do usuário:
  - A navegação pelos grupos e Servidores de Administração foi atualizada: agora é possível alternar facilmente entre eles usando um único painel de navegação.
  - As configurações de perfil foram movidas para o painel superior.
  - As seguintes seções do menu principal foram renomeadas:
    - A seção **Ativos (Dispositivos)** agora é denominada **Gerenciamento de ativos**.
    - **Os dispositivos gerenciados** são denominados **Dispositivos gerenciados**.
    - **Os links rápidos** foram renomeados para **Navegação do console**.

- É possível minimizar o menu principal para ícones, se necessário.
- A seção de **notícias da Kaspersky** foi excluída do **Monitoramento → Notificações**.

- Os filtros aplicados às tabelas nas seções **Operações → Gerenciamento de patches → Vulnerabilidades de software** e **Operações → Gerenciamento de patches → Atualizações de software** agora são salvos com êxito e não são redefinidos.
- O Kaspersky Security Center Linux é compatível:
  - com o Kaspersky NGFW
  - com as seguintes versões do sistema operacional (para os dispositivos gerenciados):
    - MosOS 15.5 Arbat
    - Microsoft Windows 11 25H2
    - CentOS 6.4
    - CentOS 6.6

Kaspersky Security Center 15.4 Linux

O Kaspersky Security Center 15.4 Linux inclui vários novos recursos e aprimoramentos:

- Agora, perfis de conexão para usuários ausentes em dispositivos Linux estão disponíveis. Ao usar perfis de conexão, é possível configurar as regras para Agentes de Rede em dispositivos Linux para que se conectem com o mesmo ou com diferentes Servidores de Administração, dependendo da localização do dispositivo.
- A transmissão de chaves de criptografia entre Servidores de Administração agora está disponível.
- Agora, o Kaspersky Thin Client é compatível.
- Agora, o cluster de alta disponibilidade integrado do Platform V Pangolin é compatível.
- Agora, o cluster de alta disponibilidade integrado do Postgres Pro é compatível. Os nós deste cluster DBMS são especificados na string de conexão ao instalar o Kaspersky Security Center Linux.
- O Kaspersky Security Center Linux agora oferece suporte ao trabalho com os seguintes DBMSs:
  - Platform V Pangolin 6.5.1
  - Tantor SE 1C for Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.8)
  - Jatoba 5
- Suporte para as versões 8.10.1, 9.0.1, 9.5.1 do Platform V SberLinux OS Server (SLO).
- O arquivo comprimido KlAkOAPI.tar.gz foi excluído da ajuda. O arquivo comprimido KlAkOAPI.tar.gz está localizado na pasta de instalação do Kaspersky Security Center Linux.

- O botão **Verificar** foi excluído da seção **Quarentena**.

- Informações sobre tamanho, hash de arquivo e caminho não estão disponíveis na lista de pacotes de instalação do pacote independente do Agente de Rede ou de quaisquer pacotes criados em Servidores de Administração virtuais, pois esses pacotes independentes são gerados no momento do download.

Kaspersky Security Center 15.4 Linux sob o licenciamento Kaspersky Next XDR Optimum

Se você ativou o Servidor de Administração sob o Licenciamento do Kaspersky Next XDR Optimum e implementou a chave de licenciamento do Kaspersky Next XDR Optimum em seus aplicativos gerenciados, poderá fazer o seguinte:

- Agrupe alertas por atributos.

- Configure integrações para responder a ameaças.

Kaspersky Security Center 15.3 Linux

O Kaspersky Security Center 15.3 Linux inclui vários novos recursos e aprimoramentos:

- O utilitário klcsngtgui é removido do kit de distribuição do Kaspersky Security Center Linux. Recomendamos usar o utilitário klnagchk no lugar do klcsngtgui.

- Agora, o Agente de Rede é compatível com as seguintes novas versões do sistema operacional:

  - Windows Server 2025

  - Servidor Fedora Linux 41

  - Fedora Linux Workstation 41

- O Kaspersky Security Center Linux agora oferece suporte ao trabalho com os seguintes DBMSs:

  - PostgreSQL 17

  - Postgres Pro 17

- Agora, você pode baixar somente as atualizações necessárias de bancos de dados e módulos de software para os aplicativos de segurança da Kaspersky usando o Utilitário de atualização da Kaspersky. Na janela de propriedades da tarefa **Baixar atualizações no repositório do Servidor de Administração**, ative a opção **Baixar o arquivo de solicitação de atualização automaticamente** e especifique o caminho onde a Kaspersky Security Center Linux criará este arquivo com informações sobre as atualizações a serem baixadas.

- Agora, a visualização de estatísticas de uso do servidor proxy KSN está disponível.

- A migração dos dados do Servidor de Administração do Kaspersky Security Center Windows para o Kaspersky Security Center Linux com o uso do utilitário klbackup foi atualizada. Agora, é possível migrar dados do Servidor de Administração armazenados no banco de dados do Microsoft SQL Server para PostgreSQL ou Postgres Pro.

- Agora, a configuração do endereço de conexão do Servidor de Administração está disponível. O endereço de conexão do Servidor de Administração é usado como endereço padrão ao criar os pacotes de instalação do Agente de Rede e como endereço do servidor proxy KSN ao conectar dispositivos gerenciados com a KSN.

- Agora, é possível reiniciar dispositivos gerenciados centralmente.
- Agora, as Informações sobre os usuários atualmente conectados ao dispositivo gerenciado Linux são exibidas na sessão **Geral** → **Sessões** da janela de propriedades do dispositivo.
- Agora, é possível obter acesso remoto aos dispositivos gerenciados Linux e Windows por meio do Agente de Rede instalado nesses dispositivos. A conexão é estabelecida com o uso de RDP, VNC ou WDS. Ao estabelecer uma conexão com o dispositivo, o administrador obtém acesso total às informações armazenadas neste dispositivo e pode gerenciar os aplicativos instalados nele.
- Carregar e executar um aplicativo (ou script) para diagnóstico em um dispositivo gerenciado. Agora, é possível carregar o diretório ou arquivo compactado contendo o arquivo executável ou o próprio arquivo executável. Após a execução bem-sucedida do aplicativo, é possível baixar os resultados da execução.
- Melhorias na experiência do usuário, incluindo uma nova seção de **Links rápidos**. Essa seção exibe o mapa do menu principal e fornece acesso rápido a todas as seções do Kaspersky Security Center Web Console. Por padrão, os **Links rápidos** são definidos como a página inicial.

Kaspersky Security Center 15.2 Linux

O Kaspersky Security Center 15.2 Linux inclui vários novos recursos e aprimoramentos:

- Novos recursos para gerenciar senhas de contas de usuários internos:
  - É possível forçar um usuário interno a alterar uma senha na primeira tentativa de fazer login (ou próxima tentativa) no Kaspersky Security Center Web Console.
  - Nova opção para configurar o período de expiração da senha para contas de usuários internos.
- Agora, é possível fazer backup de dados do Servidor de Administração do Kaspersky Security Center Windows e restaurá-lo no Kaspersky Security Center Linux com o uso do utilitário klbackup. A migração pode ser executada sem perda de dados entre DBMS do mesmo tipo ou Microsoft SQL Server → MySQL ou MariaDB.
- O Kaspersky Security Center Linux agora oferece suporte ao trabalho com os seguintes DBMSs:
  - PostgreSQL 16.x
  - Postgres Pro 16.x
- Agora, o Kaspersky Security Center Linux é compatível com alguns tipos de clusters PostgreSQL e Postgres Pro.
- Compatibilidaed com novos sistemas operacionais e novas versões de sistemas operacionais, inclusive com as novas versões do OS MES (Moscow Electronic School), MosTech e MosTech Server.
- Melhorias na experiência do usuário, incluindo:
  - Novo botão **Salvar** na janela de configurações da política. Use este botão caso queira salvar as alterações sem fechar a janela de configurações da política.

- Agora, é possível gerenciar o envio de arquivos para dispositivos Android, excluir os arquivos enviados anteriormente e configurar suas configurações na nova seção "Aplicativos e arquivos" do plug-in do Kaspersky Mobile Devices Protection and Management.

- Agora, é possível transferir pacotes de instalação de aplicativos e perfis de gerenciamento de dispositivos para dispositivos móveis sem conectá-los diretamente ao Servidor de Administração com o uso de um novo serviço de Servidor Web em um gateway de conexão.

Kaspersky Security Center 15.1 Linux

O Kaspersky Security Center 15.1 Linux inclui vários novos recursos e aprimoramentos:

- Agora, o Kaspersky Security Center Web Console é compatível com o gerenciamento de dispositivos móveis por meio do plug-in do Kaspersky Mobile Devices Protection and Management.

- Agora, é possível instalar e configurar os Servidores de MDM do iOS por meio do plug-in de configurações do Servidor de MDM do iOS para gerenciar dispositivos iOS MDM.

- Agora, é possível pode gerenciar os certificados de dispositivos móveis.

- Agora, o Kaspersky Endpoint Security for Android é compatível.

- Agora, o Kaspersky Security for iOS é compatível.

- Agora, o Kaspersky Endpoint Security for Aurora é compatível.

- Gerenciamento de vulnerabilidades e patches para dispositivos gerenciados baseados no Windows. Você pode gerenciar as atualizações de software de terceiros instaladas em dispositivos gerenciados baseados no Windows e corrigir vulnerabilidades nesse software por meio da instalação das atualizações necessárias.

- O Kaspersky Security Center Linux agora sonda controladores de domínio página por página, em vez de sondar todo o controlador de domínio de uma só vez. Isso permite que você faça a sondagem dos controladores de domínio que incluem um grande número de entradas.

- Controle Adaptativo de Anomalias. Este é um recurso do Kaspersky Endpoint Security for Windows que usa um conjunto de regras para rastrear o comportamento atípico em dispositivos clientes e permite bloquear as ações anômalas.

- Atualizações perfeitas para aplicativos Kaspersky gerenciados instalados em dispositivos Windows e Agente de Rede para Linux. Você pode gerenciar o processo de instalação da atualização aprovando as atualizações que devem ser instaladas e recusando as atualizações que não devem ser instaladas.

- Auditoria de política estendida. Agora você pode visualizar o conteúdo de uma revisão de política e salvá-la em um arquivo. Atualmente, esses recursos estão disponíveis somente para a política do Servidor de Administração e a política do Agente de Rede.

- Cloud Discovery. Este é um novo recurso que permite monitorar o uso de serviços em nuvem em dispositivos gerenciados que executam Windows e bloquear o acesso a serviços em nuvem que você considera indesejados.

- Nova subseção **Alertas** na seção **Monitoramento** do menu principal. Na subseção **Alertas**, você pode ver informações sobre a detecção de ameaças nos dispositivos de endpoints. As ameaças são detectadas pelos aplicativos de segurança da Kaspersky.

- O Kaspersky Security Center Linux agora pode atuar como um componente da solução Kaspersky Managed Detection and Response.
- Suporte para o Kaspersky Security for Virtualization Light Agent.
- Inventário de hardware estendido de dispositivos macOS. O Agente de Rede em um dispositivo macOS envia o endereço MAC e o número de série do dispositivo ao Servidor de Administração.
- Agora você pode receber um relatório sobre a instalação remota ao instalar o software nos dispositivos gerenciados por meio de scripts personalizados.
- Ao executar vários scripts personalizados em um dispositivo gerenciado, você pode definir uma prioridade para cada um deles para definir a ordem de execução. Os scripts serão executados daquele com a prioridade mais alta para aquele com a prioridade mais baixa.
- Para reduzir a quantidade de RAM consumida pelo Kaspersky Endpoint Security for Linux e pelo Agente de Rede para Linux, você pode ativar um modo de trabalho especial para o Agente de Rede para Linux. Nesse modo, o Agente de Rede para Linux requer menos RAM, mas sua funcionalidade é limitada.
- Você pode desinstalar softwares incompatíveis dos dispositivos gerenciado usando a tarefa *Desinstalar aplicativo remotamente*.
- O Relatório de ataques de rede agora inclui endereço MAC e porta do dispositivo de ataque.
- O comprimento máximo da senha para um usuário interno foi aumentado para 256 caracteres.
- Melhorias na experiência do usuário, incluindo:
  - Personalização do menu principal ao adicionar seções do Kaspersky Security Center Web Console aos favoritos para acesso rápido na seção **Favoritos**.
  - Trabalho otimizado com tabelas. A exibição padrão de cada tabela agora contém as colunas usadas com mais frequência. Além disso, agora você pode selecionar todos os itens na página atual ou em toda a tabela, assim como classificar os itens em toda a tabela.
  - Configuração de entrega de relatórios melhorada. Agora você pode especificar até 20 endereços de e-mail para enviar o relatório e o agendamento de entrega do relatório.
- Suporte para uma ampla variedade de sistemas operacionais e novas versões do sistema operacional.
- Um novo guia de dimensionamento foi desenvolvido e publicado na Ajuda on-line.
- Como resultado de uma revisão da interface de usuário, um problema que levava à exibição da seção **Diagnóstico remoto** na janela de propriedades do Servidor de Administração foi resolvido.
- Você pode criar uma tarefa *Executar scripts remotamente* para executar um pacote de instalação em um dispositivo cliente e para instalar um aplicativo remotamente.
- Um usuário pode ser atribuído como proprietário do dispositivo durante ou após a instalação do Agente de Rede em um dispositivo cliente no Linux.
- Você pode configurar uma seleção de dispositivos ou criar uma regra de migração de dispositivos com base no proprietário do dispositivo, na associação do proprietário do dispositivo em um grupo de segurança e na função do proprietário do dispositivo.

- Você pode revogar os direitos de administrador local das contas. Isso fornece uma camada extra de controle de contas de usuário. Por exemplo, você pode revogar os direitos de administrador local após a conclusão de uma atribuição única.

- Você pode alterar a senha da conta local, por exemplo, quando o usuário esquece a senha da conta local ou para executar uma alteração de senha agendada.

- Na subseção **Gerenciamento de certificados do usuário**, você pode especificar quais certificados raiz instalar. Esses certificados podem ser usados, por exemplo, para verificar a autenticidade de sites ou servidores Web.

Kaspersky Security Center 15 Linux

O Kaspersky Security Center 15 Linux inclui vários novos recursos e aprimoramentos:

- A sondagem do controlador de domínio permite sondar um controlador de domínio do Microsoft Active Directory e um controlador de domínio Samba. É possível usar o Servidor de Administração ou um ponto de distribuição para sondar o Microsoft Active Directory. É possível sondar um controlador de domínio Samba somente usando um ponto de distribuição baseado em Linux. Ao fazer a sondagem de um controlador de domínio, o Servidor de Administração ou um ponto de distribuição recupera as informações sobre a estrutura do domínio, contas de usuário, grupos de segurança e nomes DNS dos dispositivos incluídos no domínio.

- O Kaspersky Security Center Linux agora oferece suporte ao trabalho com os seguintes DBMSs:

  - PostgreSQL 15.x

  - Postgres Pro 15.x

- Caso use PostgreSQL ou Postgres Pro como um DBMS, o Kaspersky Security Center Linux é compatível com até 50.000 dispositivos gerenciados.

- Migração do Kaspersky Security Center Windows para o Kaspersky Security Center Linux. É possível executar um assistente para migrar objetos do Kaspersky Security Center, incluindo tarefas, políticas e estrutura do grupo de administração. Depois disso, é possível mover os dispositivos gerenciados importados para serem gerenciados pelo Kaspersky Security Center Linux.

- Agora, o Kaspersky Security Center Linux oferece suporte operacional aos seguintes aplicativos da Kaspersky:

  - Kaspersky Security for Virtualization Light Agent

  - Kaspersky Embedded Systems Security for Windows

  - Kaspersky Embedded Systems Security for Linux

  - Kaspersky Industrial CyberSecurity for Nodes

  - Kaspersky Industrial CyberSecurity for Networks

  - Kaspersky Endpoint Security for Mac

  - Kaspersky Endpoint Agent

  - Kaspersky Security for Virtualization Light Agent

- Diagnóstico remoto de dispositivos gerenciados baseados em Windows e Linux.

- Componente de Controle de Aplicativos aprimorado. Agora, é possível criar uma categoria de aplicativos de acordo com a lista de arquivos executáveis de uma pasta selecionada ou de acordo com uma categoria de aplicativos da Kaspersky. Em seguida, é possível especificar se deseja permitir ou bloquear os aplicativos da categoria criada em sua organização.

- Exportação e importação de seleções de eventos. É possível exportar uma seleção de evento definida pelo usuário e suas configurações para um arquivo KLO e, em seguida, importar a seleção de eventos salva no Kaspersky Security Center Windows ou o Kaspersky Security Center Linux.

- No Relatório de ameaças, agora é possível abrir uma cadeia de desenvolvimento de ameaças ao clicar no link **Exibir alerta**.

- Agora, o Kaspersky Security Center Linux é compatível com a tecnologia de cluster. Caso um grupo de administração contenha clusters ou matrizes de servidor, a página **Dispositivos gerenciados** exibe duas guias: uma para dispositivos individuais e outra para clusters e matrizes de servidor. Depois que os dispositivos gerenciados são detectados como nós de cluster, o cluster é adicionado como um objeto individual à guia **Grupamentos e matrizes de servidores**. Os nós de cluster são listados na guia **Dispositivos**, juntamente com outros dispositivos gerenciados.

- O suporte do Kaspersky Security Center Linux para algumas plataformas foi encerrado porque essas plataformas não são mais compatíveis com seus fornecedores.

Kaspersky Security Center 14.2 Linux

O Kaspersky Security Center 14.2 Linux inclui vários novos recursos e aprimoramentos:

- Agora, em uma hierarquia do servidor de administração, um Servidor de Administração baseado em Linux pode atuar como um Servidor principal pode gerenciar Servidores baseados em Linux ou Windows atuando como um servidor secundário.

- Agora, o Kaspersky Security Center Linux é compatível com Kaspersky Security Network (KSN), serviço de proxy da KSN e Kaspersky Private Security Network (KPSN).

- Agora, o Kaspersky Security Center Linux é compatível com o Kaspersky Endpoint Security for Windows como um aplicativo gerenciado.

  A instalação remota do Agente de Rede para Windows em dispositivos clientes só é possível usando ferramentas do sistema operacional mediante pontos de distribuição baseados em Windows.

- Agora os dados nos dispositivos gerenciados baseados em Windows podem ser criptografados para reduzir o risco de vazamento não intencional de dados confidenciais e corporativos caso o computador portátil ou disco rígido seja roubado ou perdido. Esse recurso é implementado mediante Kaspersky Endpoint Security for Windows.

- O Kaspersky Security Center Linux permite baixar e atualizar ambos os pacotes de distribuição de aplicativos da Kaspersky e plug-ins da Web de gerenciamento diretamente na interface do usuário do Kaspersky Security Center Linux.

- Por padrão, as informações sobre os aplicativos instalados nos dispositivos gerenciados e baseados em Linux e Windows são enviadas para o Servidor de Administração.

- O acesso aos servidores Kaspersky agora é verificado automaticamente. Se não for possível acessar os servidores por meio do DNS do sistema, o aplicativo usará o DNS público.
- Os dados confidenciais que são transferidos entre o Servidor de Administração principal, os Servidores de Administração secundários e os Agentes de Rede agora serão protegidos com o algoritmo de criptografia AES.
- Direitos do usuário em um Servidor de Administração virtual estão disponíveis para configuração a qualquer momento, seja qual for o Servidor de Administração principal. Além disso, você pode atribuir aos usuários do Servidor principal os direitos de gerenciar um Servidor virtual.
- O Kaspersky Security Center Linux agora oferece suporte ao trabalho com os seguintes DBMSs:
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (todas as edições)
  - Postgres Pro 14.x (todas as edições)
- É possível usar o Kaspersky Security Center Web Console para exportar políticas e tarefas para um arquivo e, em seguida, importar as políticas e as tarefas para o Kaspersky Security Center Windows ou Kaspersky Security Center Linux.
- A opção **Não usar o servidor proxy** foi removida das seguintes tarefas:
  - *Baixar atualizações no repositório do Servidor de Administração*
  - *Baixar atualizações para os repositórios de pontos de distribuição*

Kaspersky Security Center 14 Linux

O Kaspersky Security Center Linux inclui diversos recursos novos e aprimoramentos:

- Além da tarefa *Baixar atualizações no repositório do Servidor de Administração*, os bancos de dados antivírus para aplicativos de segurança da Kaspersky agora podem ser baixados por meio da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.
- Bancos de dados de antivírus e módulos de aplicativos nos dispositivos gerenciados podem ser propagados e atualizados por meio do Servidor de Administração ou dos pontos de distribuição. É possível escolher um esquema de atualização ideal para sua organização, reduzir a carga no Servidor de Administração e otimizar o tráfego de dados na rede corporativa.
- O Kaspersky Security Center Linux baixa dos servidores de atualização da Kaspersky apenas as atualizações solicitadas pelos aplicativos de segurança da Kaspersky. Isso reduz o tamanho dos dados baixados.
- Agora é possível usar o recurso de arquivos diff para baixar bancos de dados de antivírus e módulos de software. Um arquivo diff descreve as diferenças entre duas versões de um arquivo de banco de dados ou módulo de software. O uso de arquivos diff poupa tráfego na rede da empresa porque os arquivos diff ocupam menos espaço do que arquivos completos de bancos de dados e módulos de software.

- A tarefa *Verificação de atualizações* foi adicionada. Ao usar essa tarefa, é possível verificar automaticamente as atualizações baixadas quanto à operacionalidade e erros antes de instalar as atualizações nos dispositivos gerenciados.

- Agora, o Kaspersky Security Center Linux é compatível com o Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 como um aplicativo gerenciado.

Problemas corrigidos

A tabela abaixo lista todos os problemas encontrados nas versões anteriores do Kaspersky Security Center Linux e corrigidos na versão atual.

Lista de problemas corrigidos no Kaspersky Security Center Linux 17

Versão do Kaspersky Security Center Linux em que o problema apareceu pela primeira vez	ID do problema	Descrição do problema
16.2	10575601	Corrigido o problema que impedia a exibição da lista de grupos na lista suspensa quando a configuração **O dispositivo está localizado em um subgrupo do grupo de Domínios** estava ativada.
16.3	10519188	Corrigido um problema em que a execução de vacuum (`VACUUM`) em tabelas temporárias deixava o Servidor de Administração mais lento.
16.3	10530831	Corrigido o problema em que as alterações na seção **Dispositivos gerenciados** não eram salvas após a alteração da ordem das colunas.
16.3	10698217	Corrigido o problema em que, nas propriedades de um dispositivo gerenciado, ao clicar no link **Logs de instalação remota** na guia **Avançado → Diagnóstico remoto → Logs de eventos**, a janela exibida tinha o título **Registros de rastreamento do dispositivo**.
16.3	10696918	Corrigido o problema em que a janela de pesquisa não abria no Servidor de Administração secundário ao acessar as propriedades de uma categoria na guia **Condições** da seção **Aplicativos de terceiros → Categorias de aplicativos**.
16.3	10720529	Corrigido o problema em que os dados eram exibidos incorretamente na tabela de dispositivos gerenciados ao usar o operador "≠" (diferente) no filtro **Última conexão com o Servidor de Administração**.
16.3	10012561	Corrigido o problema em que, ao verificar um domínio com o SberLDAP, a estrutura do domínio e seus hosts não eram retornados.
16	9496192	Corrigido o problema em que, ao clicar no botão **Selecionar tudo** na tabela **Seleção de eventos** e depois exportar os eventos, apenas os eventos da página atual eram exportados.
16.3	10292104	Corrigido o problema em que, no Kaspersky Security Center Web Console versão 15.1 ou 15.2, após a atualização do plug-in do Kaspersky Endpoint Detection and Response Optimum para a versão 16.3, a seção **Alertas** poderia não exibir alertas.
16.3	10596319	Corrigido o problema em que, na seção **Tags** do formulário **Atribuir etiqueta**, a lista de tags era exibida sem ordenação.
16.3	10127434	Corrigido o problema em que, ao fazer login no Kaspersky Security Center Web Console e acessar a seção **Tarefas** no Servidor de Administração principal, o Servidor de Administração virtual era exibido como o servidor principal na janela de hierarquia.
16.3	10252324	Corrigido o problema em que alguns aplicativos da seleção de eventos gerada pelo componente **Controle de Aplicativos** na política do Kaspersky Endpoint Security não eram adicionados à seção **Categorias de aplicativos**.
16.3	10308380	Corrigido o problema em que, após a criação de uma categoria de aplicativo, não era possível abrir suas propriedades.
16.2	10698205	Corrigido o problema em que a seção **Grupamentos e matrizes de servidores** não era exibida ao selecionar um cluster na seção **Dispositivos gerenciados**, o que impedia mover o cluster para um grupo.
16.3	10373324	Corrigido o problema em que o segundo nó de cluster de um cluster de failover do Kaspersky Security Center Linux não era considerado na avaliação do status do indicador de segurança.
16.3	10563031	Corrigido o problema que causava um erro ao atualizar o cluster de failover do Kaspersky Security Center Linux da versão 16.2 para a 16.3 e da versão 16 para a 16.3. O erro era "Tentativa de alterar o modo KLFOC durante a atualização. Abortando".

16.3	10590796, 10590805	Corrigido o problema em que a atualização do nó secundário do cluster de failover da Kaspersky Security Center resultava nos erros: "Erro fatal: é proibido alterar o modo de gerenciamento KLFOC!" e "Erro fatal: não é possível obter o nome do banco de dados KSC do armazenamento de configurações."
16.3	10570574	Corrigido o problema em que a reinicialização do serviço do Servidor de Administração durante a execução da tarefa **Backup de dados do Servidor de Administração** fazia com que a tarefa fosse reiniciada com o erro "O backup já está em andamento".
16.3	10085767	Corrigido o problema em que o escopo do relatório podia ser exibido incorretamente durante a migração de dados para o Kaspersky Security Center Linux.
16.2	10135898	Corrigido o problema em que a seção **Configurações → Conexão única** não era carregada quando a sessão do usuário durava mais de uma hora.
16.3	10542356	Corrigida a validação incorreta do campo **Endereço de e-mail** ao editar um usuário na seção **Usuários e funções → Usuários e grupos**.
16.3	10534809	Corrigido o problema em que os eventos de um dispositivo gerenciado demoravam muito para carregar. O tempo de carregamento foi reduzido de 20 segundos para 2 segundos.
16.3	10537996	Corrigido o problema em que uma guia do navegador com o Kaspersky Security Center Web Console consumia mais de 1,5 GB de RAM.
15.1	9067495	Corrigido o problema em que o botão **Verificar conexão** ficava disponível ao salvar as configurações de conexão com o SIEM usando o protocolo UDP.

Lista de problemas corrigidos no Kaspersky Security Center Linux 16.3 Atualização 1

Versão do Kaspersky Security Center Linux em que o problema apareceu pela primeira vez	ID do problema	Descrição do problema
16.3	10431901	Corrigido um problema que fazia com que a seção **Conexão única** não aparecesse no menu do Web Console. Por isso, os usuários não conseguiam configurar a autenticação do domínio usando o protocolo Kerberos. A autenticação configurada anteriormente continuou funcionando.

Lista de problemas corrigidos no Kaspersky Security Center Linux 16.3

Versão do Kaspersky Security Center Linux em que o problema apareceu pela primeira vez	ID do problema	Descrição do problema
16.2	9959974	Corrigido um problema que fazia com que a opção **Selecionar tudo** aparecesse na guia **Eventos** da janela de propriedades do dispositivo. Se selecionada, essa opção poderia excluir todos os eventos do banco de dados do Servidor de Administração.
16.2	9392997	Corrigido um problema que fazia com que uma mensagem de erro fosse registrada após uma sondagem bem-sucedida de um controlador de domínio ALD Pro ou FreeIPA.
16.2	9504495	Foi corrigido um problema que podia causar a atribuição incorreta de um usuário se o proprietário do dispositivo fosse atribuído por meio dos parâmetros do pacote de instalação do Agente de Rede.
16.1	9316206	Foi corrigido um problema em que os botões de controle podiam desaparecer da guia **Autenticação de dois fatores** ao atualizar o navegador depois de abrir a guia.
16.1	7555541	Foi corrigido um problema que causava falha ao fazer login no Web Console quando a opção **Definir como uma senha única (o usuário deve alterar a senha após o primeiro login)** era ativada ao criar a tarefa *Alterar senha da conta (somente Linux)*.
15.4	7555788	Foi corrigido um problema em que a tarefa *Alterar senha da conta* podia não funcionar corretamente se o SELinux estivesse ativado no dispositivo do usuário.

16.2	9603496	Foi corrigido um problema em que era necessário instalar o Agente de Rede no dispositivo do Servidor de Administração para obter informações de diagnóstico sobre esse dispositivo.
16.2	9704308	Foi corrigido um problema em que abrir a seção **Hierarquia de grupos** durante o carregamento da página em ambientes com um grande número de grupos de administração podia resultar em um erro `429 Too Many Requests`, interromper a conexão com o Servidor de Administração e redirecionar os usuários para a página de login.
16.2	9989231	Foi corrigido um problema em que a filtragem de dispositivos pelo endereço IP de conexão podia retornar resultados incorretos.
16.2	9990025	Foi corrigido um problema em que as configurações de exibição de tabela nas seções **Políticas** e **Tarefas** não eram preservadas ao navegar entre as páginas.
15.3	9632613	Foi corrigido um problema em que o login de usuários do domínio no Web Console podia sofrer atrasos significativos quando os controladores de domínio LDAP estavam indisponíveis ou não continham a conta do usuário.
15.1	9829027	Foi corrigido um problema em que a configuração do filtro **Status da atualização** no relatório **Relatório de uso dos bancos de dados de antivírus** podia resultar em um erro.
15.1	9844707	O Kaspersky Security Center e o FCM (Firebase Cloud Messaging) interagiam diretamente, mesmo quando um servidor proxy estava configurado.

Lista de problemas corrigidos no Kaspersky Security Center Linux 16.2

Versão do Kaspersky Security Center Linux em que o problema apareceu pela primeira vez	ID do problema	Descrição do problema
15.1	10071566	Corrigido um problema em que as alterações feitas em uma programação de tarefas não eram propagadas para dispositivos gerenciados se a programação usasse a configuração "Por dias da semana".
15.4	9067754	Foi corrigido um problema que fazia com que novos eventos fossem exibidos de forma incorreta em uma política criada anteriormente após a atualização do plug-in do Kaspersky Mobile Devices Protection and Management.
16	9329729	Foi corrigido um problema em que um erro aparecia no Log de eventos da Kaspersky após a atualização do Kaspersky Security Center Linux da versão 16 para a versão 16.1 se a autenticação de dois fatores tivesse sido configurada para determinados usuários antes da atualização.
16.1	9256000	Foi corrigido um problema em que as informações sobre os componentes do aplicativo gerenciado não estavam disponíveis se o Agente de Rede estivesse instalado no Microsoft Windows XP.
16.1	9251629	Foi corrigido um problema em que alguns cabeçalhos de resposta HTTP necessários não eram adicionados ao fazer login no Kaspersky Security Center Web Console.

Sobre os certificados do Kaspersky Security Center Linux

A seção contém informações sobre a finalidade do Kaspersky Security Center Linux, seus respectivos recursos e componentes principais e maneiras de comprá-lo.

O Kaspersky Security Center Linux (também conhecido como Kaspersky Security Center) foi desenvolvido para implementar e gerenciar a proteção de dispositivos clientes com o uso do Servidor de Administração baseado em Linux.

O Kaspersky Security Center Linux permite instalar aplicativos de segurança da Kaspersky em dispositivos em uma rede corporativa, executar remotamente as tarefas de verificação e atualização, além de gerenciar as políticas de segurança dos aplicativos gerenciados. É possível utilizar um painel detalhado que fornece uma visão instantânea do status de dispositivos corporativos, relatórios detalhados e configurações granulares nas políticas de proteção.

Comparado ao Kaspersky Security Center, que possui o Servidor de Administração baseado no Windows®, o Kaspersky Security Center Linux possui um conjunto de recursos diferente.

O Kaspersky Security Center Linux é um aplicativo que se destina aos administradores de redes corporativas e funcionários responsáveis pela proteção de dispositivos em diversos tipos de organizações.

Com o uso do Kaspersky Security Center, você pode fazer o seguinte:

- Crie uma hierarquia de Servidores de Administração para gerenciar a rede corporativa, assim como redes em escritórios remotos e organizações cliente.

  A *organização cliente* é uma organização, cuja proteção antivírus é garantida pelo provedor de serviços.

- Crie uma hierarquia de grupos de administração para gerenciar uma seleção de dispositivos cliente como um todo.

- Gerenciar um sistema de proteção antivírus criado com base nos aplicativos Kaspersky.

- Execute a instalação remota de aplicativos pela Kaspersky e outros fornecedores de software.

- Realizar implementações centralizadas de chaves de licença para aplicativos Kaspersky em dispositivos cliente, monitorar seu uso e renovar licenças.

- Receber estatísticas e relatórios sobre a operação dos aplicativos e dispositivos.

- Receber notificações sobre eventos críticos durante a operação dos aplicativos Kaspersky.

- Gerenciar a criptografia de informações armazenadas em discos rígidos de dispositivos baseados em Windows e unidades removíveis.

- Gerenciar o acesso dos usuários a dados criptografados em dispositivos baseados no Windows.

- Realizar inventário de hardware conectado à rede corporativa.

- Gerencie centralizadamente os arquivos colocados em Quarentena ou em Backup pelos aplicativos de segurança, assim como gerencie os arquivos para os quais o processamento pelos aplicativos antivírus foi adiado.

É possível comprar o Kaspersky Security Center Linux pela Kaspersky (por exemplo, no site https://www.kaspersky.com) ou por meio de empresas parceiras.

Caso o Kaspersky Security Center Linux seja adquirido por meio da Kaspersky, será possível copiar o aplicativo de nosso site. As informações necessárias para ativação do aplicativo são enviadas a você por e-mail após o pagamento.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Kit de distribuição

No site da Kaspersky, você pode baixar todos os pacotes de distribuição necessários do aplicativo.

O kit de distribuição da Kaspersky Security Center Linux inclui os seguintes arquivos:

Servidor de Administração da Kaspersky Security Center Linux:

- Servidor de Administração a ser instalado em um dispositivo executando o sistema operacional baseado em Debian:

  ksc64_17.0.0-<build>_amd64.deb

- Servidor de Administração a ser instalado em um dispositivo executando o sistema operacional Red Hat Enterprise baseado em Linux:

  ksc64-17.0.0-<build>.x86_64.rpm

Kaspersky Security Center Web Console:

- Web Console a ser instalado em um dispositivo executando o sistema operacional baseado em Debian:

  ksc-web-console-17.0.<build>.x86_64.deb

- Web Console a ser instalado em um dispositivo executando o sistema operacional Red Hat Enterprise baseado em Linux:

  ksc-web-console-17.0.<build>.x86_64.rpm

Script de instalação do Kaspersky Security Center:

- ksc_fast_install.tar.gz

Agente de Rede para Windows:

- O Agente de Rede a ser instalado em um dispositivo com arquitetura Arm:

  klnagent_winarm64-17.0.0.<build>-win_<localization>.zip

- Arquivos para a instalação remota do Agente de Rede em um dispositivo com arquitetura x86-32 ou x64:

  ksc_17_17.0.0.<build>_NetAgent_<localization>.zip

- Arquivos para a instalação remota do Agente de Rede em um dispositivo com arquitetura Arm:

  ksc_17_17.0.0.<build>_NetAgent_arm64_<localization>.zip

- Arquivos para instalação remota via Kaspersky Security Center em um dispositivo com arquitetura Arm:

  ri_utils_arm64.zip

- Arquivos para instalação remota via Kaspersky Security Center em um dispositivo com arquitetura x86-32 ou x64:

  ri_utils_win32.zip

Agente de Rede para Linux:

- Agente de Rede a ser instalado em um dispositivo executando o sistema operacional baseado em Debian:

  klnagent64_17.0.0-<build>_<architecture>.deb

- Agente de Rede a ser instalado em um dispositivo executando o sistema operacional Red Hat Enterprise baseado em Linux:

  klnagent64-17.0.0-<build>_<architecture>.rpm

- Arquivos para a instalação remota do Agente de Rede em um dispositivo executando o sistema operacional baseado em Debian:

  klnagent-<architecture>-17.0.0.<build>-deb_<localization>.tar.gz

- Arquivos para a instalação remota do Agente de Rede em um dispositivo executando o sistema operacional Red Hat Enterprise baseado em Linux:

  klnagent-<architecture>-17.0.0.<build>-rpm_<localization>.tar.gz

- Arquivos para a instalação remota do Agente de Rede Elbrus Edition em um dispositivo executando um sistema operacional baseado em Debian ou Red Hat Enterprise Linux:

  klnagent-e2k-17.0.0.<build>-all-<localization>.tar.gz

- Pacote de distribuição único para a instalação remota de Agentes de Rede para Linux:

  klnagent-all-17.0.0.<build>-all_<localization>.tar.gz

  O pacote de distribuição único pode ser útil se você tiver muitos dispositivos cliente com diferentes arquiteturas de CPU e diferentes sistemas operacionais baseados em Linux. As versões necessárias dos Agentes de Rede serão selecionadas automaticamente para instalação posterior nos dispositivos.

- Arquivos para a instalação remota do Agente de Rede em um dispositivo executando um sistema operacional legado baseado em Debian ou Red Hat Enterprise Linux com glibc 2.5:

  klnagent-all-17.0.0.<build>-glibc2.5-all-<localization>.tar.gz

Plug-in da Web do Kaspersky Endpoint Detection and Response Optimum:

- signed_irp.zip

  Você só pode baixar o plug-in da Web por meio do Repositório de pacotes de distribuição de aplicativos para instalação remota.

Se você achar difícil escolher um pacote de instalação para um Agente de Rede para Linux, consulte o artigo: Como escolher o pacote de instalação para o Agente de Rede para Linux.

Requisitos de hardware e software

- Requisitos do Servidor de Administração
- Requisitos do Web Console
- Requisitos do Agente de Rede

Para informações sobre os requisitos de versão do Android e iOS para implementação da proteção e gerenciamento de dispositivos móveis, consulte a Ajuda do Kaspersky Security for Mobile e a Ajuda do Kaspersky Secure Mobility Management.

Requisitos do Servidor de Administração

Este artigo lista as versões de software nas quais o aplicativo foi testado e para as quais seu funcionamento correto é garantido. O aplicativo também pode funcionar com outras versões de software, mas essas configurações não passaram por um ciclo completo de testes e não estão incluídas na lista de versões com suporte garantido.

Requisitos mínimos de hardware:

- CPU com frequência operacional de 2,5 GHz ou superior, 2 núcleos.
- RAM: 6 GB

  Você precisa ativar o arquivo de troca no dispositivo com o Servidor de Administração instalado. O tamanho mínimo do arquivo de troca deve ser 1,5 vez maior que o volume da RAM.
- Espaço disponível em disco: 10 GB necessários para a pasta onde os dados do Servidor de Administração estão armazenados (/var/opt/kaspersky/klnagent_srv).

Para obter mais informações sobre os requisitos de hardware, consulte a seção Requisitos de hardware do SGBD e do Servidor de Administração.

Recomendamos que, após instalar o Servidor de Administração em um dispositivo, você instale o Kaspersky Endpoint Security for Linux nesse dispositivo.
Para a instalação simultânea, é necessário ter no mínimo 300 IOPS, além de acrescentar aos requisitos do Servidor de Administração 1,5 GB de RAM e 15% à CPU.
Para obter os requisitos de hardware do Kaspersky Endpoint Security, consulte a Ajuda do Kaspersky Endpoint Security for Linux.
Para obter informações sobre as configurações de segurança necessárias para trabalhar com o Kaspersky Security Center Linux, consulte a Ajuda do Kaspersky Endpoint Security for Linux.

Os seguintes sistemas operacionais são compatíveis:

Para a comunicação entre processos no sistema operacional, a interface de loopback deve estar disponível.

- Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm) 64 bits
- Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie) 64 bits
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bits
- Ubuntu Server 24.04 LTS (Noble Numbat) 64 bits
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64 bits
- CentOS Stream 9 64 bits
- CentOS Stream 10 64 bits
- Red Hat Enterprise Linux Server 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64 bits
- Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64 bits
- Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64 bits
- Red Hat Enterprise Linux Server 10.0, 10.1 64 bits
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7 64 bits
- SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7 64 bits
- Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.6) de 64 bits
- Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.7) de 64 bits
- Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.8) 64 bits
- Astra Linux Special Edition RUSB.10015-16 (versão 1) (atualização operacional 1.6) de 64 bits
- Astra Linux Special Edition RUSB.10015-17 (atualização operacional 1.7.3) 64 bits
- Astra Linux Special Edition RUSB.10015-03 (atualização operacional 7.6) de 64 bits
- Astra Linux Special Edition RUSB.10015-37 (atualização operacional 7.7) 64 bits
- Astra Linux Common Edition (atualização operacional 2.12) de 64 bits
- ALT Server 11 64 bits
- ALT SP Server 10 64 bits
- ALT SP Workstation 10 64 bits
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64 bits

- Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9 64 bits
- Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64 bits
- Platform V SberLinux OS Server (SLO) 8.10.1 64 bits
- Platform V SberLinux OS Server (SLO) 9.5.1 64 bits
- Platform V SberLinux OS Server (SLO) 9.6 64 bits
- Platform V SberLinux OS Server (SLO) 9.7 64 bits
- RED OS 7.3 Server 64 bits
- RED OS 7.3 Certified Edition 64 bits
- RED OS 8 64 bits
- ROSA COBALT 7.9 64 bits
- M OS (Moscow Electronic School) 12 Server 64 bits
- Mostech Server 64 bits
- MosOS 15.5 Arbat 64 bits
- MosOS 15.6 64 bits

Recomendamos que você use o sistema de arquivos EXT4 com as respectivas configurações padrão.

Os seguintes servidores de banco de dados são compatíveis (podem ser instalados em um dispositivo diferente):

- MySQL Standard Edition 8.0 (versão 8.0.20 e mais recentes) 32 bits/64 bits
- MySQL Enterprise Edition 8.0 (versão 8.0.20 e mais recentes) 32 bits/64 bits
- MySQL Standard Edition 8.4 32 bits/64 bits
- MySQL Enterprise Edition 8.4 32 bits/64 bits
- MariaDB 10.11 (compilação 10.11.10 e posterior) 32/64 bits
- MariaDB 11.4 64 bits
- MariaDB 11.8 64 bits
- MariaDB 12.3 64 bits
- MariaDB Galera Cluster 4 32 bits/64 bits
- PostgreSQL 15.x 64 bit
- PostgreSQL 15.x 64 bits (cluster Corosync/Pacemaker)

- PostgreSQL 16.x 64 bits
- PostgreSQL 17 64 bits
- PostgreSQL 18 64 bits
- Postgres Pro 15.x 64 bits (todas as edições)
- Postgres Pro 15.x 64 bits (cluster Corosync/Pacemaker)
- Postgres Pro 16.x 64 bits (todas as edições)
- Postgres Pro 16.x Enterprise 64 bits (cluster com alta disponibilidade integrada)
- Postgres Pro 17.x 64 bits (todas as edições)
- Postgres Pro 17.x Enterprise 64 bits (cluster com alta disponibilidade integrada)
- Postgres Pro 18.x 64 bits (todas as edições)
- Postgres Pro 18.x Enterprise 64 bits (cluster com alta disponibilidade integrada)
- Platform V Pangolin 6.5.1 64 bits
- Plataform V Pangolin 6.5.1 64 bits (cluster de alta disponibilidade integrado)
- Plataforma V Pangolin 7.2.0 64 bits
- Plataforma V Pangolin 7.2.0 64 bits (cluster de alta disponibilidade integrado)
- Jatoba 4 64 bits
- Jatoba 5 64 bits
- Tantor SE 1C 64 bits

Clusters PostgreSQL altamente disponíveis são compatíveis. Consulte o seguinte artigo para obter informações: Preparar um cluster DBMS de alta disponibilidade para trabalhar com a Kaspersky Security Center Linux.

Para obter informações sobre as plataformas de virtualização compatíveis, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

Requisitos do Web Console

Este artigo lista as versões de software nas quais o aplicativo foi testado e para as quais seu funcionamento correto é garantido. O aplicativo também pode funcionar com outras versões de software, mas essas configurações não passaram por um ciclo completo de testes e não estão incluídas na lista de versões com suporte garantido.

Kaspersky Security Center Web Console Server

Requisitos mínimos de hardware:

- CPU: 2 núcleos, frequência operacional de 2,5 GHz.
- RAM: 4 GB.
- Espaço disponível em disco: 40 GB são necessários para a pasta onde os dados do Web Console estão armazenados (/var/opt/kaspersky).

Recomendamos que, depois de instalar o Kaspersky Security Center Web Console em um dispositivo, você instale o Kaspersky Endpoint Security for Linux nesse dispositivo. Para obter os requisitos de hardware do Kaspersky Endpoint Security, consulte a Ajuda do Kaspersky Endpoint Security for Linux.

Um dos seguintes sistemas operacionais (**somente versões de 64 bits**):

> Para a comunicação entre processos no sistema operacional, a interface de loopback deve estar disponível.

- Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm)
- Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- Ubuntu Server 24.04 LTS (Noble Numbat)
- Ubuntu Server 26.04 LTS (Resolute Raccoon)
- CentOS Stream 9
- CentOS Stream 10
- Red Hat Enterprise Linux Server 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10
- Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6
- Red Hat Enterprise Linux Server 10.0, 10.1
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7
- SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7
- Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.6)
- Astra Linux Special Edition RUSB.10015-16 (versão 1) (atualização operacional 1.6)
- Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.7)
- Astra Linux Special Edition RUSB.10015-17 (atualização operacional 1.7.3)

- Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.8)
- Astra Linux Special Edition RUSB.10015-03 (atualização 7.6)
- Astra Linux Special Edition RUSB.10015-37 (atualização operacional 7.7)
- Astra Linux Common Edition (atualização operacional 2.12)
- ALT Server 11
- ALT SP Server 10
- ALT SP Workstation 10
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9
- Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6
- Servidor do sistema operacional Platform V SberLinux (SLO) 8.10.1
- Servidor do sistema operacional Platform V SberLinux (SLO) 9.5.1
- Platform V SberLinux OS Server (SLO) 9.6
- Platform V SberLinux OS Server (SLO) 9.7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- RED OS 8
- ROSA COBALT 7.9
- M OS (Moscow Electronic School) 12 Server
- Mostech Server
- MosOS 15.5 Arbat
- MosOS 15.6

Para obter informações sobre as plataformas de virtualização compatíveis, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

Dispositivos cliente

Em um dispositivo cliente, o uso do Kaspersky Security Center Web Console requer apenas um navegador.

A resolução mínima da tela é de 1366x768 pixels.

Os requisitos de hardware e software para o dispositivo são idênticos aos requisitos do navegador utilizado com o Kaspersky Security Center Web Console.

Navegadores:

- Google Chrome 149.0.7827.115 ou posterior
- Microsoft Edge 149.0.4022.62 ou posterior
- Safari 18.6 (20621.3.11.11.3) no macOS
- Yandex Browser 26.4.4.799 ou posterior
- Mozilla Firefox Extended Support Release 140.11.0 ou posterior

Requisitos do Agente de Rede

Este artigo lista as versões de software nas quais o aplicativo foi testado e para as quais seu funcionamento correto é garantido. O aplicativo também pode funcionar com outras versões de software, mas essas configurações não passaram por um ciclo completo de testes e não estão incluídas na lista de versões com suporte garantido.

Requisitos mínimos de hardware:

- CPU com frequência operacional de 1 GHz ou superior. Para um sistema operacional de 64 bits, a frequência mínima de CPU é de 1.4 GHz.
- RAM: 512 MB.
- Espaço livre em disco: 1 GB.

Requisito de software para dispositivos baseados em Linux: o intérprete de linguagem Perl versão 5.10 ou superior deve estar instalado.

Agente de Rede. Plataformas compatíveis

Sistemas operacionais. Estações de trabalho Microsoft Windows	Microsoft Windows Embedded POSReady 2009 com o Service Pack de 32 bits mais recente Microsoft Windows Embedded 7 Standard with Service Pack 1 32 bits/64 bits Microsoft Windows Embedded 8.1 Industry Pro 32 bits/64 bits Microsoft Windows 10 Enterprise 2015 LTSB 32 bits/64 bits Microsoft Windows 10 Enterprise 2016 LTSB 32 bits/64 bits Microsoft Windows 10 Enterprise 2019 LTSC 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1507, 1607, 1703, 1709, 1803, 1809, 1909 32 bits/64 bits Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32/64 bits Microsoft Windows 10 TH1 (julho de 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bits Microsoft Windows 10 TH2 (novembro de 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bits Microsoft Windows 10 RS1 (agosto de 2016) Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bits Microsoft Windows 10 RS2 (abril de 2017) Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bits Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 10 RS4 (atualização de abril de 2018, 17134) Home/Pro/Pro for Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 10 RS5 (outubro de 2018) Home/Pro/Pro for Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 10 RS6 (maio de 2019) Home/Pro/Pro Home/Pro/Pro para Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 10 20H1 (atualização de maio de 2020) Home/Pro/Pro for Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 10 20H2 (atualização de outubro de 2020) Home/Pro/Pro for Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 10 21H1 (Atualização de maio de 2021) Home/Pro/Pro for Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 10 21H2 (atualização de outubro de 2021) Home/Pro/Pro for Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 10 22H2 (atualização de outubro de 2023) Home/Pro/Pro for Workstations/Enterprise/Education 32 bits/64 bits Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64 bits Microsoft Windows 11 IoT Enterprise version 25H2 64 bits Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 bits Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 bits Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 bits Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 bits Microsoft Windows 11 26H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 bits Microsoft Windows 8.1 Pro/Enterprise 32 bits/64 bits Microsoft Windows 8 Pro/Enterprise 32 bits/64 bits Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium com Service Pack 1 e posterior 32 bits/64 bits Microsoft Windows XP Professional com Service Pack 2, 32 bits/64 bits (compatível apenas com o Agente de Rede versão 10.5.1781) Microsoft Windows XP Professional com Service Pack 3 e posterior, 32 bits (compatível com o Agente de Rede versão 14.0.0.20023, requer o Security Update for Windows XP KB2868626) Microsoft Windows XP Professional for Embedded Systems com Service Pack 3 de 32 bits (compatível com o Agente de Rede versão 14.0.0.20023)

Sistemas operacionais. Servidores Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64 bits Microsoft Windows Server 2003 SP1 32 bits/64 bits (suportado somente pelo Agente de Rede versão 10.5.1781, que você pode solicitar através do Suporte Técnico) Microsoft Windows Server 2003 SP2 Standard/Enterprise 32 bits/64 bits (compatível apenas com a versão 10.5.1781 do Agente de Rede) Microsoft Windows Server 2003 R2 Standard/Enterprise with SP2 32 bits/64 bits (compatível apenas com a versão 10.5.1781 do Agente de Rede) Microsoft Windows Server 2008 Standard/Enterprise com Service Pack 2 32 bits/64 bits Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard com Service Pack 1 e posterior 64 bits Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64 bits Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64 bits Microsoft Windows Server 2016 Datacenter/Standard/Server Core (opção de instalação) (LTSB) 64 bits Microsoft Windows Server 2019 Standard/Datacenter/Núcleo de 64 bits Microsoft Windows Server 2019 RS5 Essentials/Standard 64 bits Microsoft Windows Server 2022 Standard/Datacenter/Núcleo de 64 bits Microsoft Windows Server 2025 Standard/Datacenter/Núcleo de 64 bits Microsoft Windows Server 2022 21H2 Standard/Datacenter de 64 bits Microsoft Windows Small Business Server 2011 Standard 64 bits Microsoft Windows Small Business Server 2011 Essentials 64 bits

Sistemas operacionais. Linux	Debian GNU/Linux 10.0, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12 (Buster) 32 bits/64 bits Debian GNU/Linux 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11 (Bullseye) 32 bits/64 bits Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm) 32 bits/64 bits Debian GNU/Linux 12.10, 12.11, 12.14 (Bookworm) ARM 64 bits Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie) 64 bits Ubuntu Server 10.04 LTS (Lucid Lynx) 32 bits/64 bits Ubuntu Server 16.04 LTS (Xenial Xerus) 32 bits/64 bits Ubuntu Server 18.04 LTS (Bionic Beaver) 64 bits Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bits Ubuntu Server 22.04 LTS ARM 64-bit Ubuntu Server 24.04 LTS (Noble Numbat) 64 bits Ubuntu Server 26.04 LTS (Resolute Raccoon) 64 bits Ubuntu Server 26.04 LTS ARM 64 bits Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32 bits/64 bits Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 bits/64 bits CentOS 5.2 de 64 bits (compatível apenas com o Agente de Rede para Linux Legacy, que você pode baixar usando a interface do Web Console ou no site da Kaspersky) CentOS 5.4 de 64 bits (compatível apenas com o Agente de Rede para Linux Legacy, que você pode baixar usando a interface do Web Console ou no site da Kaspersky) CentOS 6.4 de 64 bits (compatível apenas com o Agente de Rede para Linux Legacy, que você pode baixar usando a interface do Web Console ou no site da Kaspersky) CentOS 6.6 de 32 bits/64 bits (compatível apenas com o Agente de Rede para Linux Legacy, que você pode baixar usando a interface do Web Console ou no site da Kaspersky) CentOS 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 de 64 bits CentOS Stream 8 de 64 bits CentOS Stream 9 64 bits CentOS Stream 9 ARM 64 bits CentOS Stream 10 64 bits Red Hat Enterprise Linux Server 6.5, 6.6, 6.7, 6.8, 6.9, 6.10 de 32 bits/64 bits Red Hat Enterprise Linux Server 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64 bits Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64 bits Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64 bits Red Hat Enterprise Linux Server 10.0, 10.1 64 bits SUSE Linux Enterprise Server 12.5, 12.6, 12.7 64 bits SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7 64 bits SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7 ARM 64 bits openSUSE Leap 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6 64 bits EulerOS 2.0 SP10 64 bits EulerOS 2.0 SP10 ARM 64 bits Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.4) 32 bits Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.4) 64 bits (compatível apenas com o Agente de Rede para Linux Legacy, que você pode baixar usando a interface do Web Console ou no site da Kaspersky) Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.5) de 64 bits Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.6) de 64 bits Astra Linux Special Edition RUSB.10015-16 (versão 1) (atualização operacional 1.6) de 64 bits Astra Linux Special Edition RUSB.10015-16 (versão 2) (atualização operacional 8.1) E2K Astra Linux Special Edition RUSB.10015-17 (atualização operacional 1.7.3) 64 bits Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.7) de 64 bits Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.8) 64 bits Astra Linux Special Edition RUSB.10015-03 (atualização operacional 7.6) de 64 bits Astra Linux Special Edition RUSB.10015-37 (atualização operacional 7.7) 64 bits Astra Linux Special Edition RUSB.10152-02 (atualização operacional 4.7) ARM de 64 bits Astra Linux Special Edition RUSB.10265-01 (atualização operacional 8.1) E2K Astra Linux Common Edition (atualização operacional 2.12) de 64 bits ALT Workstation 11.2 ARM 64 bits

ALT Workstation 11 64 bits
ALT Server 11.1 ARM 64 bits
ALT Server 11 64 bits
ALT Education 11 64 bits
ALT Workstation 10.1 64 bits
ALT Server 10.1 64 bits
ALT Education 10.1 64 bits
ALT SP Server 10 32 bits/64 bits
ALT SP Server 10 ARM 64 bits
ALT SP Server 10 E2K
ALT SP Workstation 10 32 bits/64 bits
ALT SP Workstation 10 ARM 64 bits
ALT SP Workstation 10 E2K
Servidor ALT 8 SP (LKNV.11100-01) 32/64 bits
Servidor ALT 8 SP (LKNV.11100-02) 32/64 bits
ALT 8 SP Server (LKNV.11100-03) 32 bits/64 bits
ALT SP Server 8 E2K
ALT 8 SP Workstation (LKNV.11100-01) 32 bits/64 bits
ALT 8 SP Workstation (LKNV.11100-02) 32 bits/64 bits
ALT 8 SP Workstation (LKNV.11100-03) 32 bits/64 bits
ALT 8 SP Workstation E2K
Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64 bits
Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64 bits
Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7 64 bits
Linux Mint 21.1, 21.2, 21.3 64 bits
Linux Mint 22.0, 22.1, 22.2 64 bits
AlterOS 7.5 64 bits
AlterOS 2025 64 bits
SberOS 3.4.0 64 bits
SberOS 3.5.0 64 bits
SberOS 3.6.1 64 bits
Platform V SberLinux OS Server (SLO) 8.10.1 64 bits
Plataforma V SberLinux OS Server (SLO) 9.1 64 bits
Platform V SberLinux OS Server (SLO) 9.5.1 64 bits
Platform V SberLinux OS Server (SLO) 9.6 64 bits
Platform V SberLinux OS Server (SLO) 9.7 64 bits
RED OS 7.3 Server 64 bits
RED OS 7.3 Certified Edition 64 bits
RED OS 8 64 bits
RED OS 8 ARM 64 bits
ROSA Enterprise Linux Server 7.9 de 64 bits
ROSA Enterprise Linux Desktop 7.9 64 bits
ROSA COBALT 7.9 64 bits
ROSA CHROME 12 64 bits
AlmaLinux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64 bits
AlmaLinux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64 bits
Rocky Linux 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64 bits
Rocky Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64 bits
Atlant, compilação Alcyone, versão 2022.02 64 bits
MSVSPHERE 9.2 SERVER de 64 bits
MSVSPHERE 9.2 ARM 64 bits
MSVSPHERE 9.4 SERVER 64 bits
MSVSPHERE 9.4 ARM 64 bits
MSVSPHERE 9.5 SERVER de 64 bits
MSVSPHERE 9.5 ARM 64 bits
SynthesisM Server 8.6 de 64 bits

	Cliente SynthesisM 8.6 64 bits OSnova 2.9, 2.14 64 bits OSnova 3.0.5, 3.1 64 bits Kylin 10 64 bits EMIAS 1.0 64 bits Amazon Linux 2 64 bits Amazon Linux 2023 64 bits MosOS 15.5 Arbat 64 bits MosOS 15.6 64 bits OS MES 12 para escolas de Moscou para desktops e laptops (com telemetria e suporte do DIT) 64 bits. OS MES 12 para escolas de Moscou para painéis interativos (com telemetria e suporte do DIT) 64 bits. M OS (Moscow Electronic School) 12 Server 64 bits Mostech 64 bits Mostech Server 64 bits Fedora Linux Server 41 64 bits Fedora Linux Workstation 41 64 bits Elbrus 9.3.6 E2K
Sistemas operacionais macOS	Para obter a lista de sistemas operacionais compatíveis, consulte a Ajuda do Kaspersky Endpoint Security for Mac.
Plataformas de virtualização	Para obter informações sobre as plataformas de virtualização compatíveis, consulte a Ajuda on-line do Kaspersky Security for Virtualization Light Agent.

Em versões do Windows anteriores ao Microsoft Windows Server 2008 R2 (versões de servidor) e ao Microsoft Windows 7 (versões de desktop), o Agente de Rede não é compatível com a seguinte funcionalidade:

- Retradução de atualizações (usada por pontos de distribuição)
- Proxy KSN (usado por pontos de distribuição)
- Tarefa de verificação de vulnerabilidades

Em dispositivos com Microsoft Windows 10 versão RS4 ou RS5, o Kaspersky Security Center pode não conseguir detectar algumas vulnerabilidades em pastas onde a diferenciação entre maiúsculas e minúsculas está ativada.

Antes de instalar o Agente de Rede nos dispositivos que executam o Windows 7, Windows Server 2008, Windows Server 2008 R2 ou Windows MultiPoint Server 2011, certifique-se de ter instalado a atualização de segurança KB3063858 para SO Windows: Atualização de segurança para Windows 7 (KB3063858), Atualização de segurança para Windows 7 para sistemas baseados em x64 (KB3063858), Atualização de segurança para Windows Server 2008 (KB3063858), Atualização de segurança para Windows Server 2008 x64 Edition (KB3063858), Atualização de segurança para Windows Server 2008 R2 x64 Edition (KB3063858).

No Microsoft Windows XP, o Agente de Rede poderá não executar algumas operações corretamente.

É possível instalar ou atualizar o Agente de Rede para Windows XP somente no Microsoft Windows XP. As edições compatíveis do Microsoft Windows XP e suas versões correspondentes do Agente de Rede estão indicadas na lista de sistemas operacionais compatíveis. É possível baixar a versão necessária do Agente de Rede para Microsoft Windows XP nesta página.

Recomendamos a instalação da mesma versão do Agente de Rede para Linux que o Kaspersky Security

Center Linux.

O Kaspersky Security Center Linux é totalmente compatível com o Agente de Rede da mesma versão ou de versões mais recentes.

O Agente de Rede para macOS é fornecido com o aplicativo de segurança Kaspersky para este sistema operacional.

Aplicativos e soluções da Kaspersky compatíveis

O Kaspersky Security Center Linux é compatível com a implementação e o gerenciamento centralizados de todos os aplicativos e soluções da Kaspersky que são compatíveis atualmente. Para conhecer as versões dos aplicativos e soluções, consulte a página da Web de ciclo de vida de suporte ao aplicativo.

Aplicativos das Kaspersky compatíveis:

- Kaspersky Endpoint Security for Windows (compatível com servidores de arquivo)
- Kaspersky Endpoint Security for Linux (compatível com servidores de arquivo)
- Kaspersky Endpoint Security for Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security for iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux
- Kaspersky Security for Virtualization Light Agent
- KATA Sandbox (um dos componentes do Kaspersky Anti Targeted Attack Platform)
- Kaspersky Thin Client
- Kaspersky NGFW

- Kaspersky Sandbox
- Kaspersky Password Manager for Business
- Kaspersky Vulnerability Management

O Kaspersky Security Center Linux está incluído nas seguintes soluções:

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

Para conhecer as versões dos aplicativos e soluções, consulte a página da Web de ciclo de vida de suporte ao aplicativo.

Problemas conhecidos e limitações

A conexão única (SSO) não é compatível com o Kaspersky Industrial CyberSecurity for Networks.

Sobre a compatibilidade dos componentes do Kaspersky Security Center Linux

Na tabela abaixo, é possível encontrar informações sobre a compatibilidade dos componentes do Kaspersky Security Center Linux.

Compatibilidade dos componentes do Kaspersky Security Center Linux

Componente	Compatível com
Servidor de Administração Linux do Kaspersky Security Center 17	• Kaspersky Security Center Web Console das seguintes versões: 17, 16.3 e 16.2 • Agente de Rede do Kaspersky Security Center das seguintes versões: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 14*, 10.5**
Kaspersky Security Center 17 Web Console	Servidor de Administração do Kaspersky Security Center Linux das seguintes versões: 17, 16.3 e 16.2
Servidor de Administração principal do Kaspersky Security Center 17 Linux	Servidores de administração secundários: • Kaspersky Security Center Linux das seguintes versões: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1 • Kaspersky Security Center Windows das seguintes versões: 15.1
Servidor de Administração secundário do Kaspersky Security Center 17 Linux	Servidores de Administração principais: • Kaspersky Security Center Linux das seguintes versões: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1 • Kaspersky Security Center Windows das seguintes versões: 15.1
Agente de Rede do Kaspersky Security Center 17	Servidores de Administração: • Kaspersky Security Center Linux das seguintes versões: 17, 16.3, 16.2, 16.1, 16.0, 15.4, 15.3, 15.2, 15.1 • Kaspersky Security Center Windows das seguintes versões: 15.1
Backup e restauração dos dados do Servidor de Administração do Kaspersky Security Center	O backup e a restauração de dados são compatíveis com as seguintes versões do Servidor de Administração do Kaspersky Security Center Linux: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1

*Esta versão é compatível com o Microsoft Windows XP Professional com Service Pack 3. Você pode baixar esta versão do Agente de Rede nesta página.

**Esta versão é compatível com o Microsoft Windows XP Professional com Service Pack 2. Você pode solicitar esta versão do Agente de Rede no Suporte Técnico.

Recomendamos o uso da versão mais recente do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center Web Console. Caso contrário, a funcionalidade do Kaspersky Security Center poderá ficar limitada. Você pode instalar e fazer o upgrade do Servidor de Administração do Kaspersky Security Center e o Kaspersky Security Center Web Console de forma independente. Neste caso, garanta que a versão do Kaspersky Security Center Web Console instalado seja compatível com a versão do Servidor de Administração ao qual você se conecta:

Caso tenha a versão mais recente do Kaspersky Security Center Web Console e a versão anterior do Kaspersky Security Center e ocorrer um erro durante a autenticação do domínio, o texto de erro terá uma mensagem padrão.

Comparativo do Kaspersky Security Center: baseado em Windows X baseado em Linux

A Kaspersky fornece o Kaspersky Security Center como uma solução local para duas plataformas: Windows e Linux. Na solução para Windows, você instala o Servidor de Administração em um dispositivo que executa um sistema operacional Windows. A solução para Linux tem uma versão do Servidor de Administração que pode ser instalada em um dispositivo Linux. Esta Ajuda on-line contém informações sobre o Kaspersky Security Center. Para obter informações detalhadas sobre a solução baseada em Windows, consulte a Ajuda do Kaspersky Security Center Windows.

A tabela abaixo permite comparar os principais recursos do Kaspersky Security Center como uma solução baseada no Windows e como uma solução baseada no Linux.

Comparativo de recursos do Kaspersky Security Center funcionando como uma solução baseada em Windows e uma solução baseada em Linux

Recurso ou propriedade	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Servidor de Administração		
Localização do Sistema de gerenciamento de banco de dados (DBMS)	No local	No local (O Microsoft SQL não é compatível)
Sistema operacional para instalar o Servidor de Administração	Windows	Linux
Hierarquia de Servidores de Administração	✓	✓
Compatível com Servidores de administração virtuais	✓	✓
Implementação do cluster de failover do Kaspersky Security Center	✓ Somente um cluster de local único	✓ A partir do Kaspersky Security Center 16.2 Linux, o cluster de failover distribuído geograficamente é compatível
Uso do SNMP para enviar estatísticas do Servidor de Administração a aplicativos de terceiros	✓	✓

Recurso ou propriedade	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Servidor Web para publicação de pacotes de instalação e outros arquivos	✓	✓
Console de Administração		
Tipo de Console de Administração	baseado em MMC e baseado na Web	Baseado na web
Sistema operacional para instalar o Console de Administração baseado na Web	Windows ou no Linux	Linux
Faça login no console usando a autenticação do domínio	✓	✓
Gerenciamento de dispositivos clientes e grupos de administração		
Número máximo de dispositivos gerenciados (por Servidor de Administração)	100 mil (com o Microsoft SQL Server)	50.000 (com PostgreSQL e Postgres Pro)
Sondagem da rede	✓	✓
Proteção de dispositivos gerenciados Windows, macOS e Linux	✓	✓
Proteção de dispositivos móveis	✓ Gerenciamento básico de dispositivos móveis	✓ MDM e usando a funcionalidade do Kaspersky Secure Mobility Management (sob a licença)
Gerenciamento da proteção de máquinas virtuais	✓	✓
Proteção da infraestrutura de nuvem pública	✓	—
Conexão remota à Área de trabalho de um dispositivo cliente	✓	✓
Criptografia e proteção de dados	✓ Em dispositivos gerenciados baseados no Windows com o Kaspersky Endpoint Security for Windows ou o Kaspersky Endpoint Security for Mac instalado	✓ Em dispositivos gerenciados baseados no Windows com o Kaspersky Endpoint Security for Windows ou o Kaspersky Endpoint Security for Mac instalado
Suporte a clusters e matrizes de servidores em grupos de administração	✓	✓
Hierarquia do grupo de administração	✓	✓
Adicionando um gateway de conexão na DMZ como um ponto de distribuição	✓ (não compatível com o Web Console)	✓
Trabalhar com usuários		
Criação e gerenciamento de contas de usuário	✓	✓
Gerenciamento de aplicativos da Kaspersky		
Políticas do aplicativo	✓	✓
Tarefas para aplicativos da Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Servidor Proxy da KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Implementação centralizada de chaves de licença para aplicativos da Kaspersky	✓	✓

Recurso ou propriedade	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.3 Linux
Diagnóstico remoto de dispositivos cliente	✓	✓
Atualização automática dos aplicativos Kaspersky	✓	✓
Suporte ao Controle Adaptativo de Anomalias	✓	✓
Gerenciamento de segurança centrada no dispositivo	✓	✓
Gerenciamento de segurança centrada no usuário	✓	✓
Gerenciamento do sistema		
Implementação de sistemas operacionais em dispositivos cliente	✓	—
Gerenciamento de licenças de terceiros	✓	A ser implementado em 2026
Usar Servidor de Administração como servidor WSUS	✓	✓ (somente no modo de pesquisa passiva do Windows Update)
Gerenciar aplicativos de terceiros em dispositivos cliente		
Instalação de atualizações de software de terceiros e correção de vulnerabilidades de software de terceiros	✓	✓
Importar e exportar categorias de aplicativos	✓ (não compatível com o Web Console)	A ser implementado em 2026
Monitoramento, relatórios e auditoria		
Gerenciar revisões de objeto	✓	✓
Comparar as revisões de uma política	✓	✓
Visualização e trabalho com alertas detectados pelo Kaspersky Endpoint Detection and Response Optimum	✓	✓
Notificações sobre eventos que ocorreram em dispositivos gerenciados	✓	✓
Monitoramento do status de políticas e do status das tarefas	✓	✓
Integrações		
Integração com o Kaspersky Managed Detection and Response	✓	✓
Integração com sistemas SIEM	✓	✓
Agregar alertas e executar ações de resposta usando o Active Directory, KASAP e Kaspersky TIP Sandbox	—	✓ Você deve ativar o Servidor de Administração com uma licença Kaspersky Next XDR Optimum e, em seguida, implementar a chave de licença do Kaspersky Next XDR Optimum nos seus aplicativos gerenciados

Sobre o Kaspersky Next Expert View

Usar o Kaspersky Security Center como um aplicativo local significa que o usuário instala o Kaspersky Security Center, incluindo o Servidor de Administração, em um dispositivo local e gerencia o sistema de segurança de rede por meio do Console de Administração baseado no console de gerenciamento Microsoft (disponível somente no Kaspersky Security Center Windows) ou no Kaspersky Security Center Web Console.

No entanto, é possível usar o Kaspersky Security Center como um serviço de nuvem. Nesse caso, o Kaspersky Security Center é instalado e mantido no ambiente em nuvem pelos especialistas da Kaspersky, e a Kaspersky fornece o acesso ao Servidor de Administração como um serviço. Você gerencia o sistema de segurança da rede através do Console de Administração baseado na nuvem chamado Kaspersky Next Expert View. Esse console tem uma interface semelhante à interface do Kaspersky Security Center Web Console.

A interface e a documentação do Kaspersky Next Expert View estão disponíveis nos seguintes idiomas:

- Inglês
- Francês
- Alemão
- Italiano
- Japonês
- Português (Brasil)
- Russo
- Chinês simplificado
- Espanhol
- Espanhol (LATAM)
- Chinês tradicional

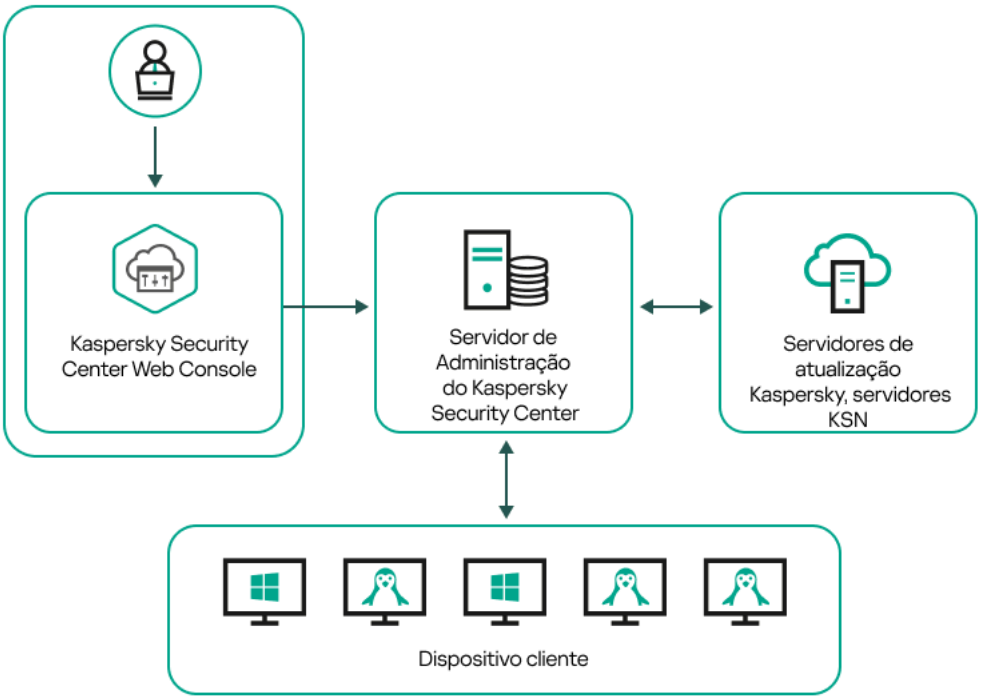
Mais informações sobre o Kaspersky Next Expert View e os seus recursos estão disponíveis na documentação do Kaspersky Next Expert View e na documentação do Kaspersky Endpoint Security for Business.

Arquitetura e conceitos básicos

Esta seção explica a arquitetura dos aplicativos e os conceitos básicos relacionados com o Kaspersky Security Center Linux.

Arquitetura

Esta seção fornece uma descrição dos componentes do Kaspersky Security Center e sua interação.



Arquitetura do Kaspersky Security Center Linux

O Kaspersky Security Center Linux inclui os seguintes componentes básicos:

- **Kaspersky Security Center Web Console**. Fornece uma interface Web para criar e manter o sistema de proteção da rede de uma organização cliente gerenciada pelo Kaspersky Security Center.
- **Servidor de Administração do Kaspersky Security Center** (também chamado de *Servidor*). Centraliza o armazenamento das informações sobre os aplicativos instalados na rede da organização e a forma como é possível gerenciá-los.
- **Servidores de atualização Kaspersky**. Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.
- **Servidores da KSN**. Servidores que contêm informações o banco de dados da Kaspersky com informações constantemente atualizadas sobre a reputação de arquivos, recursos da Web e software. O Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky quanto a ameaças, aprimora o desempenho de alguns componentes de proteção e reduz a probabilidade ocorrerem falsos positivos.
- **Dispositivos cliente.** Dispositivos cliente da empresa, protegidos pelo Kaspersky Security Center Linux. Cada dispositivo que precisa ser protegido deve ter um dos aplicativos de segurança da Kaspersky instalado.

Diagrama de implementação do Servidor de Administração do Kaspersky Security Center Linux e do Kaspersky Security Center Web Console

A figura abaixo demonstra o diagrama de implementação do Servidor de Administração do Kaspersky Security Center Linux e do Kaspersky Security Center Web Console.

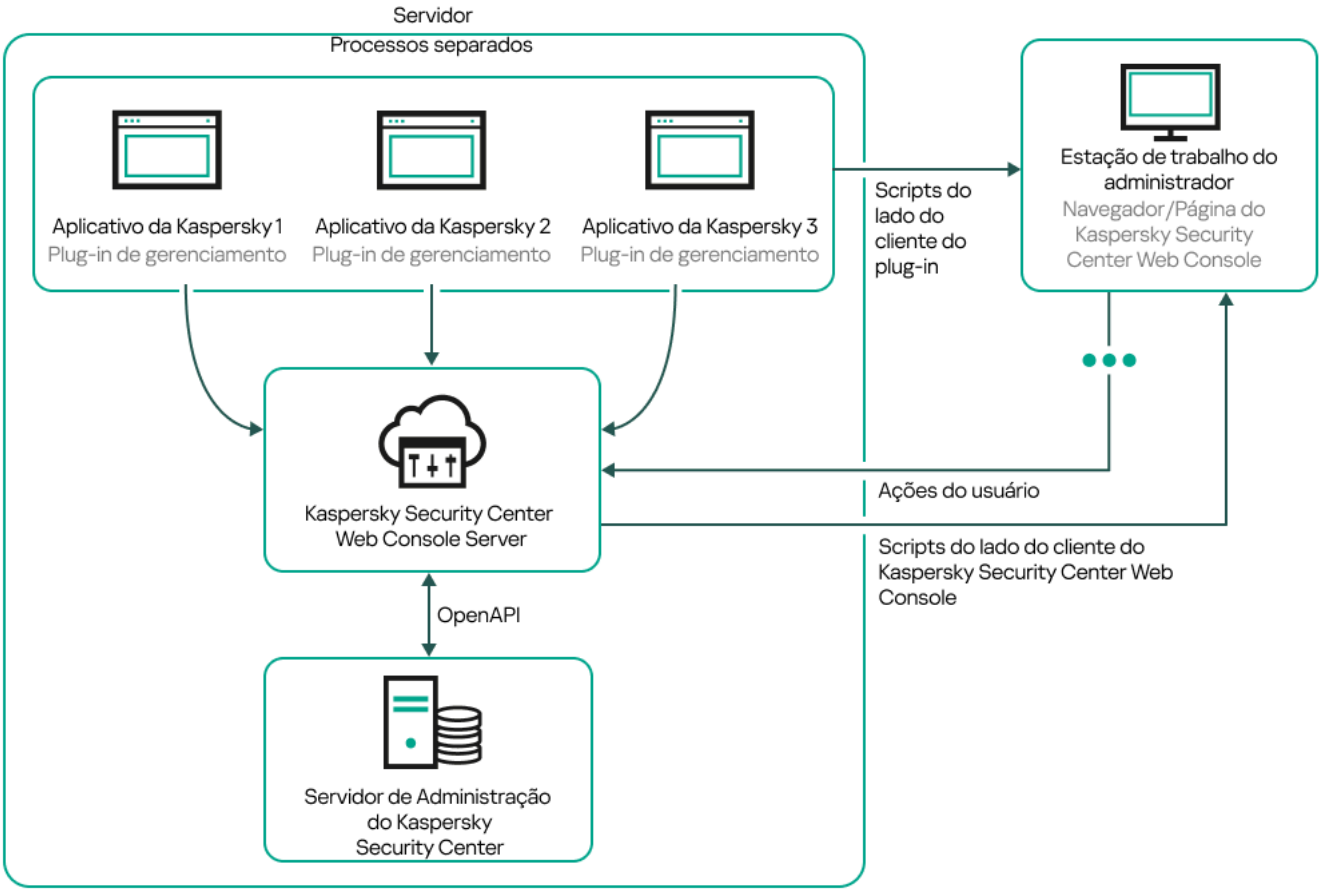


Diagrama de implementação do Servidor de Administração do Kaspersky Security Center Linux e do Kaspersky Security Center Web Console

Os plugins para gerenciamento de aplicativos Kaspersky instalados em dispositivos protegidos (um plugin para cada aplicativo) são implementados juntamente com o Kaspersky Security Center Web Console Server.

Como administrador, você acessa o Kaspersky Security Center Web Console usando um navegador na sua estação de trabalho.

Quando as ações específicas são executadas no Kaspersky Security Center Web Console, o Kaspersky Security Center Web Console Server se comunica com o Servidor de Administração do Kaspersky Security Center Linux por meio da OpenAPI. O Kaspersky Security Center Web Console Server solicita as informações necessárias do Servidor de Administração do Kaspersky Security Center Linux e exibe os resultados das operações no Kaspersky Security Center Web Console.

Portas usadas pelo Kaspersky Security Center Linux

As tabelas abaixo mostram as portas padrão utilizadas pelo Servidor de Administração e pelos dispositivos clientes. Se desejar, você pode alterar cada um desses números de porta padrão.

Portas utilizadas pelo servidor de Administração do Kaspersky Security Center Linux

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
8060	klcsweb	TCP	Transmissão de pacotes de instalação publicados aos dispositivos cliente	Publicando pacotes de instalação. É possível alterar o número da porta padrão no **Servidor Web** seção da janela de propriedades do Servidor de Administração. Esta porta é opcional. Por razões de segurança, recomendamos usar a porta TCP 8061.
8061	klcsweb	TCP (TLS)	Transmitindo pacotes de instalação publicados aos dispositivos cliente	Publicando pacotes de instalação. É possível alterar o número da porta padrão no **Servidor Web** seção da janela de propriedades do Servidor de Administração.
13000	klserver	TCP (TLS)	Receber conexões de Agentes de Rede e Servidores de Administração secundários; também usado em Servidores de Administração secundários para receber conexões do Servidor de Administração principal (por exemplo, se o Servidor de Administração secundário estiver na DMZ)	Gerenciando dispositivos clientes e Servidores de Administração secundários. Você pode alterar o número da porta padrão para conexões de entrada dos Agentes de Rede ao configurar as portas de conexão durante a instalação do Kaspersky Security Center Linux. Você pode alterar a porta padrão para conexões de entrada dos Servidores de Administração secundários ao criar a hierarquia de Servidores de Administração.
13000	klserver	UDP	Recebendo informações sobre dispositivos que foram desativados a partir de Agentes de Rede	Gerenciamento de dispositivos cliente. Você pode alterar o número da porta padrão na janela nas Configurações de política do Agente de Rede.
13291	klserver	TCP (TLS)	Uso do utilitário klakaut para automatizar a operação do Kaspersky Security Center Linux	Como trabalhar com o utilitário klakaut. O utilitário klakaut e seu sistema de Ajuda estão localizados na pasta de instalação do Kaspersky Security Center Linux. Esta porta é fechada por padrão. Se você quiser usar o utilitário klakaut para automatizar a operação do Kaspersky Security Center Linux, abra a porta 13291 usando o utilitário klscflag.
13299	klserver	TCP (TLS)	Recebimento de conexões do Identity and Access Manager (IAM) para o Servidor de Administração; recebimento de conexões para o Servidor de Administração pela OpenAPI	Como gerenciar o Servidor de Administração com o Kaspersky Security Center Web Console; como trabalhar com a OpenAPI. É possível alterar o número da porta padrão na janela de propriedades do Servidor de Administração (na subseção **Portas de conexão** da seção **Geral**) ou ao criar uma hierarquia de Servidores de Administração.

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
14000	klserver	TCP	Receber conexões dos Agentes de Rede	Gerenciando dispositivos cliente. É possível alterar o número da porta padrão ao configurar portas de conexão durante a instalação do Kaspersky Security Center Linux ou ao conectar manualmente um dispositivo cliente ao Servidor de Administração. Esta porta é opcional e está fechada por padrão. Por razões de segurança, recomendamos usar a porta TCP 13000.
13111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	TCP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela Propriedades do Servidor de Administração.
15111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	UDP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela Propriedades do Servidor de Administração.
17111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	HTTPS	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela Propriedades do Servidor de Administração.
17000	klactprx	TCP (TLS)	Recebendo conexões de dispositivos gerenciados para a ativação do aplicativo	Servidor proxy de ativação para dispositivos gerenciados. Você pode alterar o número da porta padrão na janela de propriedades do Servidor de Administração (na subseção **Portas adicionais** da seção **Geral**).
13292 (apenas se você gerencia dispositivos móveis)	klserver	TCP (TLS)	Receber conexões de dispositivos móveis	Gerenciamento de Dispositivos Móveis. Você pode alterar o número da porta padrão na janela de propriedades do Servidor de Administração no Console de Administração ou no Kaspersky Security Center Web Console.
19170	klserver	HTTPS (TLS)	Conexões em túnel para dispositivos gerenciados com o uso do utilitário klsctunnel	Conexão remota a dispositivos gerenciados com o uso do Kaspersky Security Center Web Console. É possível alterar o número da porta padrão na janela de propriedades do Servidor de Administração (**Geral** → **Portas de conexão** → **Tunelamento de conexão RDP**).
4444	kliam	HTTPS	Autenticação usando o protocolo OpenID Connect	Troca de tokens de autenticação entre o navegador e o Identity and Access Manager (IAM).
9050	kliam	HTTPS	Conexão ao Servidor de Administração usando o IAM	Troca de tokens de autenticação entre o Kaspersky Security Center Web Console e o IAM.

Caso o Servidor de Administração e o banco de dados sejam instalados em dispositivos diferentes, será necessário disponibilizar as portas necessárias no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MariaDB Server). Consulte a documentação do DBMS para obter informações relevantes.

A tabela abaixo mostra a porta utilizada pelo Servidor de MDM do iOS™ (somente se você gerencia dispositivos móveis).

Porta usada pelo Servidor de MDM do iOS

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
443	kliosmdmservicesrv	TCP (TLS)	Receber conexões de dispositivos móveis iOS	Gerenciamento de Dispositivos Móveis. Você pode alterar o número da porta padrão ao instalar o MDM do iOS Server.

A tabela abaixo mostra a porta utilizada pelo Kaspersky Security Center Web Console Server. Pode ser o mesmo dispositivo no qual o Servidor de Administração está instalado ou em outro.

Porta usada pelo Kaspersky Security Center Web Console

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
8080	Node.js: JavaScript do lado do servidor	TCP (TLS)	Receber conexões do navegador no Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. É possível alterar o número da porta padrão ao instalar o Kaspersky Security Center Web Console. Ao instalar o Kaspersky Security Center Web Console no sistema operacional ALT Linux, é necessário especificar um número de porta diferente de 8080, pois essa porta é usada pelo sistema operacional.

A tabela abaixo mostra as portas utilizadas pelos dispositivos gerenciados nos quais o Agente de Rede está instalado.

Portas usadas pelo Agente de Rede

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
15000	klnagent	UDP	Sinais de gerenciamento do Servidor de Administração ou de um ponto de distribuição para os Agentes de Rede	Gerenciando dispositivos cliente. Você pode alterar o número da porta padrão na janela nas Configurações de política do Agente de Rede.
15000	klnagent	Transmissão UDP	Obtendo dados sobre outros Agentes de Rede no mesmo domínio de transmissão (os dados são enviados ao Servidor de Administração)	Fornecendo atualizações e pacotes de instalação.
15001	klnagent	UDP	Recebendo solicitações de multicast de um ponto de distribuição (se estiver em uso)	Recebendo atualizações e pacotes de instalação de um ponto de distribuição. Você pode alterar o número da porta padrão na janela propriedades do ponto de distribuição.
30522, 30523 (portas na interface localhost)	klnagent	TCP	Transferência de atualizações de aplicativos do Agente de Rede para os aplicativos da Kaspersky instalados localmente usando o componente FileTransferBridge	Dispositivos gerenciados que recebem atualizações do aplicativo da Kaspersky do Servidor de Administração especificado como uma fonte de atualização de bancos de dados.

Observe que o processo klnagent também pode solicitar portas livres do intervalo de portas dinâmicas de um sistema operacional de endpoint. Essas portas são alocadas automaticamente para o processo klnagent pelo sistema operacional. Assim, o processo klnagent poderá usar algumas portas que são usadas por outro software. Caso o processo klnagent afete as operações desse software, altere suas configurações da porta ou altere o intervalo padrão de porta dinâmica no sistema operacional para excluir a porta usada pelo software afetado.

Também é preciso levar em consideração que as recomendações sobre a compatibilidade do Kaspersky Security Center Linux com software de terceiros são descritas apenas como referência e podem não ser aplicáveis a novas versões de software de terceiros. As recomendações descritas para configurar as portas são baseadas nas experiências do Suporte Técnico e em nossas práticas recomendadas.

A tabela abaixo mostra a porta utilizada pelos dispositivos gerenciados nos quais o Agente de Rede instalado atua como um ponto de distribuição. As portas listadas são utilizadas pelos dispositivos do ponto de distribuição, além das portas utilizadas pelos Agentes de Rede (consulte a tabela acima).

Portas usadas pelo Agente de Rede funcionando como ponto de distribuição

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
13000	klnagent	TCP (TLS)	Recebendo conexões a partir dos Agentes de Rede e gateways de conexão	Gerenciar dispositivos clientes, entregar atualizações e pacotes de instalação. É possível alterar o número da porta padrão nas propriedades do ponto de distribuição.
13111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	TCP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. É possível alterar o número da porta padrão nas propriedades do ponto de distribuição.
15111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	UDP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. É possível alterar o número da porta padrão nas propriedades do ponto de distribuição.
17111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	HTTPS	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. É possível alterar o número da porta padrão nas propriedades do ponto de distribuição.
13295 (apenas se você usar o ponto de distribuição como um servidor push)	klnagent	TCP (TLS)	Receber conexões de dispositivos cliente	Servidor push. É possível alterar o número da porta padrão nas propriedades do ponto de distribuição.
8060	klcsweb	TCP	Transmissão de pacotes de instalação publicados aos dispositivos cliente	Publicando pacotes de instalação. É possível alterar o número da porta padrão no **Servidor Web** seção da janela de propriedades do Servidor de Administração.
8061	klcsweb	TCP (TLS)	Transmitindo pacotes de instalação publicados aos dispositivos cliente	Publicando pacotes de instalação. É possível alterar o número da porta padrão no **Servidor Web** seção da janela de propriedades do Servidor de Administração.

A tabela abaixo mostra as portas utilizadas por um dispositivo controlador de domínio.

Portas utilizadas por um dispositivo controlador de domínio

Número da porta	Protocolo	Propósito da porta	Escopo
389	LDAP via TCP ou UDP	Conexão com um servidor LDAP	Sondagem do controlador de domínio
636	LDAP via TLS	Conexão com um servidor LDAP	Sondagem do controlador de domínio

A tabela abaixo lista as portas que devem ser abertas nos dispositivos clientes nos quais o Agente de Rede não está instalado.

Porta usada no dispositivo cliente não atribuído

Número da porta	Protocolo	Propósito da porta	Escopo
22	SSH	Conexão com um dispositivo cliente por SSH	Instalação remota de aplicativos da Kaspersky.

Portas usadas pelo Kaspersky Security Center Web Console

A tabela abaixo lista as portas que devem estar abertas no dispositivo em que o Servidor do Kaspersky Security Center Web Console (também chamado de Kaspersky Security Center Web Console) está instalado.

Portas usadas pelo Kaspersky Security Center Web Console

Número da porta	Nome do serviço	Protocolo	Propósito da porta	Escopo
2001	Servidor de plugins de produto do Kaspersky Security Center	HTTPS	Porta de API utilizada pelos processos do plug-in de gerenciamento para receber solicitações do "Serviço de gerenciamento do Kaspersky Security Center Web Console".	Execução de processos do nó de plugins de gerenciamento
1329, 2003	Serviço de gerenciamento do Kaspersky Security Center Web Console	HTTPS	Portas de API utilizadas para receber solicitações do "Serviço de gerenciamento do Kaspersky Security Center Web Console" em execução no mesmo dispositivo.	Atualização de componentes do Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	Porta de API utilizada para receber solicitações do "Serviço de gerenciamento do Kaspersky Security Center Web Console" em execução no mesmo dispositivo.	Execução de processos do nó do Kaspersky Security Center Web Console
4222	NATS do Kaspersky Security Center Web Console	HTTPS	Portas de API do Message Broker baseado em NATS usadas para comunicação entre processos do Kaspersky Security Center Web Console e plug-ins de gerenciamento. A porta 8222 é utilizada para monitorar o NATS.	Interação de processos entre o Kaspersky Security Center Web Console e os plugins de gerenciamento
4444	Identity and Access Manager (IAM)	HTTPS	Porta utilizada pelo protocolo de autenticação OpenID Connect.	Troca de tokens de autenticação entre o Kaspersky Security Center Web Console e o Identity and Access Manager (IAM)
9050	IAM	HTTPS	Porta utilizada pelo IAM.	Interação entre o Kaspersky Security Center Web Console e o IAM

Conceitos básicos

Esta seção explica os conceitos básicos relacionados com o Kaspersky Security Center Linux.

Servidor de Administração

Os componentes do Kaspersky Security Center Linux permitem o gerenciamento remoto dos aplicativos Kaspersky instalados em dispositivos cliente.

Os dispositivos com o componente do Servidor de Administração instalado serão referidos como *Servidores de Administração* (aqui referidos como *Servidores*). Os Servidores de Administração devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

O Servidor de Administração é instalado em um dispositivo como um serviço, com o seguinte conjunto de atributos:

- Com o nome `kladminserver_srv`
- Configurado para iniciar automaticamente ao inicializar o sistema operacional
- Com a conta `ksc` ou a conta do usuário selecionada durante a instalação do Servidor de Administração

Consulte o seguinte artigo para obter a lista completa de configurações de instalação: Instalação do Kaspersky Security Center Linux.

O Servidor de Administração realiza as seguintes funções:

- Armazenamento da estrutura dos grupos de administração
- Armazenamento de informações sobre a configuração de dispositivos cliente
- Organização dos repositórios para pacotes de distribuição de aplicativos
- Instalação remota de aplicativos para dispositivos cliente e remoção de aplicativos
- Atualização de bancos de dados de aplicativos e módulos de software dos aplicativos Kaspersky
- Gerenciamento de políticas e tarefas nos dispositivos cliente
- Armazenamento de informações sobre eventos que ocorreram em dispositivos cliente
- Geração de relatórios na operação dos aplicativos Kaspersky
- Implementação de chaves de licença para os dispositivos cliente e armazenamento de informações sobre chaves de licença
- O encaminhamento de notificações sobre o progresso das tarefas (tal como detecção de vírus em um dispositivo cliente)

Nomeando Servidores de Administração na interface do aplicativo

Na interface do Kaspersky Security Center Web Console, os Servidores de Administração podem ter os seguintes nomes:

- Nome do dispositivo do Servidor de Administração, por exemplo: "*nome do dispositivo*" ou "Servidor de Administração: *nome do dispositivo*".
- Endereço IP do dispositivo do Servidor de Administração, por exemplo: "*Endereço de IP*" ou "Servidor de Administração: *Endereço de IP*".
- Os Servidores de Administração secundários e virtuais têm nomes personalizados que você especifica ao conectar um Servidor de Administração virtual ou secundário ao Servidor de Administração principal.
- Se você usar o Kaspersky Security Center Web Console: instalado em um dispositivo Linux, o aplicativo exibe os nomes dos Servidores de Administração especificados como confiáveis no arquivo de resposta.

Você pode conectar-se ao Servidor de Administração por meio do Kaspersky Security Center Web Console.

Hierarquia de Servidores de Administração

Os Servidores de Administração podem ser dispostos numa hierarquia principal/secundário. Cada Servidor de Administração pode possuir vários Servidores de Administração secundários (citados como *Servidores secundários*) em diferentes níveis de alojamento da hierarquia. O nível de alojamento para Servidores secundários não é limitado. Os grupos de administração do Servidor de Administração principal incluirão então os dispositivos cliente de todos os Servidores de Administração secundários. Portanto, as seções isoladas e independentes das redes podem ser gerenciadas por diferentes Servidores de Administração que, por sua vez, são gerenciadas pelo Servidor principal.

Em uma hierarquia, um Servidor de Administração baseado em Linux pode funcionar tanto como um servidor primário quanto como um servidor secundário. O servidor primário baseado em Linux pode gerenciar servidores secundários baseados em Linux e em Windows. Um servidor principal baseado em Windows pode gerenciar um servidor secundário baseado em Linux.

Os *Servidores de Administração virtuais* são um caso particular de Servidores de Administração secundários.

A hierarquia dos Servidores de Administração pode ser usada para o seguinte:

- Diminuir a carga no Servidor de Administração (em comparação com um único Servidor de Administração instalado para uma rede inteira).
- Diminuir o tráfego na intranet e simplificar o trabalho com escritórios remotos. Você não é precisa estabelecer conexões entre o Servidor de Administração principal e todos os dispositivos na rede, os quais podem estar localizados, por exemplo, em outras regiões. É suficiente para instalar em cada segmento de rede um Servidor de Administração secundário, distribuir dispositivos entre os grupos de administração de servidores secundários e estabelecer conexões entre os servidores secundários e o servidor principal em canais de comunicação rápida.
- Distribuir responsabilidades entre os administradores de segurança antivírus. Todos os recursos para gerenciamento e monitoramento centralizado do status de segurança antivírus em redes corporativas permanecem disponíveis.
- Uso do Kaspersky Security Center Linux por provedores de serviços. Um provedor de serviços somente necessita instalar o Kaspersky Security Center Linux e o Kaspersky Security Center Web Console. Para gerenciar um número maior de dispositivos cliente de várias organizações, um provedor de serviço pode adicionar Servidores de Administração secundários (inclusive servidores virtuais) na hierarquia de Servidores de Administração.

Cada dispositivo incluído na hierarquia dos grupos de administração pode ser conectado apenas a um Servidor de Administração. Você deve monitorar de forma independente a conexão de dispositivos aos Servidores de Administração. Use os recursos para a pesquisa de dispositivo em grupos de administração de diferentes Servidores com base em atributos de rede.

Servidor de Administração virtual

O Servidor de Administração virtual (também referido como *Servidor virtual*) é um componente do Kaspersky Security Center Linux projetado para gerenciar a proteção antivírus da rede de uma organização cliente.

O Servidor de Administração virtual é um caso particular de um Servidor de Administração secundário com as seguintes restrições em comparação com o Servidor de Administração físico:

- O Servidor de Administração virtual só pode ser criado no Servidor de Administração principal.
- O Servidor de Administração virtual usa o banco de dados do Servidor de Administração principal. Tarefas de backup e restauração de dados, bem como tarefas de verificação de atualização e download, não são compatíveis com um Servidor de Administração virtual.
- O Servidor virtual não é compatível com a criação de Servidores de Administração secundários (incluindo Servidores virtuais).

Além disso, o Servidor de Administração virtual possui as seguintes restrições:

- Na janela de propriedades do Servidor de Administração virtual, o número de seções é limitado.
- Para instalar aplicativos Kaspersky remotamente em dispositivos cliente gerenciados pelo Servidor Administrativo virtual, você deve certificar-se de que o Agente de Rede está instalado em um dos dispositivos cliente para poder garantir a comunicação com o Servidor de Administração virtual. Na primeira conexão ao Servidor de Administração virtual, esse dispositivo é automaticamente atribuído como o ponto de distribuição, funcionando como um gateway de conexão entre os dispositivos cliente e o Servidor de Administração virtual.
- Um servidor virtual pode amostrar a rede somente através de pontos de distribuição.
- Para reiniciar um Servidor virtual que não está funcionando corretamente, o Kaspersky Security Center Linux reinicia o Servidor de Administração principal e todos os Servidores virtuais.
- Os usuários criados em um servidor virtual não podem receber uma função no Servidor de Administração.

O administrador de um Servidor virtual possui todos os privilégios neste Servidor virtual em particular.

Servidor Web

O *Servidor Web* do Kaspersky Security Center (daqui em diante referido como *Servidor Web*) é um componente do Kaspersky Security Center que é instalado junto com o Servidor de Administração. O Servidor Web foi projetado para a transmissão, através de uma rede, de pacotes de instalação independentes e arquivos de uma pasta compartilhada.

Ao criar um pacote de instalação independente, ela é automaticamente publicada no Servidor da Web. Um link para o download do pacote independente é exibido na lista de pacotes de instalação independentes criados. Se necessário, você poderá cancelar a publicação do pacote independente ou publicá-lo novamente no Servidor da Web.

A pasta compartilhada é usada para armazenar as informações que estão disponíveis para todos os usuários cujos dispositivos são gerenciados através do Servidor de Administração. Se um usuário não tiver acesso direto à pasta compartilhada, ele poderá receber informações a partir dessa pasta usando o Servidor da Web.

Para fornecer aos usuários informações da pasta compartilhada usando o Servidor Web, o administrador deve criar uma subpasta com o nome de "pública" na pasta compartilhada e colar as informações nela.

A sintaxe do link de transferência de informações é a seguinte:

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

onde:

- `<Web Server name>` é o nome do Servidor Web do Kaspersky Security Center.
- `<HTTPS port>` é uma porta HTTPS do Servidor Web que foi definida pelo Administrador. A porta HTTPS pode ser definida na seção **Servidor Web** da janela Propriedades do Servidor de Administração. O número da porta padrão é 8061.
- `<object>` é uma subpasta ou um arquivo ao qual o usuário tem acesso.

O administrador pode enviar o novo link ao usuário de qualquer forma prática: por exemplo, por e-mail.

Ao usar este link, o usuário poderá baixar as informações necessárias para um dispositivo local.

Servidor Web do Kaspersky Security Center Linux

O Kaspersky Security Center Linux Web Server (doravante denominado Web Server) é um componente do Kaspersky Security Center Linux. O Servidor Web foi projetado para publicar pacotes de instalação independentes e arquivos da pasta compartilhada.

Os pacotes de instalação que foram criados são publicados no Servidor Web automaticamente e então removidos após o primeiro download. O administrador pode enviar o novo link ao usuário de qualquer forma prática: por exemplo, por e-mail.

Ao clicar no link, o usuário poderá baixar as informações necessárias para um dispositivo móvel.

Configurações do Servidor Web

Se um ajuste fino do Servidor Web for necessário, suas propriedades lhe permitem alterar as portas para HTTP (8060) e HTTPS (8061). Além de alterar as portas, você pode substituir o certificado do servidor por HTTPS e alterar o FQDN o Servidor Web para HTTP.

Configurações do servidor Web em um gateway de conexão

Um serviço de Servidor Web separado é implementado em um ponto de distribuição em um modo de gateway de conexão, o que permite trabalhar com dispositivos móveis conectados ao Kaspersky Security Center Linux. Este serviço é responsável por transferir pacotes de instalação de aplicativos e perfis de gerenciamento de dispositivos para dispositivos sem conectá-los diretamente ao Servidor de Administração. Os arquivos são transferidos à medida que o serviço processa solicitações de arquivos HTTP/HTTPS em um gateway de conexão.

O serviço do servidor Web em um gateway de conexão é instalado juntamente com o Agente de Rede do Linux. Para usar essa funcionalidade, é necessário atribuir um dispositivo que atuará como um ponto de distribuição em um modo de gateway de conexão para ser usado como Servidor Web e, em seguida, especificar as configurações correspondentes. Para obter informações detalhadas sobre como configurar as definições do Servidor Web em um gateway de conexão, consulte a ajuda do Kaspersky Secure Mobility Management

https://support.kaspersky.com/secure-mobility-management/9.0/294935

.

Agente de Rede

A interação entre o Servidor de Administração e os dispositivos é realizada pelo componente *Agente de Rede* do Kaspersky Security Center Linux. O Agente de Rede deve ser instalado em todos os dispositivos cliente nos quais o Kaspersky Security Center Linux é usado para gerenciar os aplicativos da Kaspersky.

Um dispositivo com o Agente de Rede instalado é denominado de *dispositivo gerenciado* ou *dispositivo*. Você pode baixar o pacote de instalação do Agente de Rede das seguintes fontes:

- Armazenamento do Servidor de Administração (você deve ter o Servidor de Administração instalado)
- Site da Kaspersky

O Agente de Rede para Linux é instalado no dispositivo como um serviço com o seguinte conjunto de atributos:

- O nome "Agente de Rede do Kaspersky"
- Configurado para iniciar automaticamente ao inicializar o sistema operacional
- Uso da conta root

O Agente de Rede para Windows é instalado no dispositivo como um serviço com o seguinte conjunto de atributos:

- O nome "Agente de Rede do Kaspersky Security Center"
- Configurado para iniciar automaticamente ao inicializar o sistema operacional
- Usar o LocalSystem Account

O Agente de Rede para macOS é instalado no dispositivo como um serviço, com o seguinte conjunto de atributos:

- O nome "com.kaspersky.klnagent.core"
- Configurado para iniciar automaticamente ao inicializar o sistema operacional
- Uso da conta root

Os nomes dos processos de serviço:

- Para Linux:
  - klnagent64.service (para um sistema operacional de 64 bits)
  - klnagent.service (para um sistema operacional de 32 bits)
- Para Windows:
  - klnagent

- Para macOS:
  - com.kaspersky.klnagent

Por padrão, o Agente de Rede é instalado nos seguintes locais:

- Para Linux:
  - Sistemas de 32 bits: /opt/kaspersky/klnagent/
  - Sistemas de 64 bits: /opt/kaspersky/klnagent64/
- Para Windows:
  - Sistemas de 32 bits: C:\Program Files\Kaspersky Lab\NetworkAgent
  - Sistemas de 64 bits: C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
- Para macOS:
  - Sistemas de 64 bits: /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

Em dispositivos Windows, é possível especificar uma pasta diferente para a instalação do Agente de Rede nas configurações do pacote de instalação. Entretanto, para dispositivos Linux, o Agente de Rede só pode ser instalado no diretório padrão.

A pasta de instalação do Agente de Rede também contém utilitários para gerenciar e diagnosticar a operação do Agente de Rede, como os utilitários klmover e klnagchk.

Ao instalar o Servidor de Administração, a versão do servidor do Agente de Rede é instalada automaticamente junto com o Servidor de Administração. No entanto, para gerenciar o dispositivo do Servidor de Administração como qualquer outro dispositivo gerenciado, instale o Agente de Rede para Linux no dispositivo do Servidor de Administração. Nesse caso, o Agente de Rede para Linux é instalado e funciona independentemente da versão do servidor do Agente de Rede que você instalou junto com o Administration Server.

O Agente de Rede sincroniza o dispositivo gerenciado com o Servidor de Administração. Recomendamos definir o intervalo de sincronização (também conhecido como *heartbeat*) para 15 minutos a cada 10.000 dispositivos gerenciados.

Grupos de administração

Um *grupo de administração* (aqui também referido como um *grupo*) é um conjunto lógico de dispositivos gerenciados e combinados na base de um tratado específico com o propósito de gerenciar os dispositivos agrupados como uma unidade única dentro do Kaspersky Security Center Linux.

Todos os dispositivos gerenciados dentro de um grupo de administração são configurados para fazer o seguinte:

- Usar as mesmas configurações de aplicativo (que você pode definir nas políticas de grupo).
- Use um modo de operação comum para todos os aplicativos por meio da criação de tarefas de grupo com configurações especificadas. Exemplos de tarefas de grupo incluem criar e instalar um pacote de instalação comum, atualizar os bancos de dados e módulos de aplicativos, verificar dispositivo sob demanda e ativar a proteção em tempo real.

Um dispositivo gerenciado pode pertencer a um somente grupo de administração.

Você pode criar hierarquias que têm qualquer grau de aninhamento para Servidores de Administração e grupos. Um único nível de hierarquia pode incluir servidores de administração secundários e virtuais, grupos e dispositivos gerenciados. Você pode migrar dispositivos de um grupo ao outro sem movê-los fisicamente. Por exemplo, se o cargo de um funcionário na empresa for alterado de contador para desenvolvedor, você pode mover o dispositivo desse funcionário do grupo de administração Contadores para o grupo de administração Desenvolvedores. Depois disso, o dispositivo receberá automaticamente as configurações de aplicativo necessárias para os desenvolvedores.

Dispositivo gerenciado

Um *dispositivo gerenciado* é um dispositivo que executa Linux, Windows ou macOS e que tem o Agente de Rede instalado. Você pode gerenciar esses dispositivos criando tarefas e políticas para os aplicativos instalados nos dispositivos. Você também pode receber relatórios dos dispositivos gerenciados.

Você pode transformar uma função de dispositivo gerenciado em um ponto de distribuição e em um gateway de conexão.

Um dispositivo pode ser gerenciado somente por um Servidor de Administração. O número de dispositivos que podem ser gerenciados por um Servidor de Administração depende da configuração do dispositivo que hospeda o Servidor de Administração e das restrições do DBMS.

Dispositivo não atribuído

Um *dispositivo não atribuído* é um dispositivo na rede que não estava incluído em nenhum grupo de administração. Você pode executar algumas ações em dispositivos não atribuídos, por exemplo, movê-los para seus grupos de administração ou instalar aplicativos neles.

Quando um novo dispositivo é descoberto na rede, esse dispositivo vai para o grupo de administração **Dispositivos não atribuídos**. Você pode configurar regras para que os dispositivos sejam movidos automaticamente para outros grupos de administração após serem descobertos.

Estação de trabalho do administrador

Os dispositivos nos quais o Kaspersky Security Center Web Console Server está instalado, são referidos como *estações de trabalho do administrador*. Os administradores podem usar esses dispositivos para o gerenciamento remoto centralizado dos aplicativos Kaspersky instalados nos dispositivos cliente.

Não há restrições quanto ao número de estações de trabalho do administrador. Em qualquer estação de trabalho do administrador, você pode gerenciar os grupos de administração de vários Servidores de Administração na rede de uma só vez. Você pode conectar uma estação de trabalho do administrador a um Servidor de Administração (físico ou virtual) de qualquer nível de hierarquia.

Você pode incluir uma estação de trabalho do administrador em um grupo de administração como um dispositivo cliente.

Dentro dos grupos de administração de qualquer Servidor de Administração, o mesmo dispositivo pode funcionar como um Servidor de Administração cliente, um Servidor de Administração ou uma estação de trabalho do administrador.

Plug-in da Web de gerenciamento

Um componente especial (o *plugin de gerenciamento da Web*) é usado para a administração remota de softwares da Kaspersky por meio do Kaspersky Security Center Web Console. No presente documento, o plug-in da Web de gerenciamento será referido como *plug-in de gerenciamento*. Um plug-in de gerenciamento é uma interface entre o Kaspersky Security Center Web Console e um aplicativo da Kaspersky específico. Com um plug-in de gerenciamento, você pode configurar tarefas e políticas para o aplicativo.

É possível baixar plug-ins de gerenciamento da Web pelo site da Kaspersky.

O plug-in de gerenciamento fornece o seguinte:

- Interface para criar e editar tarefas e configurações de aplicativo
- Interface para criar e editar políticas e perfis da política para a configuração remota e centralizada de aplicativos e dispositivos da Kaspersky
- Transmissão de eventos gerados pelo aplicativo
- Funções do Kaspersky Security Center Web Console para exibir os dados operacionais e os eventos do aplicativo, além das estatísticas transmitidas de dispositivos clientes

Políticas

Uma *política* é um conjunto de configurações do aplicativo Kaspersky, aplicadas a um grupo de administração e seus subgrupos. Você pode instalar vários aplicativos Kaspersky nos dispositivos de um grupo de administração. O Kaspersky Security Center fornece uma única política para cada aplicativo Kaspersky em um grupo de administração. Uma política possui um dos seguintes status:

O status da política

Estado	Descrição
Ativo	A política atual aplicada ao dispositivo. Apenas uma política pode estar ativa por aplicativo Kaspersky em cada grupo de administração. Os dispositivos aplicam os valores de configuração de uma política ativa para um aplicativo Kaspersky.
Inativo	Uma política que não é aplicada atualmente a um dispositivo.
Ausência	Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

As políticas funcionam de acordo com as seguintes regras:

- Várias políticas com valores diferentes podem ser configuradas para um único aplicativo.
- Apenas uma política pode estar ativa para o aplicativo atual.
- Uma política pode ter políticas secundárias.

Geralmente, você pode usar políticas como preparação para situações de emergência, como um ataque de vírus. Se houver um ataque por meio de unidades flash, você pode ativar uma política que bloqueie o acesso a unidades flash. Nesse caso, a política ativa atual torna-se automaticamente inativa.

Para evitar ter que efetuar manutenção de várias políticas, por exemplo, quando ocasiões diferentes pressupõem a alteração de várias configurações apenas, você pode usar perfis de política.

Um *perfil* de *política* é um subconjunto nomeado de valores de configuração que substitui os valores de configuração de uma política. Um perfil de política afeta a formação de configurações efetivas em um dispositivo gerenciado. *Configurações em vigor* são um conjunto de configurações de política, configurações de perfil de política e configurações de aplicativo locais aplicadas atualmente ao dispositivo.

Os perfis de política funcionam de acordo com as seguintes regras:

- Um perfil de política entra em vigor quando ocorre uma condição de ativação específica.
- Os perfis contêm valores de configurações que diferem das configurações de política.
- A ativação de um perfil de política altera as configurações em vigor do dispositivo gerenciado.
- Uma política pode incluir no máximo 100 perfis de política.

Perfis da política

Às vezes pode ser necessário criar diversas instâncias de uma única política para diferentes grupos de administração; também convém sincronizar os as configurações dessas políticas centralmente. Essas instâncias podem diferir por apenas uma ou duas configurações. Por exemplo, todos os contadores em uma empresa trabalham segundo a mesma política, mas os contadores sênior estão autorizados a usar unidades flash e os contadores júnior, não. Neste caso, aplicar políticas aos dispositivos somente através da hierarquia de grupos de administração pode ser inconveniente.

Para ajudá-lo a evitar a criação de várias instâncias de uma única política, o Kaspersky Security Center Linux permite criar *perfis de política*. Os perfis de política são destinados se você quiser que os dispositivos dentro de um grupo de administração único executem sob configurações de política diferentes.

Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos de destino em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo gerenciado. A ativação de um perfil modifica as configurações da política "básica" que estavam inicialmente ativas no dispositivo. As configurações modificadas assumem valores que foram especificados no perfil.

Tarefas

O Kaspersky Security Center Linux gerencia os aplicativos de segurança da Kaspersky instalados nos dispositivos cliente criando e executando *tarefas*. As tarefas são necessárias para a instalação, inicialização e interrupção de aplicativos, verificação de arquivos, atualização de bancos de dados e módulos de software e para a realização de outras ações em aplicativos.

As tarefas de um aplicativo específico podem ser criadas apenas se o plugin de gerenciamento desse aplicativo estiver instalado.

As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

As seguintes tarefas que são realizadas no Servidor de Administração:

- Distribuição automática de relatórios
- Baixar atualizações no repositório do Servidor de Administração
- Backup de dados do Servidor de Administração
- Manutenção do banco de dados

Os seguintes tipos de tarefas são executados nos dispositivos:

- *Tarefas locais* – Tarefas que são executadas em um dispositivo específico

  As tarefas locais podem ser modificadas pelo administrador, usando o Kaspersky Security Center Web Console ou por um usuário de um dispositivo remoto (por exemplo, por meio da interface do aplicativo de segurança). Se uma tarefa local tiver sido modificada simultaneamente pelo administrador e pelo usuário de um dispositivo gerenciado, as modificações feitas pelo administrador entrarão em vigor porque elas têm uma maior prioridade.

- *Tarefas de grupo* – Tarefas que são executadas em todos os dispositivos de um grupo específico

  Salvo de especificado de outra maneira nas propriedades de tarefa, uma tarefa de grupo também afeta todos os subgrupos do grupo selecionado. Uma tarefa de grupo também afeta (opcionalmente) os dispositivos que foram conectados aos Servidores de Administração secundários e virtuais implementados no grupo ou em algum dos seus subgrupos.

- *Tarefas globais* – Tarefas que são realizadas em um conjunto de dispositivos, independentemente se os mesmos estão incluídos em qualquer grupo

Para cada aplicativo, você pode criar qualquer número de tarefas de grupo, tarefas globais ou tarefas locais.

Você pode efetuar alterações nas configurações de tarefas, exibir o andamento das tarefas, copiar, exportar, importar e excluir tarefas.

Uma tarefa é iniciada em um dispositivo cliente somente se um aplicativo para o qual a tarefa foi criada estiver sendo executado.

Os resultados das tarefas são salvos no log de eventos do Syslog e no log de eventos do Kaspersky Security Center Linux, tanto centralmente no Servidor de Administração como localmente em cada dispositivo.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Escopo da tarefa

O *escopo de uma tarefa* é o conjunto de dispositivos nos quais a tarefa é executada. Os tipos de escopo são os seguintes:

- Para uma *tarefa local*, o escopo é o próprio dispositivo.
- Para uma tarefa do *Servidor de Administração*, o escopo é o Servidor de Administração.
- Para uma *tarefa de grupo*, o escopo é a lista de dispositivos incluídos no grupo.

Ao criar uma *tarefa global*, você pode usar os seguintes métodos para especificar o escopo:

- Especificar determinados dispositivos manualmente.

  Você pode usar um endereço IP (ou uma faixa IP) ou nome DNS como o endereço do dispositivo. Também é possível selecionar dispositivos na rede detectados pelo Servidor de Administração.

- Importar uma lista de dispositivos de um arquivo .txt com os endereços dos dispositivos a serem adicionados (cada endereço deve ser colocado em uma linha individual).

  Se você importar uma lista de dispositivos a partir de um arquivo ou cria uma lista manualmente, e se os dispositivos cliente estão identificados pelos seus nomes, a lista deve conter somente os dispositivos cuja informação já foi adicionada ao banco de dados do Servidor de Administração. Além disso, as informações devem ter sido inseridas quando os dispositivos foram conectados ou durante a descoberta de dispositivos.

- Especificar uma seleção de dispositivos.

  Ao longo do tempo, o escopo de uma tarefa se modifica quando o conjunto de dispositivos incluídos na seleção são modificados. Uma seleção de dispositivos pode ser feita com base nos atributos do dispositivo, incluindo o software instalado em um dispositivo, e com base em tags atribuídas aos dispositivos. A seleção de dispositivos é o modo mais flexível para especificar o escopo de uma tarefa.

  As tarefas para seleções de dispositivos sempre são executadas de acordo com um agendamento pelo Servidor de Administração. Estas tarefas não podem ser executadas em dispositivos que não tenham uma conexão com o Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas diretamente nos dispositivos e, por isso, não dependem da conexão do dispositivo com o Servidor de Administração.

  As tarefas para Seleções de dispositivos não são executadas na hora local de um dispositivo; em vez disso, elas serão executadas na hora local do Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas na hora local de um dispositivo.

Como as configurações do aplicativo local se relacionam com as políticas

Você pode usar as políticas para definir valores idênticos das configurações do aplicativo para todos os dispositivos no grupo.

Os valores das configurações especificados por uma política podem ser redefinidos para dispositivos individuais em um grupo usando as configurações do aplicativo locais. Você somente pode definir os valores das configurações, cuja alteração seja permitida pela política, ou seja, configurações desbloqueadas.

O valor de uma configuração que um aplicativo usa em um dispositivo cliente é definido pela posição do cadeado ( ) para aquela configuração na política:

- Se a modificação da configuração estiver bloqueada, o mesmo valor (definido na política) é utilizado e todos os dispositivos cliente.
- Se a modificação da configuração estiver desbloqueada, o aplicativo usa um valor de configuração local em cada dispositivo cliente em vez do valor especificado na política. O valor do parâmetro pode então ser alterado nas configurações de aplicativo locais.

Deste modo, quando a tarefa está sendo executada em um dispositivo cliente, o aplicativo usa as configurações definidas de duas formas diferentes:

- Por configurações de tarefa e configurações locais de aplicativo, se a configuração não estiver bloqueada contra alteração na política.
- Por política de grupo, se a configuração estiver bloqueada contra alteração.

As configurações de aplicativo locais são alteradas depois da primeira imposição de política de acordo com as configurações de política.

Ponto de distribuição

Ponto de distribuição (anteriormente conhecido como agente de atualização) é um dispositivo com o Agente de Rede instalado, que é usado para a distribuição da atualização, a instalação remota de aplicativos e a recuperação de informações sobre os dispositivos na rede.

Os recursos e casos de uso do Agente de Rede instalado em um dispositivo usado como ponto de distribuição variam conforme o sistema operacional.

Um ponto de distribuição pode executar as seguintes funções:

- Distribuir as atualizações e os pacotes de instalação recebidos do Servidor de Administração para os dispositivos cliente no grupo (incluindo a distribuição por meio de multicasting usando UDP). As atualizações podem ser recebidas do Servidor de Administração ou dos servidores de atualização Kaspersky. Nesse caso, uma tarefa de atualização precisa ser criada para o ponto de distribuição.

  Os pontos de distribuição agilizam a distribuição da atualização e permite liberar recursos do Servidor de Administração.

- Distribuir políticas e tarefas de grupo através de multicasting usando UDP.

- Atua como um gateway para conexão ao Servidor de Administração para dispositivos em um grupo de administração.

  Se não for possível estabelecer uma conexão direta entre os dispositivos gerenciados no grupo e o Servidor de Administração, o ponto de distribuição pode ser usado como um gateway de conexão para o Servidor de Administração para esse grupo. Nesse caso, os dispositivos gerenciados serão conectados ao gateway de conexão, o qual, por sua vez, será conectado ao Servidor de Administração.

  A presença de um ponto de distribuição que opera como um gateway de conexão não bloqueia a opção de conexão direta entre os dispositivos gerenciados e o Servidor de Administração. Se o gateway de conexão não estiver disponível, mas a conexão direta com o Servidor de Administração for tecnicamente possível, os dispositivos gerenciados serão conectados ao Servidor de Administração diretamente.

- Faça a sondagem da rede para detectar novos dispositivos e para atualizar as informações sobre os existentes. Um ponto de distribuição pode aplicar os mesmos métodos de localização dos dispositivos que os do Servidor de Administração.

- Execute a instalação remota de aplicativos pela Kaspersky e outros fornecedores de software, incluindo a instalação em dispositivos clientes sem o Agente de Rede.

  Esse recurso permite a transferência remota de pacotes de instalação do Agente de Rede para dispositivos cliente localizados em redes às quais o Servidor de Administração não tem acesso direto.

- Atue como um servidor proxy participando da Kaspersky Security Network (KSN).

  Você pode ativar o servidor proxy da KSN no lado do ponto de distribuição para fazer o dispositivo funcionar como um servidor proxy da KSN. Neste caso, o serviço de proxy da KSN é executado no dispositivo.

Os Arquivos são transmitidos do Servidor de Administração a um ponto de distribuição através de HTTP ou, se a Conexão SSL estiver ativada, através de HTTPS. Usar HTTP ou HTTPS resulta em um desempenho mais alto, comparando com o SOAP, através da redução de tráfego.

Aos dispositivos com o Agente de Rede instalado podem ser atribuídos pontos de distribuição de forma manual (pelo administrador) ou automaticamente (pelo Servidor de Administração). A lista completa de pontos de distribuição para grupos de administração especificados é exibida no relatório na lista de pontos de distribuição.

O escopo de um ponto de distribuição é o grupo de administração ao qual ele foi atribuído pelo administrador, assim como seus subgrupos de todos os níveis de incorporação. Se múltiplos pontos de distribuição tiverem sido atribuídos na hierarquia de grupos de administração, o Agente de Rede do dispositivo gerenciado se conecta ao ponto de distribuição mais próximo na hierarquia.

Se os pontos de distribuição forem automaticamente atribuídos pelo Servidor de Administração, ele os atribui por domínios de difusão, não por grupos de administração. Isso ocorre quando todos os domínios de difusão são conhecidos. O Agente de Rede troca mensagens com outros Agentes de Rede na mesma sub-rede e, a seguir, envia informações ao Servidor de Administração sobre si mesmo e de outros Agentes de Rede. O Servidor de Administração usa estas informações para agrupar os Agentes de atualização por domínios de difusão. Os domínios de difusão são conhecidos para o Servidor de Administração após mais de 70% dos Agentes de rede nos grupos de administração forem amostrados. O Servidor de Administração efetua a sondagem dos domínios de difusão a cada duas horas. Após os pontos de distribuição terem sido atribuídos pelo domínio de difusão, eles não podem ser reatribuídos por grupos de administração.

Se o administrador atribuir manualmente pontos de distribuição, eles poderão ser atribuídos a grupos de administração ou locais de rede.

Os Agentes de Rede com um perfil de conexão ativo não participam na detecção do domínio de difusão.

O Kaspersky Security Center Linux atribui a cada Agente de Rede um endereço IP multicast único que se diferencia de cada outro endereço. Isto lhe permite evitar a sobrecarga de rede que poderia ocorrer devido a sobreposições de IP. Os endereços IP multicast que foram atribuídos em versões anteriores do aplicativo não serão modificados.

Quando dois ou mais pontos de distribuição forem atribuídos à uma única área de rede ou para um único grupo de administração, um deles se torna o ponto de distribuição ativo, e o restante deles se tornam pontos de distribuição em standby. O ponto de distribuição ativo baixa as atualizações e os pacotes de instalação diretamente do Servidor de Administração, enquanto os pontos de distribuição em standby recuperam as atualizações somente do ponto de distribuição ativo. Neste caso, após os arquivos terem sido baixados do Servidor de Administração eles são distribuídos entre os pontos de distribuição. Se o ponto de distribuição ativo se tornar indisponível por qualquer motivo, um dos pontos de distribuição independentes se torna ativo. O Servidor de Administração atribui automaticamente um ponto de distribuição para agir como standby.

O status do ponto de distribuição (*Ativo* / *Standby*) é exibido com uma caixa de seleção no relatório klnagchk.

Um ponto de distribuição requer ao menos 4 GB de espaço livre no disco. Caso o espaço disponível livre do ponto de distribuição seja menor do que 2 GB, o Kaspersky Security Center Linux cria um incidente de segurança com o nível de importância *Advertência*. O incidente de segurança será publicado nas propriedades do dispositivo, na seção **Problemas de segurança**.

Executar tarefas de instalação remota em um dispositivo atribuído como ponto de distribuição exige espaço livre adicional no disco. O volume do espaço em disco disponível livre deve exceder o tamanho total de todos os pacotes de instalação a ser instalados.

Executar qualquer tarefa de atualização (patch) e de correção de vulnerabilidades em um dispositivo atribuído como ponto de distribuição exige espaço livre adicional no disco. O volume do espaço em disco disponível livre deve ser pelo menos duas vezes o tamanho total de todos os patches a serem instalados.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Gateway de conexão

Um *gateway de conexão* é um Agente de Rede atuando em um modo especial. Um gateway de conexão aceita conexões de outros Agentes de Rede e os canaliza para o Servidor de Administração por meio de sua própria conexão com o Servidor. Ao contrário de um Agente de Rede comum, um gateway de conexão aguarda por conexões do Servidor de Administração, em vez de estabelecer conexões com o Servidor de Administração.

Um gateway de conexão pode receber conexões de até 10.000 dispositivos.

Você tem duas opções para usar gateways de conexão:

- Recomendamos instalar um gateway de conexão em uma zona desmilitarizada (DMZ). Para outros Agentes de Rede instalados em dispositivos externos, você precisa configurar especialmente uma conexão ao Servidor de Administração por meio do gateway de conexão.

  Um gateway de conexão não modifica ou processa de forma alguma os dados transmitidos dos Agentes de Rede para o Servidor de Administração. Além disso, ele não grava esses dados em nenhum buffer e, portanto, não pode aceitar dados de um Agente de Rede e posteriormente encaminhá-los ao Servidor de Administração. Se o Agente de Rede tentar se conectar ao Servidor de Administração através do gateway de conexão, mas esse não puder se conectar ao Servidor de Administração, o Agente de Rede interpretará isso como se o Servidor de Administração estivesse inacessível. Todos os dados permanecem no Agente de Rede (não no gateway de conexão).

  Um gateway de conexão não pode se conectar ao Servidor de Administração por meio de outro gateway de conexão. Isso significa que o Agente de Rede não pode ser simultaneamente um gateway de conexão e usar um gateway de conexão para se conectar ao Servidor de Administração.

Todos os gateways de conexão estão incluídos na lista de pontos de distribuição nas propriedades do Servidor de Administração.

- Você também pode usar gateways de conexão dentro da rede. Por exemplo, pontos de distribuição atribuídos automaticamente também se tornam gateways de conexão em seu próprio escopo. No entanto, em uma rede interna, os gateways de conexão não oferecem benefícios consideráveis. Eles reduzem o número de conexões de rede recebidas pelo Servidor de Administração, mas não reduzem o volume de dados de entrada. Mesmo sem gateways de conexão, todos os dispositivos ainda podem se conectar ao Servidor de Administração.

Servidores de Administração virtual

Com base em um Servidor de Administração físico, múltiplos Servidores de Administração virtuais podem ser criados, que serão semelhantes a Servidores de Administração secundários. Em comparação com o modelo de acesso discricionário, que tem base em listas de controle de acesso (ACLs), o modelo de Servidor de Administração virtual é mais funcional e fornece um maior grau de isolamento. Além de uma estrutura dedicada de grupos de administração para dispositivos atribuídos com políticas e tarefas, cada Servidor de Administração virtual apresenta seu próprio grupo de dispositivos não atribuídos, conjuntos próprios de relatórios, dispositivos e eventos selecionados, pacotes de instalação, regras de movimentação etc. O escopo funcional dos Servidores de Administração virtuais pode ser usado tanto por provedores de serviços (xSP) para maximizar o isolamento de clientes quanto por organizações de grande porte com fluxos de trabalho sofisticados e vários administradores.

Os Servidores de Administração virtuais são muito semelhantes aos Servidores de Administração secundários, mas com as seguintes distinções:

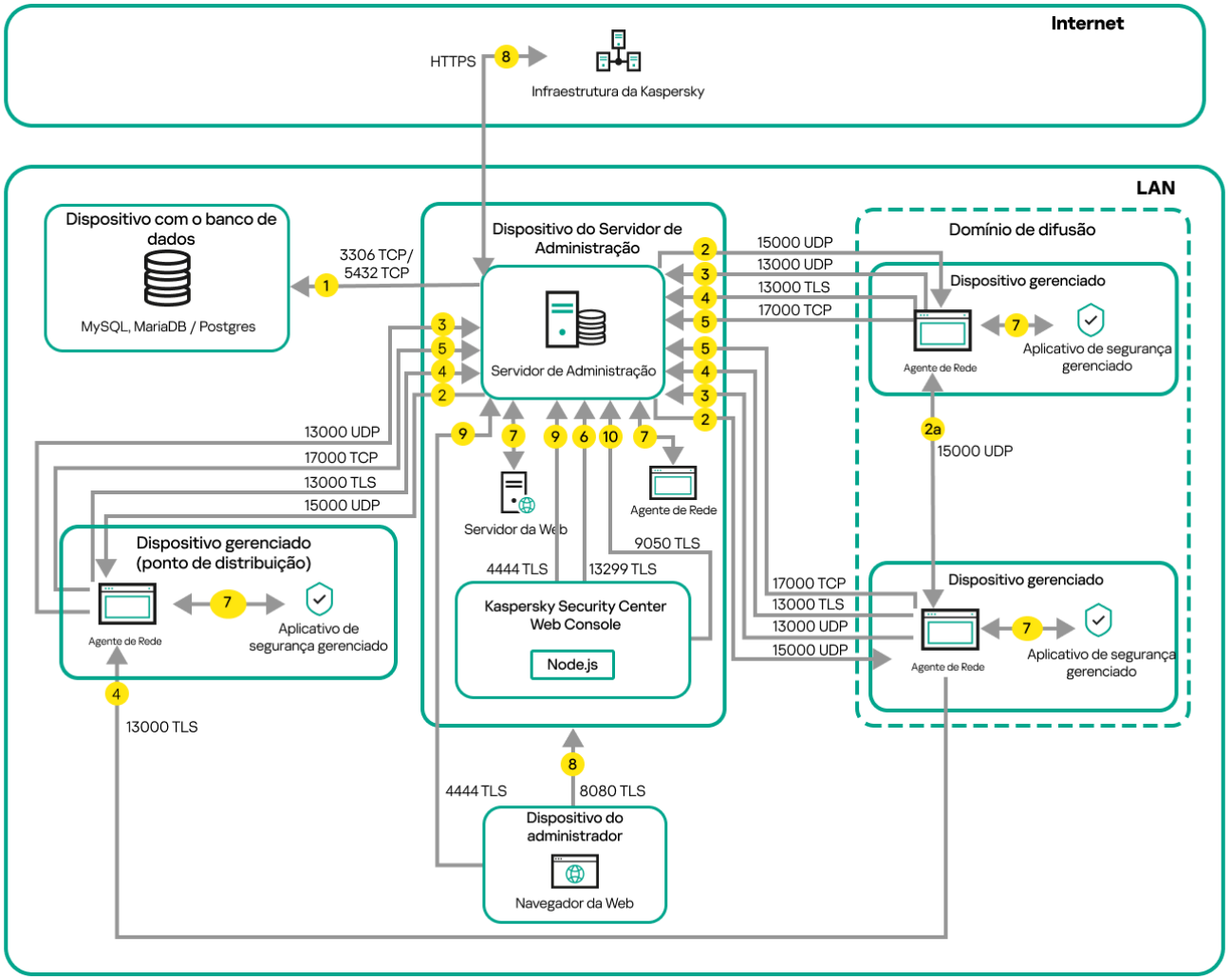
- Em um Servidor de Administração virtual falta a maior parte das configurações globais e as suas próprias portas TCP.
- Um Servidor de Administração virtual não tem Servidores de Administração secundários.
- Um Servidor de Administração virtual não tem outros Servidores de Administração virtuais.
- Um Servidor de Administração físico exibe dispositivos, grupos, eventos e objetos em dispositivos gerenciados (itens em Quarentena, registro de aplicativos e etc.) de todos os seus Servidores de Administração virtuais.
- Um Servidor de Administração virtual somente pode verificar a rede com pontos de distribuição conectados.

Esquemas para o tráfego de dados e uso de porta

Esta seção fornece esquemas para o tráfego de dados entre os componentes do Kaspersky Security Center Linux, aplicativos de segurança gerenciados e servidores externos sob diversas configurações. Os esquemas são fornecidos com o número de portas que precisam estar disponíveis nos dispositivos locais.

Servidor de Administração e dispositivos gerenciados em uma rede de área local (LAN)

A figura abaixo mostra o tráfego dos dados se o Kaspersky Security Center estiver implementado somente em uma rede de área local (LAN).



Servidor de Administração e dispositivos gerenciados em uma rede de área local (LAN)

A figura mostra como diferentes dispositivos gerenciados conectam-se ao Servidor de Administração de diferentes maneiras: diretamente ou via um ponto de distribuição. Os pontos de distribuição reduzem a carga no Servidor de Administração durante a distribuição da atualização e otimizam o tráfego de rede. No, entanto, os pontos de distribuição somente são necessários se o número de dispositivos gerenciados for suficientemente grande. Se o número de dispositivos gerenciados for pequeno, todos os dispositivos gerenciados recebem as atualizações diretamente do Servidor de Administração.

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração seja instalado e o banco de dados esteja em dispositivos diferentes, será preciso disponibilizar as portas necessárias no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server e MariaDB Server ou porta 5432 para PostgreSQL Server ou Postgres Pro Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

   2a. Os Agentes de Rede em dispositivos gerenciados não móveis trocam dados sobre outros Agentes de Rede dentro do mesmo domínio de difusão (os dados são, então, enviados ao Servidor de Administração).

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. O Kaspersky Security Center Web Console Server envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

   O componente Identity and Access Manager (IAM) se conecta ao Servidor de Administração pela porta TLS 13299.

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

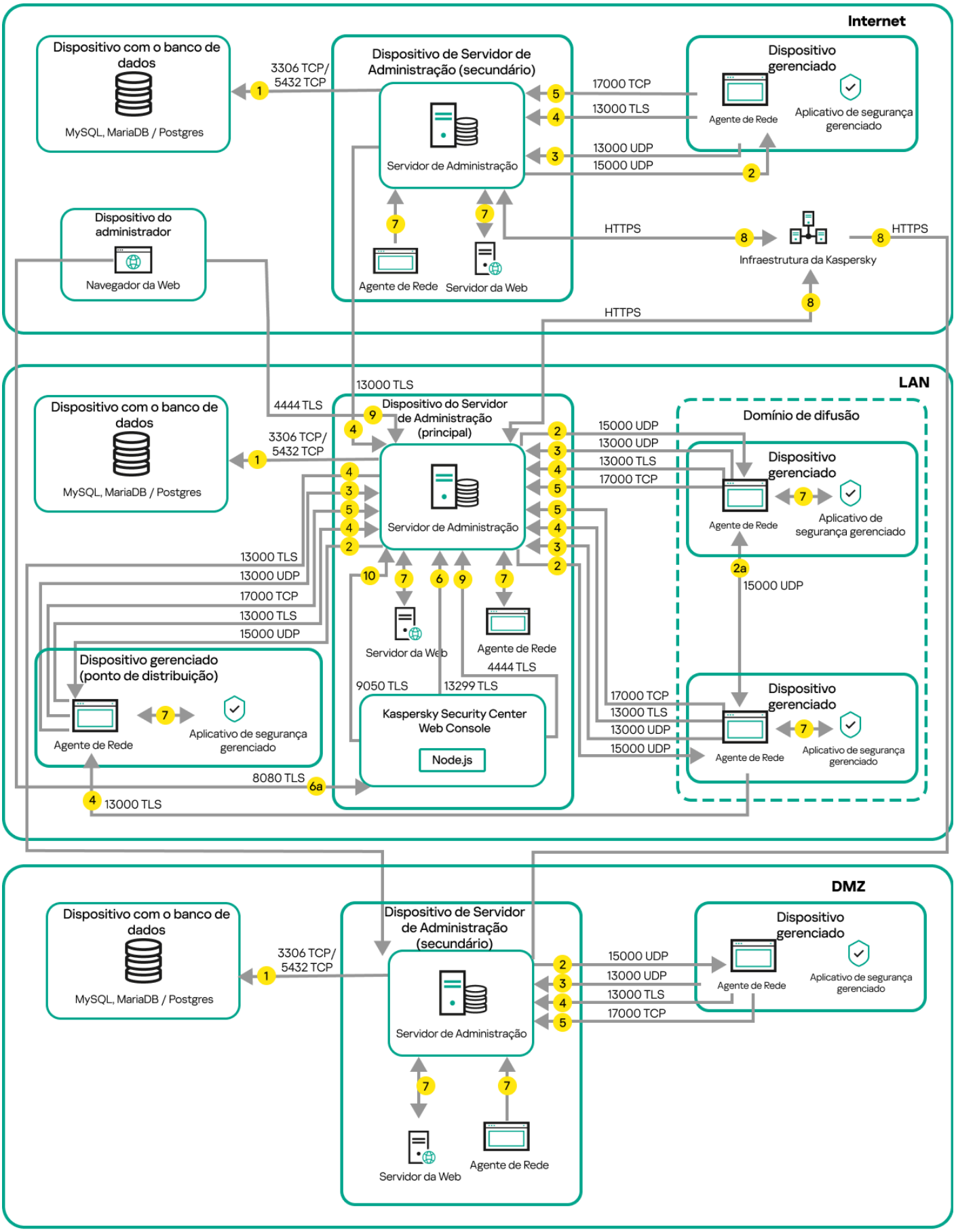
   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. O Kaspersky Security Center Web Console Server e o navegador (utilizado com o Kaspersky Security Center Web Console) se conectam ao Servidor de Administração usando o protocolo de autenticação OpenID Connect pela porta TLS 4444.

10. O Kaspersky Security Center Web Console Server se conecta ao Servidor de Administração pela porta TLS 9050.

Servidor de Administração principal dentro da rede de área local e dois Servidores de Administração secundários

A figura abaixo mostra a hierarquia dos Servidores de Administração: o Servidor de Administração principal está na rede de área local (LAN). Um Servidor de Administração secundário encontra-se na zona desmilitarizada (DMZ); outros Servidores de Administração secundários estão na Internet.



Hierarquia de Servidores de Administração: Servidor de Administração principal e dois Servidores de Administração secundários

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração seja instalado e o banco de dados esteja em dispositivos diferentes, será preciso disponibilizar as portas necessárias no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server e MariaDB Server ou porta 5432 para PostgreSQL Server ou Postgres Pro Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center Linux também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. O Kaspersky Security Center Web Console Server envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

   O componente Identity and Access Manager (IAM) se conecta ao Servidor de Administração pela porta TLS 13299.

   6a. O dados do navegador, que está instalado em um dispositivo separado do administrador, são transferidos ao Kaspersky Security Center Web Console Server através da porta 8080 TLS. O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

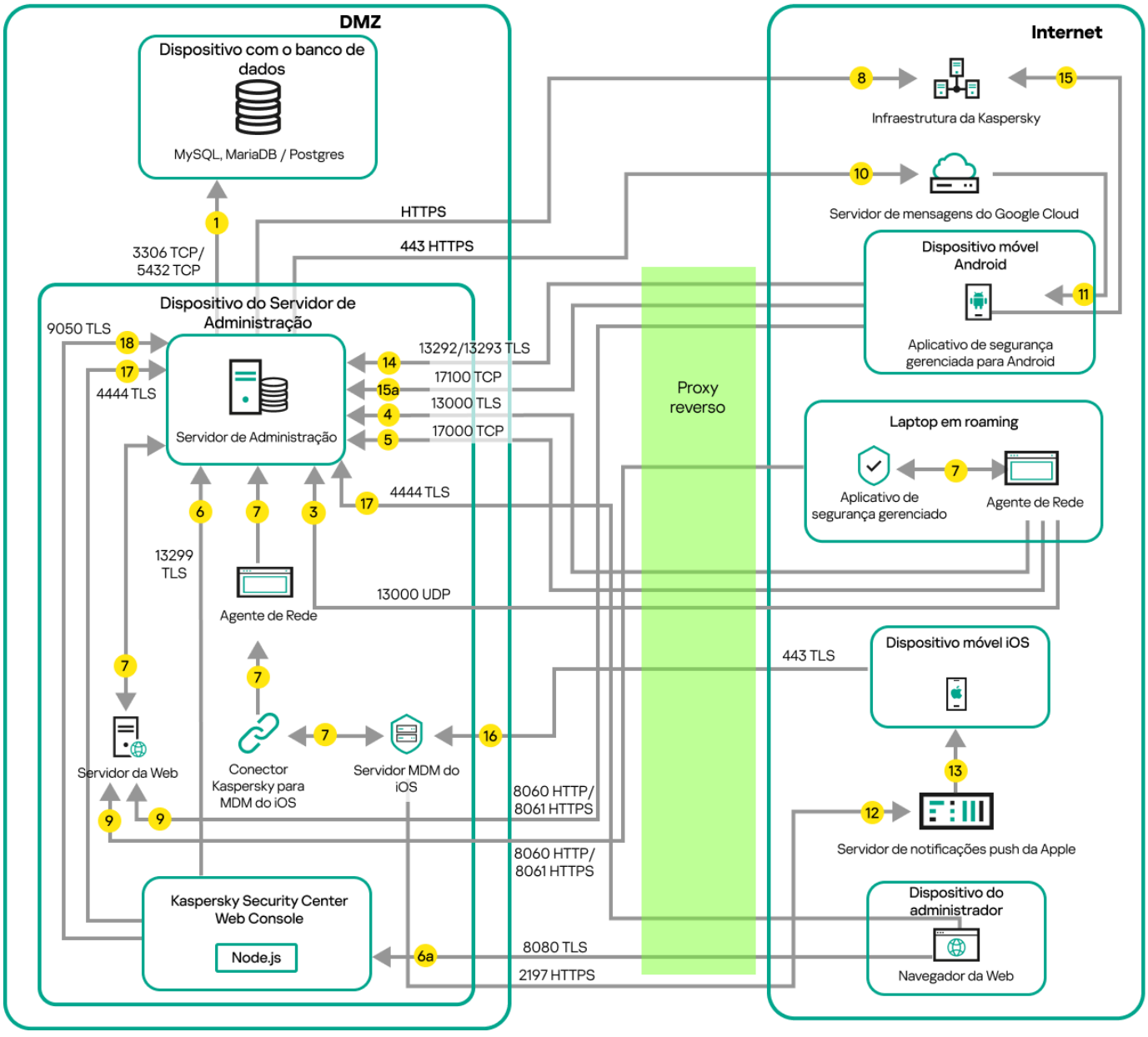
   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. O Kaspersky Security Center Web Console Server e o navegador (utilizado com o Kaspersky Security Center Web Console) se conectam ao Servidor de Administração usando o protocolo de autenticação OpenID Connect pela porta TLS 4444.

10. O Kaspersky Security Center Web Console Server se conecta ao Servidor de Administração pela porta TLS 9050.

Servidor de Administração na LAN, dispositivos gerenciados na Internet, proxy reverso em uso

A figura abaixo exibe o tráfego de dados caso o Servidor de Administração esteja dentro da rede de área local (LAN), e se os dispositivos gerenciados estiverem na Internet. Nesta figura, um proxy reverso de sua escolha está em uso. Consulte a documentação dos aplicativos correspondentes para saber mais detalhes.



Servidor de Administração em uma rede local; dispositivos gerenciados estabelecem conexão com o Servidor de Administração por meio de um proxy reverso

Este esquema de implementação é recomendado se você não deseja que os dispositivos móveis se conectem ao Servidor de Administração diretamente e não deseja atribuir um gateway de conexão na DMZ.

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração seja instalado e o banco de dados esteja em dispositivos diferentes, será preciso disponibilizar as portas necessárias no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server e MariaDB Server ou porta 5432 para PostgreSQL Server ou Postgres Pro Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center Linux também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. O Kaspersky Security Center Web Console Server envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

   O componente Identity and Access Manager (IAM) se conecta ao Servidor de Administração pela porta TLS 13299.

   6a. O dados do navegador, que está instalado em um dispositivo separado do administrador, são transferidos ao Kaspersky Security Center Web Console Server através da porta 8080 TLS. O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. Solicitações por pacotes feitas por dispositivos gerenciados, incluindo dispositivos móveis, são transferidas para o Servidor Web, que está no mesmo dispositivo onde está o Servidor de Administração.

10. Somente para dispositivos Android: os dados do Servidor de Administração são transferidos para os servidores da Google. Esta conexão é usada para notificar os dispositivos móveis Android de que precisam se conectar ao Servidor de Administração. As notificações push são enviadas para os dispositivos móveis.

11. Somente para dispositivos móveis Android: as notificações push dos servidores da Google são enviadas para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis de que precisam se conectar ao Servidor de Administração.

12. Somente para dispositivos móveis iOS: os dados do Servidor de MDM do iOS são transferidos para os servidores Apple Push Notification. As notificações push são enviadas para os dispositivos móveis.

13. Somente para dispositivos móveis iOS: as notificações push são enviadas dos servidores da Apple para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis iOS de que precisam se conectar com o Servidor de MDM do iOS.

14. Somente para dispositivos móveis: os dados do aplicativo gerenciado são transferidos para o Servidor de Administração (ou para o gateway de conexão) por meio da porta TLS 13292/13293, diretamente ou por um proxy reverso.

15. Somente para dispositivos móveis: os dados do dispositivo móvel são transferidos para a infraestrutura da Kaspersky.

    Se o dispositivo móvel não tiver acesso à Internet, os dados são transferidos para o Servidor de Administração pela porta 17100, e o Servidor de Administração os envia para a infraestrutura da Kaspersky. No entanto, este cenário é raramente usado.

16. Somente para dispositivos iOS: os dados do dispositivo móvel são transferidos através da porta 443 TLS para o Servidor de MDM do iOS, que está no mesmo dispositivo que o Servidor de Administração.

17. O Kaspersky Security Center Web Console Server e o navegador (utilizado com o Kaspersky Security Center Web Console) se conectam ao Servidor de Administração usando o protocolo de autenticação OpenID Connect pela porta TLS 4444.

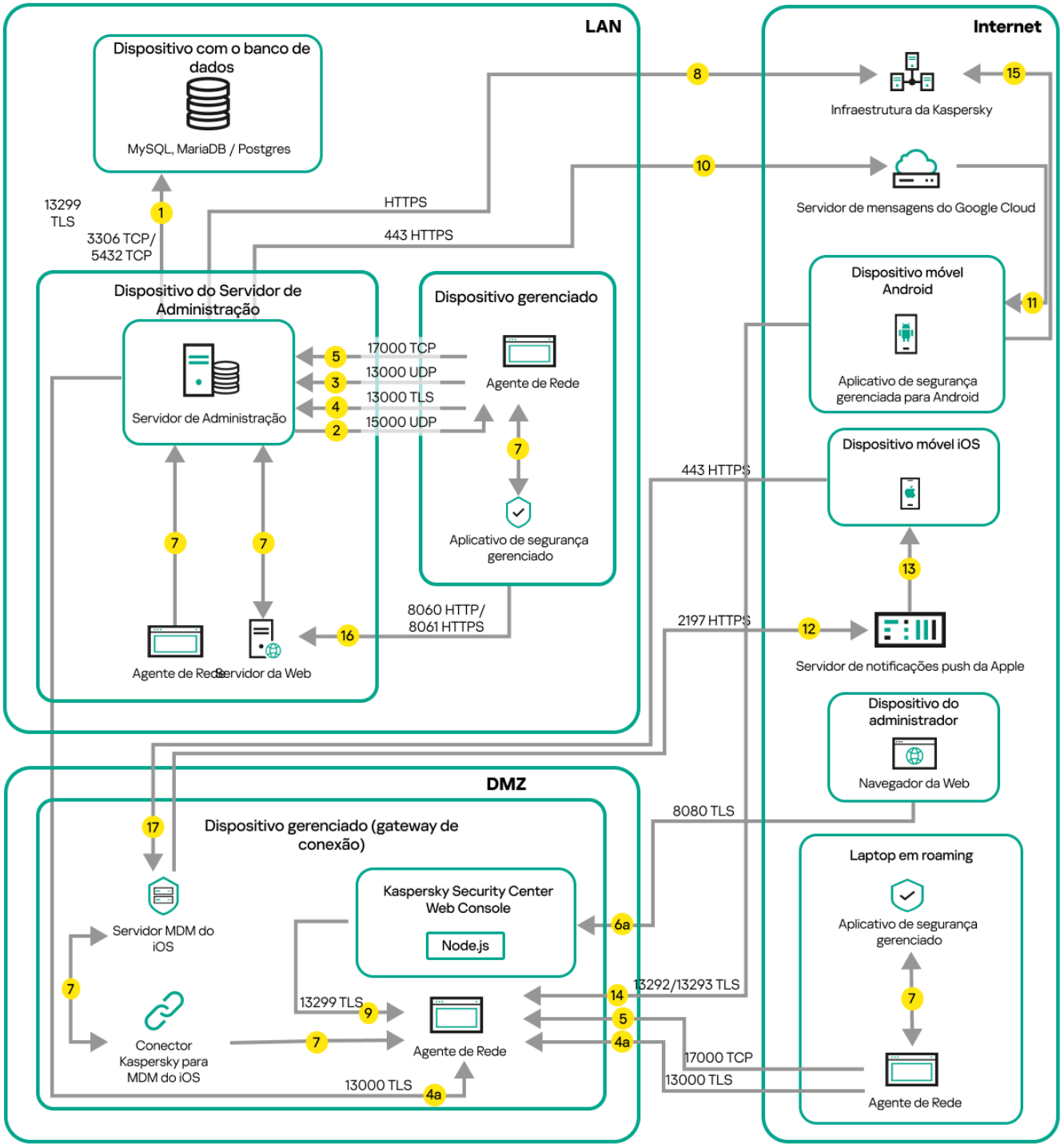
18. O Kaspersky Security Center Web Console Server se conecta ao Servidor de Administração pela porta TLS 9050.

Servidor de Administração dentro da LAN, dispositivos gerenciados na Internet, e o gateway de conexão em uso

A figura abaixo exibe o tráfego de dados caso o Servidor de Administração esteja dentro da rede de área local (LAN), e se os dispositivos gerenciados estiverem na Internet. O gateway de conexão está em uso.

Este esquema de implementação é recomendado caso não se queira que os dispositivos gerenciados se conectem diretamente com o Servidor de Administração e não se queira usar um proxy reverso ou firewall corporativo.

Para este esquema de implementação, a autenticação do domínio (conexão única) fornecida pelo Identity and Access Manager (IAM) não é compatível.



Gerenciar dispositivos móveis conectados com o Servidor de Administração através de um gateway de conexão

Nesta figura, os dispositivos gerenciados estão conectados com o Servidor de Administração através de um gateway de conexão que está localizado na DMZ. Nenhum proxy reverso ou firewall corporativo está em uso.

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração seja instalado e o banco de dados esteja em dispositivos diferentes, será preciso disponibilizar as portas necessárias no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server e MariaDB Server ou porta 5432 para PostgreSQL Server ou Postgres Pro Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center Linux também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

   4a. Um gateway de conexão na DMZ também recebe a conexão do Servidor de Administração por meio da porta TLS 13000. Como um gateway de conexão na DMZ não pode alcançar as portas do Servidor de Administração, o Servidor de Administração cria e mantém uma conexão de sinal permanente com um gateway de conexão. A conexão de sinal não é usada para transferência de dados, mas apenas para enviar um convite para a interação de rede. Quando o gateway de conexão precisa se conectar ao Servidor, notifica o Servidor por meio dessa conexão de sinal e, em seguida, o Servidor cria a conexão necessária para a transferência de dados.

   Os dispositivos externos também se conectam ao gateway de conexão por meio da porta TLS 13000.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. O Kaspersky Security Center Web Console Server envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

   6a. O dados do navegador, que está instalado em um dispositivo separado do administrador, são transferidos ao Kaspersky Security Center Web Console Server através da porta 8080 TLS. O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. Solicitações por pacotes feitas por dispositivos gerenciados, incluindo dispositivos móveis, são transferidas para o Servidor Web, que está no mesmo dispositivo onde está o Servidor de Administração.

10. Somente para dispositivos Android: os dados do Servidor de Administração são transferidos para os servidores da Google. Esta conexão é usada para notificar os dispositivos móveis Android de que precisam se conectar ao Servidor de Administração. As notificações push são enviadas para os dispositivos móveis.

11. Somente para dispositivos móveis Android: as notificações push dos servidores da Google são enviadas para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis de que precisam se conectar ao Servidor de Administração.

12. Somente para dispositivos móveis iOS: os dados do Servidor de MDM do iOS são transferidos para os servidores Apple Push Notification. As notificações push são enviadas para os dispositivos móveis.

13. Somente para dispositivos móveis iOS: as notificações push são enviadas dos servidores da Apple para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis iOS de que precisam se conectar com o Servidor de MDM do iOS.

14. Somente para dispositivos móveis: os dados do aplicativo gerenciado são transferidos para o Servidor de Administração (ou para o gateway de conexão) por meio da porta TLS 13292/13293, diretamente ou por um proxy reverso.

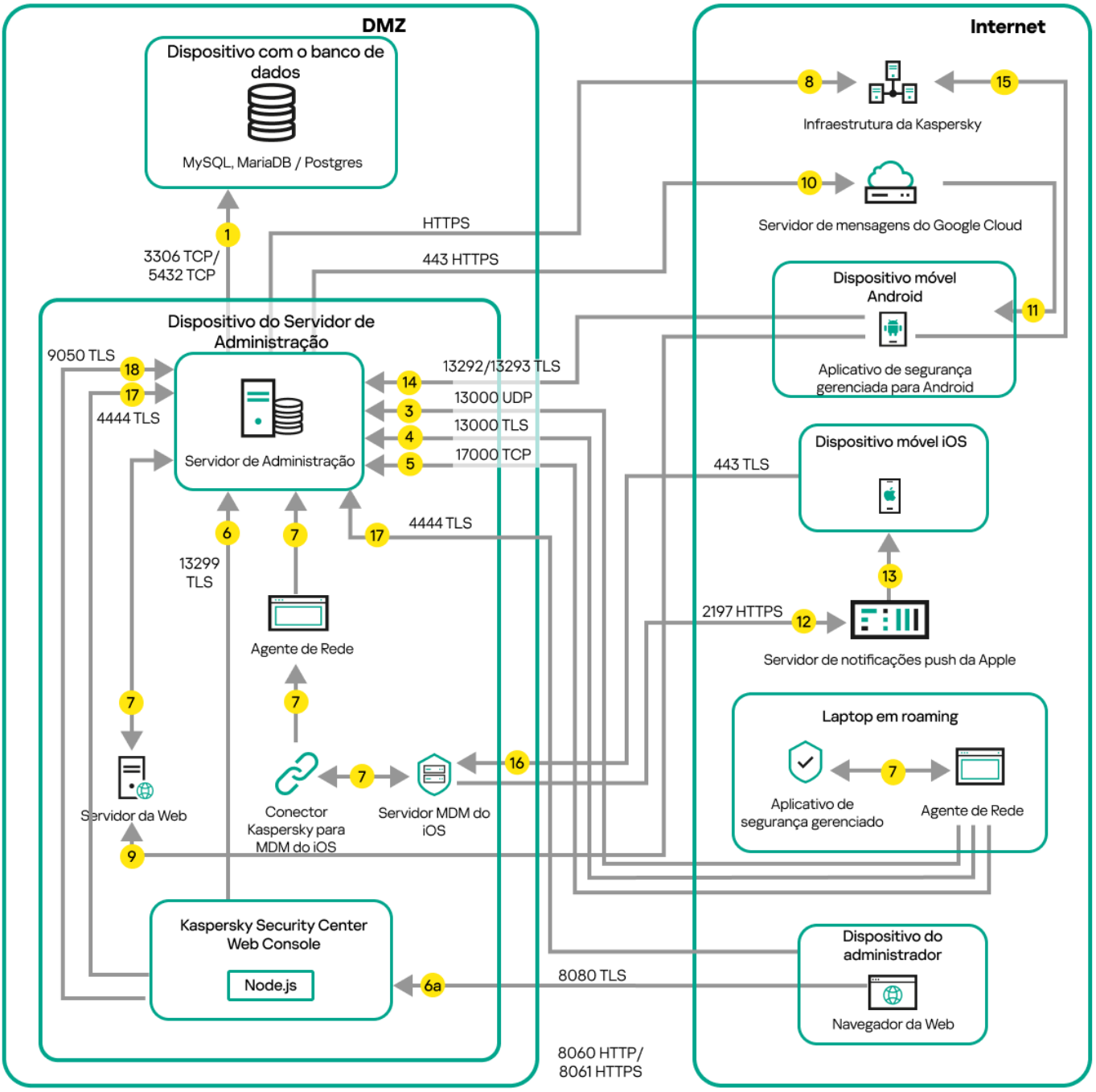
15. Somente para dispositivos móveis: os dados do dispositivo móvel são transferidos para a infraestrutura da Kaspersky.

    Se o dispositivo móvel não tiver acesso à Internet, os dados são transferidos para o Servidor de Administração pela porta 17100, e o Servidor de Administração os envia para a infraestrutura da Kaspersky. No entanto, este cenário é raramente usado.

16. Somente para dispositivos iOS: os dados do dispositivo móvel são transferidos através da porta 443 TLS para o Servidor de MDM do iOS, que está no mesmo dispositivo que o Servidor de Administração.

Servidor de Administração dentro do DMZ, dispositivos gerenciados na Internet

A figura abaixo mostra o tráfego de dados se o Servidor de Administração estiver dentro da zona desmilitarizada (DMZ) e os dispositivos gerenciados estiverem na Internet.



O Servidor de Administração na DMZ, dispositivos móveis gerenciados na Internet

Nesta figura, nenhum gateway de conexão está em uso: os dispositivos móveis se conectam diretamente ao Servidor de Administração.

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração seja instalado e o banco de dados esteja em dispositivos diferentes, será preciso disponibilizar as portas necessárias no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server e MariaDB Server ou porta 5432 para PostgreSQL Server ou Postgres Pro Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center Linux também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. O Kaspersky Security Center Web Console Server envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

   O componente Identity and Access Manager (IAM) se conecta ao Servidor de Administração pela porta TLS 13299.

   6a. O dados do navegador, que está instalado em um dispositivo separado do administrador, são transferidos ao Kaspersky Security Center Web Console Server através da porta 8080 TLS. O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. As solicitações de pacotes de dispositivos gerenciados são transferidas para o Servidor Web, que está no mesmo dispositivo onde está o Servidor de Administração.

10. Somente para dispositivos Android: os dados do Servidor de Administração são transferidos para os servidores da Google. Esta conexão é usada para notificar os dispositivos móveis Android de que precisam se conectar ao Servidor de Administração. As notificações push são enviadas para os dispositivos móveis. O serviço FCM também é executado na porta 443 HTTPS.

11. Somente para dispositivos móveis Android: as notificações push dos servidores da Google são enviadas para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis de que precisam se conectar ao Servidor de Administração.

12. Somente para dispositivos móveis iOS: os dados do Servidor de MDM do iOS são transferidos para os servidores Apple Push Notification. As notificações push são enviadas para os dispositivos móveis.

13. Somente para dispositivos móveis iOS: as notificações push são enviadas dos servidores da Apple para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis iOS de que precisam se conectar com o Servidor de MDM do iOS.

14. Somente para dispositivos móveis: os dados do aplicativo gerenciado são transferidos para o Servidor de Administração (ou para o gateway de conexão) por meio da porta TLS 13292/13293, diretamente ou por um proxy reverso.

15. Somente para dispositivos móveis: os dados do dispositivo móvel são transferidos para a infraestrutura da Kaspersky.

    Se o dispositivo móvel não tiver acesso à Internet, os dados são transferidos para o Servidor de Administração pela porta 17100, e o Servidor de Administração os envia para a infraestrutura da Kaspersky. No entanto, este cenário é raramente usado.

16. Somente para dispositivos iOS: os dados do dispositivo móvel são transferidos através da porta 443 TLS para o Servidor de MDM do iOS, que está no mesmo dispositivo que o Servidor de Administração.

17. O Kaspersky Security Center Web Console Server e o navegador (utilizado com o Kaspersky Security Center Web Console) se conectam ao Servidor de Administração usando o protocolo de autenticação OpenID Connect pela porta TLS 4444.

18. O Kaspersky Security Center Web Console Server se conecta ao Servidor de Administração pela porta TLS 9050.

Interação dos componentes e aplicativos de segurança do Kaspersky Security Center Linux: mais informações

Esta seção fornece os esquemas para a interação de componentes do Kaspersky Security Center Linux e aplicativos de segurança gerenciados. Os esquemas fornecem os números das portas que devem estar disponíveis e os nomes dos processos que abrem aquelas portas.

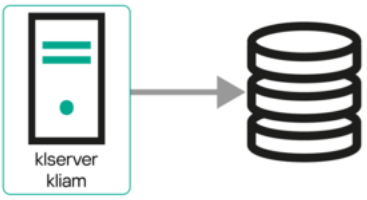
Convenções usadas em esquemas de interação

A tabela a seguir fornece as convenções usadas através dos esquemas.

Ícone	Valor
	Servidor de Administração
	Servidor de Administração secundário
	DBMS
	O dispositivo cliente (que tem o Agente de Rede e um aplicativo da família do Kaspersky Endpoint Security instalado ou que tem um aplicativo de segurança diferente do Kaspersky Security Center Linux pode gerenciar)
	Gateway de conexão
	Ponto de distribuição
	Navegador no dispositivo do usuário
	Processo em execução no dispositivo e abrir uma porta
	Porta e seu número
	Tráfego TCP (a direção da seta mostra a direção do fluxo de tráfego)
	Tráfego UDP (a direção da seta mostra a direção do fluxo de tráfego)
	Transporte de DBMS
	Limite de DMZ

Servidor de Administração e DBMS

Os dados do Servidor de Administração e do Identity and Access Manager (IAM) são armazenados em bancos de dados separados dentro do mesmo DBMS.



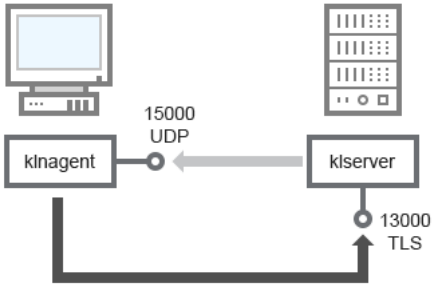
Servidor de Administração, Identity and Access Manager e DBMS

Caso o Servidor de Administração e o banco de dados sejam instalados em dispositivos diferentes, será necessário disponibilizar as portas necessárias no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MariaDB Server). Consulte a documentação do DBMS para obter informações relevantes.
A porta para conectar o IAM ao DBMS é especificada por um usuário durante a instalação do Kaspersky Security Center Linux.

O Servidor de Administração não faz a remoção automática do banco de dados do Servidor de Administração e do banco de dados do IAM ao desinstalar ou mover o servidor para outro dispositivo. Se necessário, você deve remover os bancos de dados manualmente.

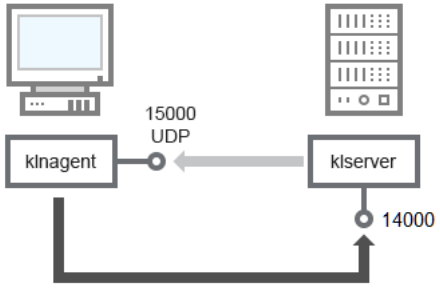
Servidor de Administração e dispositivo cliente: Gerenciar o aplicativo de segurança

O Servidor de Administração recebe a conexão dos Agentes de Rede pela porta TLS 13000 (veja a figura abaixo).



Servidor de Administração e dispositivo cliente: gerenciando o aplicativo de segurança, conexão através da porta 13000 (recomendado)

Caso tenha usado uma versão anterior do Kaspersky Security Center Linux, o Servidor de Administração na sua rede poderá receber as conexões dos Agentes de Rede pela porta não SSL 14000 (veja a figura abaixo). O Kaspersky Security Center Linux também é compatível com a conexão do Agente de Rede pela porta 14000, embora o uso da porta SSL 13000 seja o recomendado.



Servidor de Administração e dispositivo cliente: gerenciando o aplicativo de segurança, conexão através da porta 14000 (segurança mais baixa)

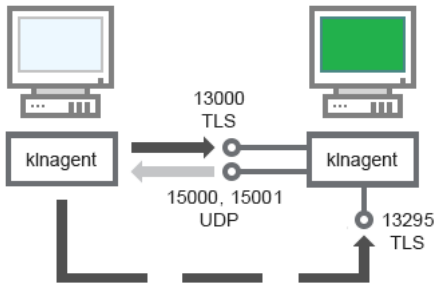
Para obter a clarificação dos esquemas, consulte a tabela abaixo.

Servidor de Administração e dispositivo cliente: Gerenciar o aplicativo de segurança (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta
Agente de Rede	15000	klnagent	UDP	Multicasting para Agente de Rede
Servidor de Administração	13000	klserver	TCP (TLS)	Receber conexões dos Agentes de Rede
Servidor de Administração	14000	klserver	TCP	Receber conexões dos Agentes de Rede

Atualizar o software em um dispositivo cliente através de uma ponto de distribuição

O dispositivos cliente conecta-se ao ponto de distribuição via porta 13000 e, se você estiver usando um ponto de distribuição como servidor push, também via porta 13295. O ponto de distribuição efetua uma transmissão multicast para os Agentes de Rede via port 15000 (ver figura abaixo). Atualizações e pacotes de instalação são recebidos de um ponto de distribuição pela porta 15001.



Atualizar o software em um dispositivo cliente através de uma ponto de distribuição

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Atualizar o software através de um ponto de distribuição (tráfego)

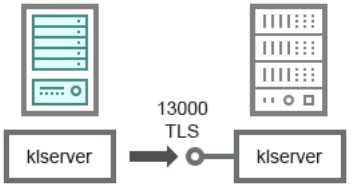
Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta
Agente de Rede	15000	klnagent	UDP	Multicasting para Agente de Rede
Agente de Rede	15001	klnagent	UDP	Recebendo atualizações e pacotes de instalação de um ponto de distribuição

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta
Ponto de distribuição	13000	klnagent	TCP (TLS)	Receber conexões dos Agentes de Rede
Ponto de distribuição	13295	klnagent	TCP (TLS)	Recebendo conexões de dispositivos cliente (push do servidor)

Hierarquia de Servidores de Administração: Servidor de Administração principal e Servidor de Administração secundário

O esquema (veja a figura abaixo) mostra como usar a porta 13000 para assegurar a interação entre os Servidores de Administração combinados em uma hierarquia.

Na sequência, quando os Servidores de Administração são combinados em uma hierarquia, é possível administrá-los com o uso do Kaspersky Security Center Web Console conectado ao Servidor de Administração principal. Portanto, a acessibilidade da porta 13299 do Servidor de Administração principal é o único prerrequisito.



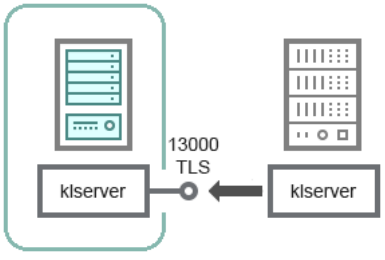
Hierarquia de Servidores de Administração: Servidor de Administração principal e Servidor de Administração secundário

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Hierarquia de Servidores de Administração (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta
Servidor de Administração principal	13000	klserver	TCP (TLS)	Receber conexões dos Servidores de Administração secundários

Hierarquia de Servidores de Administração com um Servidor de Administração secundário na DMZ



Hierarquia de Servidores de Administração com um Servidor de Administração secundário na DMZ

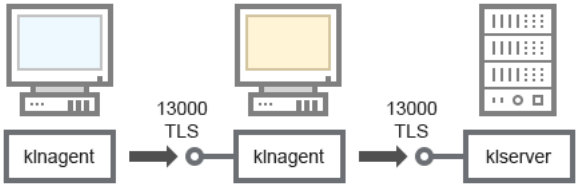
O esquema mostra uma hierarquia de Servidores de Administração nos quais o Servidor de Administração secundário localizado na DMZ recebe uma conexão do Servidor de Administração principal (consulte a tabela abaixo para obter explicações sobre o esquema). Ao combinar dois Servidores de Administração em uma hierarquia, garanta que a porta 13299 esteja acessível em ambos os Servidores de Administração. O Kaspersky Security Center Web Console se conecta a um Servidor de Administração usando a porta 13299.

Na sequência, quando os Servidores de Administração são combinados em uma hierarquia, é possível administrá-los com o uso do Kaspersky Security Center Web Console conectado ao Servidor de Administração principal. Portanto, a acessibilidade da porta 13299 do Servidor de Administração principal é o único prerrequisito.

Hierarquia de Servidores de Administração com um Servidor de Administração de secundário na DMZ (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta
Servidor de Administração secundário	13000	klserver	TCP (TLS)	Recebendo conexões do Servidor de Administração principal

Servidor de Administração, um gateway de conexão em um segmento da rede e um dispositivo cliente



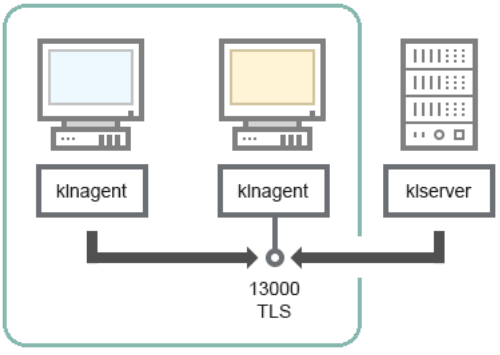
Servidor de Administração, um gateway de conexão em um segmento da rede e um dispositivo cliente

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Servidor de Administração, um gateway de conexão em um segmento da rede e um dispositivo cliente (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta
Servidor de Administração	13000	klserver	TCP (TLS)	Receber conexões dos Agentes de Rede
Agente de Rede	13000	klnagent	TCP (TLS)	Receber conexões dos Agentes de Rede

Servidor de Administração e dois dispositivos na DMZ: um gateway de conexão e um dispositivo cliente



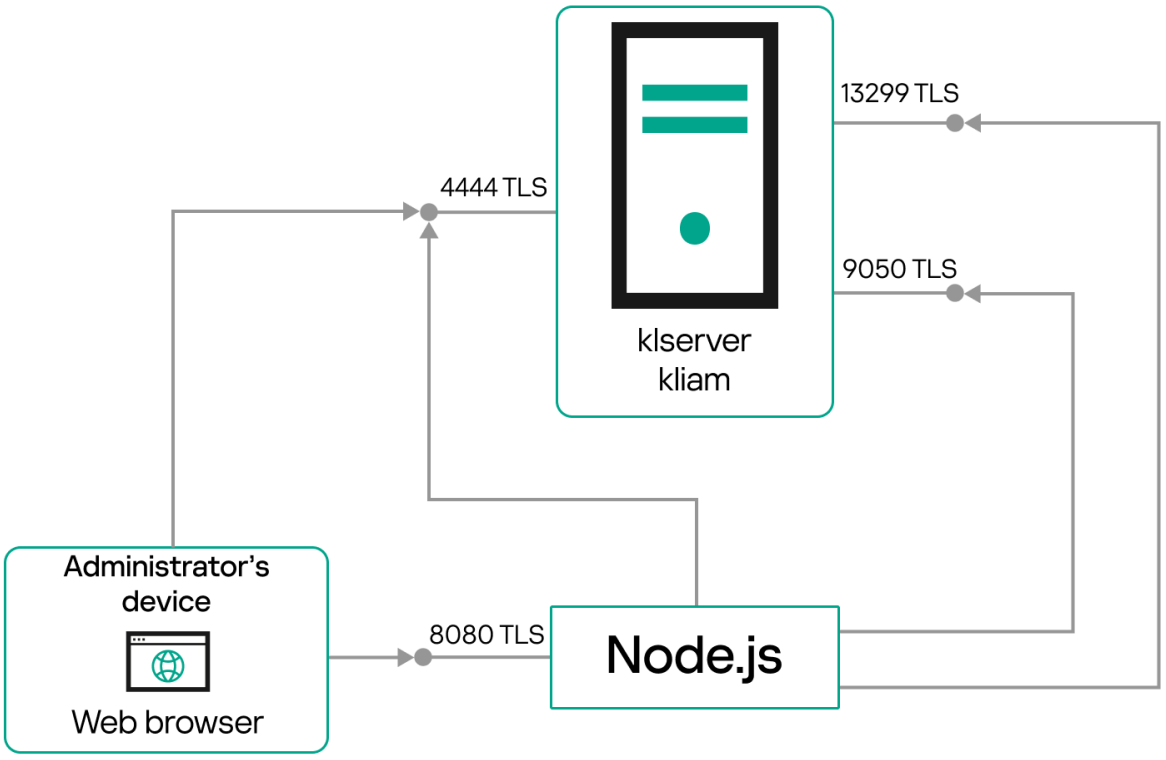
Servidor de Administração com um gateway de conexão e um dispositivo cliente em DMZ

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Servidor de Administração, um gateway de conexão em um segmento da rede e um dispositivo cliente (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta
Agente de Rede	13000	klnagent	TCP (TLS)	Receber conexões dos Agentes de Rede

Servidor de Administração e Kaspersky Security Center Web Console



Servidor de Administração e Kaspersky Security Center Web Console

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Servidor de Administração e Kaspersky Security Center Web Console (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta
Servidor de Administração	13299	klserver	TCP (TLS)	Recebimento de conexões do Kaspersky Security Center Web Console e do Identity and Access Manager (IAM) para o Servidor de Administração pela OpenAPI
Kaspersky Security Center Web Console Server ou Servidor de Administração	8080	Node.js: JavaScript do lado do servidor	TCP (TLS)	Receber conexões do Kaspersky Security Center Web Console
Servidor de Administração	4444	kliam	TCP (TLS)	Recebimento de conexões do Servidor Web do Kaspersky Security Center e do navegador (utilizado com o Kaspersky Security Center Web Console) para o Servidor de Administração com o IAM sobre o protocolo de autenticação OpenID Connect
Servidor de Administração	9050	kliam	TCP (TLS)	Recebimento de conexões do Kaspersky Security Center Web Console para o IAM

O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

Guia de Introdução

Seguindo este cenário, é possível instalar o Servidor de Administração do Kaspersky Security Center Linux e o Kaspersky Security Center Web Console, executar a configuração inicial do Servidor de Administração usando o assistente de início rápido e instalar aplicativos Kaspersky nos dispositivos gerenciados usando o assistente de implementação da proteção.

Pré-requisitos

Você deve ter uma chave de licença (código de ativação) para o Kaspersky Endpoint Security for Business ou chaves de licença (códigos de ativação) para os aplicativos de segurança Kaspersky.

Se deseja testar primeiro o Kaspersky Security Center Linux, é possível obter uma avaliação gratuita de 30 dias no site da Kaspersky.

Fases

O cenário principal de implementação ocorre nas seguintes fases:

1 Selecionar uma estrutura para a proteção de uma empresa

Saiba mais sobre os componentes do Kaspersky Security Center Linux. Com base na configuração da rede e na produtividade dos canais de comunicação, defina o número de Servidores de Administração a serem usados e como eles devem ser distribuídos entre seus escritórios (se você executar uma rede distribuída). Siga as recomendações para escolher a estrutura da rede.

Defina se uma hierarquia de Servidores de Administração será usada na sua organização. Para fazer isto, você deve avaliar se é possível e conveniente cobrir todos os dispositivos clientes com um único Servidor de Administração ou se é necessário criar uma hierarquia de Servidores de Administração.

2 Preparação para o uso de certificados personalizados

Se a infraestrutura de chave pública (PKI) da sua organização exige que você use certificados personalizados emitidos por uma autoridade de certificação (CA) específica, prepare esses certificados e garanta que eles atendam a todos os requisitos.

3 Configurar o acesso à rede

Configure a interação entre os componentes na rede da sua organização de acordo com a estrutura de proteção escolhida na etapa 1.

Para fazer isso, você deve:

- Abra o acesso à rede conforme necessário.
- Garanta a possibilidade de conexão com os servidores da Kaspersky ou estabeleça um fluxo de trabalho de atualização com uma fonte de atualização diferente.
- Para conectar os dispositivos gerenciados ao Servidor de Administração pela Internet, configure o acesso por meio de gateways de conexão ou coloque o Servidor de Administração na DMZ.

4 Dimensionar o equipamento e planejar a instalação dos componentes

Se você pretende instalar todos os componentes do Kaspersky Security Center Linux no mesmo servidor, use os cálculos de dimensionamento prontos disponíveis no arquivo de configurações do script de instalação rápida (klfi_netsize). Certifique-se de que todos os requisitos para usar o script de implementação automatizada de componentes sejam adequados à sua infraestrutura.

Caso contrário, faça um cálculo completo do dimensionamento de hardware para o Servidor de Administração, o DBMS e o Web Console, levando em consideração os requisitos de hardware e software e a seção sobre o cálculo dos recursos de hardware para implementar a solução manualmente, componente por componente.

Para aumentar o nível de proteção do Kaspersky Security Center Linux, inclua nos cálculos os requisitos de hardware do aplicativo Kaspersky Endpoint Security for Linux.

5 Instalar os componentes do Kaspersky Security Center Linux

Instale um sistema operacional compatível com o Servidor de Administração e o Kaspersky Security Center Web Console nos dispositivos de destino nos quais você deseja implementar a solução.

Instale o Kaspersky Security Center Linux de acordo com o tipo de implementação planejada:

- Usando o script de instalação rápida automatizada.
- Seguindo as instruções para a instalação e configuração manuais dos componentes Servidor de Administração e Web Console.

6 Instalando o Kaspersky Endpoint Security para Linux e Agente de Rede no dispositivo do Servidor de Administração

Por padrão, o aplicativo não considera o dispositivo do Servidor de Administração como um dispositivo gerenciado. Para proteger o Servidor de Administração e gerenciar esse dispositivo, instale o Kaspersky Endpoint Security for Linux e o Agente de Rede para Linux no dispositivo do Servidor de Administração. Nesse caso, o Agente de Rede para Linux é instalado e funciona independentemente da versão do servidor do Agente de Rede que você instalou junto com o Administration Server.

Gerencie as configurações de segurança necessárias para o Kaspersky Security Center Linux de acordo com as recomendações da Ajuda do Kaspersky Endpoint Security for Linux.

Para obter detalhes, consulte a etapa "Configurar a proteção antivírus do Servidor de Administração" na seção que apresenta o cenário de migração para o Kaspersky Security Center Linux usando o script de instalação rápida.

7 Execução da configuração inicial

Quando você se conecta ao Servidor de Administração por meio do Web Console pela primeira vez, o assistente de início rápido é iniciado automaticamente.

Durante a etapa de configuração inicial, o assistente usa as configurações padrão para criar as políticas e tarefas que são necessárias para implementar a proteção. No entanto, as configurações padrão podem ser menos ótimas para as necessidades da sua organização. Se necessário, você pode editar as configurações das políticas e tarefas.

8 Localização de dispositivos na rede

Configure e faça a sondagem da rede para descobrir os dispositivos manualmente. O Kaspersky Security Center Linux recebe os endereços e os nomes de todos os dispositivos detectados na rede. Você então pode usar o Kaspersky Security Center Linux para instalar aplicativos Kaspersky e software de outros fornecedores nas dispositivos detectados. O Kaspersky Security Center Linux regularmente inicia uma descoberta de dispositivos, o que significa que se alguma nova instância aparecer na rede, ela será detectada automaticamente.

9 Organização de dispositivos em grupos de administração

Em alguns casos, implementar a proteção em dispositivos na rede no modo mais conveniente pode necessitar que você divida todo o conjunto de dispositivos em grupos de administração, considerando a estrutura da organização. Você pode criar regras para mover para distribuir dispositivos entre grupos ou pode distribuir os dispositivos manualmente. Você pode atribuir tarefas de grupo para grupos de administração, definir o escopo das políticas e atribuir pontos de distribuição.

Assegure-se de que todos os dispositivos gerenciados foram corretamente atribuídos aos grupos de administração apropriados, e que não mais haja dispositivos não atribuídos na rede.

10 Atribuir os pontos de distribuição

Recomendamos que você use pontos de distribuição em redes de larga escala para reduzir a carga no Servidor de Administração, e em redes que têm uma estrutura distribuída para fornecer ao Servidor de Administração o acesso aos dispositivos (ou grupos de dispositivos) comunicado através de canais com baixas taxas de produtividade. Os pontos de distribuição para grupos de administração podem ser atribuídos automaticamente ou manualmente.

Você pode atribuir gateways de conexão somente ao atribuir pontos de distribuição manualmente.

Para fazer isso:

- Certifique-se de que haja pontos de distribuição suficientes após alterar o modo de atribuição para manual.
- Configure as conexões necessárias do Servidor de Administração e dos gateways de conexão antes de prosseguir com a implementação dos Agentes de Rede nos dispositivos dos locais de rede em que os dispositivos devem se conectar ao Servidor de Administração por meio de um gateway de conexão.

11 Instalar o Agente de Rede e aplicativos de segurança em dispositivos na rede

A implementação da proteção em uma rede corporativa engloba a instalação do Agente de Rede e de aplicativos de segurança nos dispositivos que foram detectados pelo Servidor de Administração durante a descoberta de dispositivos.

Para instalar os aplicativos remotamente, execute o Assistente de implementação da proteção.

Os aplicativos de segurança protegem os dispositivos contra vírus e outros programas que apresentem uma ameaça. O Agente de Rede assegura a comunicação entre o dispositivo e o Servidor de Administração. As configurações do Agente de Rede são definidas automaticamente por padrão.

Antes que você inicie a instalação do Agente de Rede e dos aplicativos de segurança nos dispositivos na rede, assegure-se de que estes dispositivos estejam acessíveis (ligados).

12 Implementação de chaves de licença para dispositivos clientes

Implemente chaves de licença em dispositivos clientes para ativar aplicativos de segurança gerenciados naqueles dispositivos.

13 Configuração de políticas de aplicativo da Kaspersky

Para aplicar configurações de aplicativo diferentes a dispositivos diferentes, você pode usar gerenciamento de segurança centrado no dispositivo e/ou gerenciamento de segurança centrado no usuário. O gerenciamento de segurança centrado no dispositivo pode ser implementado usando políticas e tarefas. Você pode aplicar tarefas somente aos dispositivos que atendem a condições específicas. Para definir as condições para filtrar dispositivos, use seleções de dispositivos e identificadores.

14 Monitorar o status da proteção da rede

Você pode monitorar sua rede usando widgets no relatório, gerar relatórios a partir de aplicativos da Kaspersky, configurar e visualizar seleções de eventos recebidos dos aplicativos nos dispositivos gerenciados e visualizar listas de notificações.

O armazenamento de eventos a longo prazo, o recebimento imediato de eventos, o processamento e a correlação devem ser realizados em um sistema externo especializado em tarefas de SIEM.

Os indicadores dos componentes da solução são monitorados por meio do protocolo SNMP em sistemas de monitoramento da infraestrutura de TI e outras soluções de agentes de terceiros.

O monitoramento contínuo do status da proteção está disponível na seção **Central de fortalecimento da segurança** do Web Console.

Guia de Proteção

O Kaspersky Security Center Linux foi projetado para a execução centralizada de administração básica e tarefas de manutenção em uma rede corporativa. O aplicativo fornece ao administrador acesso a informações detalhadas sobre o nível de segurança da rede da organização. O Kaspersky Security Center Linux permite configurar todos os componentes de proteção criados com o uso dos aplicativos da Kaspersky.

O Servidor de Administração do Kaspersky Security Center Linux tem acesso total ao gerenciamento de proteção de dispositivos clientes, além de ser o componente mais importante do sistema de segurança da organização. Portanto, métodos de proteção aprimorados são necessários para o Servidor de Administração.

Antes de configurar, crie uma cópia backup do Servidor de Administração do Kaspersky Security Center Linux com o uso da tarefa Backup de dados do Servidor de Administração ou do utilitário klbackup. Mantenha a cópia backup dos dados em um local seguro.

O guia de proteção descreve as recomendações e recursos de configuração do Kaspersky Security Center Linux e seus componentes com o objetivo de reduzir os riscos de seu comprometimento.

O Guia de Proteção contém as seguintes informações:

- Seleção da arquitetura do Servidor de Administração
- Configuração de uma conexão segura com o Servidor de Administração
- Configuração de contas para acesso ao Servidor de Administração
- Gerenciamento da proteção do Servidor de Administração
- Gerenciamento de proteção dos dispositivos cliente
- Configuração da proteção para aplicativos gerenciados
- Manutenção do Servidor de Administração
- Transferência de informações para aplicativos de terceiros

- Recomendações de segurança para sistemas de informações de terceiros

Lista de verificação de proteção

Implementação do Servidor de Administração

- Instale o Servidor de Administração em um servidor físico ou virtual dedicado.
- Não use o servidor dedicado para executar outros serviços.
- Não instale o Servidor de Administração (aqui referido como o Servidor) no:
  - Controlador de domínio
  - Servidor de terminal
  - Dispositivo do usuário

Segurança de conexão

- Configure um firewall para restringir o acesso ao dispositivo Servidor em todas as portas e protocolos, com exceção das portas exigidas pelo Servidor. Permita o acesso ao dispositivo Servidor somente de dispositivos confiáveis.
- Configure uma lista de permissão de endereços IP para as portas do Servidor usadas para conectar o Kaspersky Security Center Web Console (também conhecido como Web Console) ao Servidor.
- Configure o firewall para permitir o acesso ao Servidor por meio do Web Console somente de dispositivos confiáveis.
- Configure o protocolo TLS versão 1.2 ou superior no Servidor.
- Configure um firewall para restringir o acesso ao dispositivo com o Servidor DBMS instalado.
- Configure a autenticação SSL entre o Servidor e o DBMS (MySQL ou PostgreSQL).

Contas e autenticação

- Configure a autenticação de dois fatores (TOTP, RFC 6238) para acessar o Servidor.
- Não instale o aplicativo autenticador no mesmo dispositivo a partir do qual a conexão ao Servidor por meio do Web Console é estabelecida.
- Use a autenticação multifator (MFA) para acessar o dispositivo do Servidor com o uso de um token, um cartão inteligente ou outro método.

- Crie um grupo de administração dedicado para o dispositivo Servidor e crie uma política de segurança especial para ele.
- Restrinja o número de usuários com a função de Administrador principal.
- Configure os direitos de acesso aos recursos do Servidor com base nas funções de usuários e grupos.
- Permita a instalação remota de aplicativos somente para uma conta de usuário separada.
- Realize uma auditoria regular de todos os usuários no dispositivo Servidor.

Gerenciamento da proteção do Servidor de Administração

- Instale um aplicativo de segurança no dispositivo do Servidor:
  - Para um servidor físico: Kaspersky Endpoint Security
  - Para um servidor virtual: Kaspersky Security for Virtualization
- Crie e aplique uma política separada para a proteção do Servidor (diferente das políticas de segurança para outros dispositivos gerenciados).
- Crie e aplique uma senha separada para a proteção do Servidor (diferente da senha para outros dispositivos gerenciados).
- Ative todos os módulos de proteção disponíveis no aplicativo de segurança (para obter informações sobre as configurações de segurança necessárias para usar o Servidor de Administração, consulte a Ajuda do Kaspersky Endpoint Security for Linux).

Configuração de políticas e tarefas para aplicativos gerenciados

- Crie e aplique políticas a todos os dispositivos gerenciados ou ao grupo com novos dispositivos gerenciados para os seguintes aplicativos:
  - Agente de Rede
  - Kaspersky Endpoint Security for Windows/Linux/macOS
  - Kaspersky Endpoint Agent (ou outros aplicativos da Kaspersky)
- Ative a proteção por senha contra a desativação da proteção ou desinstalação de aplicativos Kaspersky.
- Bloqueie as configurações da política (feche o "bloqueio") para impedir a reatribuição dessas configurações em dispositivos gerenciados.
- Crie uma tarefa de verificação completa programada de todos os dispositivos.
- Ative o uso da Kaspersky Security Network (KSN) e aceite a Declaração da KSN mais recente.

- Configure a descoberta de dispositivos e especifique o grupo de administração padrão para dispositivos recém-descobertos.
- Restrinja o uso de regras automáticas para mover dispositivos entre grupos de administração.
- Proteja os pontos de distribuição contra acesso não autorizado.
- Evite atribuir pontos de distribuição automaticamente em redes pequenas ou de alta importância.

Manutenção do Servidor de Administração

- Não exclua nem desative as seguintes tarefas:
  - Backup
  - Manutenção do Servidor de Administração
- Instale regularmente o SO e as atualizações de software de terceiros.

Transferência de eventos para sistemas de terceiros

- Configure o monitoramento e a elaboração de relatórios de eventos de segurança.
- Configure a exportação de eventos para um sistema SIEM.
- Configure as notificações do Servidor para:
  - Eventos de auditoria
  - Eventos críticos
  - Eventos de falha e advertências

Recomendações de segurança para sistemas de informações de terceiros

- Aplique as recomendações de segurança do CIS Benchmarks aos sistemas operacionais, DBMS e hipervisores usados.
- Para o Astra Linux, siga as recomendações de segurança da versão correspondente do Red Book.
- Para o RED OS, siga as recomendações fornecidas na documentação oficial do RED OS.

Implementação do Servidor de Administração

Arquitetura do Servidor de Administração

Em geral, a escolha de uma arquitetura de gerenciamento centralizado depende da localização dos dispositivos protegidos, acesso a redes adjacentes, esquemas de entrega de atualizações do banco de dados e assim por diante.

Na fase inicial de desenvolvimento da arquitetura, recomendamos conhecer os componentes do Kaspersky Security Center Linux e sua interação uns com os outros, assim como os esquemas para o tráfego de dados e uso de porta.

De acordo com essas informações, será possível formar uma arquitetura que especifique:

- A localização do Servidor de Administração e as conexões de rede
- Organização dos espaços de trabalho do administrador e métodos de conexão com o Servidor de Administração
- Os métodos de implementação do Agente de Rede e do software de proteção
- Uso dos pontos de distribuição
- Uso de Servidores de Administração virtuais
- Uso de uma hierarquia de Servidores de Administração
- O esquema de atualização do banco de dados de antivírus
- Outros fluxos de informação

Seleção de um dispositivo para a instalação do Servidor de Administração

Recomendamos instalar o Servidor de Administração em um servidor dedicado na infraestrutura da organização. Caso não haja outro software de terceiros instalado no servidor, é possível definir as configurações de segurança de acordo com os requisitos do Kaspersky Security Center Linux sem haver a dependência dos requisitos de software de terceiros.

É possível implementar o Servidor de Administração em um servidor físico ou em um servidor virtual. Verifique e confirme se o dispositivo selecionado atende aos requisitos de hardware e software.

Restrição de implementação do Servidor de Administração em um controlador de domínio, um servidor de terminal ou um dispositivo de usuário

Não recomendamos instalar o Servidor de Administração em um controlador de domínio, um servidor de terminal ou um dispositivo de usuário.

Recomendamos que a separação funcional dos nós de chave de rede seja fornecida. Essa abordagem permite manter a operacionalidade de diferentes sistemas quando um nó falhar ou for comprometido. Ao mesmo tempo, é possível criar diferentes políticas de segurança para cada nó.

Contas para instalar e executar o Servidor de Administração

Durante a implementação do Servidor de Administração, é necessário criar duas contas sem privilégios. Os serviços incluídos no Servidor de Administração funcionarão sob essas contas sem privilégios. Siga o princípio do menor privilégio ao conceder direitos e permissões às contas. Evite incluir contas desnecessárias no grupo "kladmins."

Também é necessário criar uma conta DBMS interna. O Servidor de Administração usa essa conta DBMS interna para acessar o DBMS selecionado.

O conjunto de contas necessárias e seus direitos depende do tipo de DBMS selecionado e método de criação do banco de dados do Servidor de Administração.

Segurança de conexão

Uso de TLS

Recomendamos proibir as conexões inseguras com o Servidor de Administração. Por exemplo, é possível proibir as conexões que usam HTTP nas configurações do Servidor de Administração.

Observe que, por padrão, várias portas HTTP do Servidor de Administração estão fechadas. A porta restante é usada para o servidor web do Servidor de Administração (8060). Essa porta pode ser limitada pelas configurações do firewall do dispositivo do Servidor de Administração.

Configurações estritas de TLS

Recomendamos usar o protocolo TLS, versão 1.2 e posterior, e restringir ou proibir algoritmos de criptografia inseguros.

Você pode configurar os protocolos de criptografia (TLS) usados pelo Servidor de Administração. Observe que no momento do lançamento de uma versão do Servidor de Administração, por padrão, as configurações do protocolo de criptografia são definidas para garantir a transferência segura de dados.

Restrição de acesso ao banco de dados do Servidor de Administração

Recomendamos restringir o acesso ao banco de dados do Servidor de Administração. Por exemplo, conceda acesso apenas ao dispositivo a partir do Servidor de Administração. Isso reduz a probabilidade de o banco de dados do Servidor de Administração ser comprometido devido a vulnerabilidades conhecidas.

É possível configurar os parâmetros de acordo com as instruções de operação do banco de dados usado, assim como fornecer portas fechadas em firewalls.

Interação de segurança com um DBMS externo

Se o DBMS for instalado em um dispositivo separado durante a instalação do Servidor de Administração (DBMS externo), recomendamos configurar os parâmetros para interação segura e autenticação com este DBMS. Para obter mais informações sobre como configurar a autenticação SSL, consulte autenticação do Servidor PostgreSQL e Cenário: Autenticação do Servidor MySQL.

Configuração de uma lista de permissão de endereços IP para conexão ao Servidor de Administração

Por padrão, os usuários do Kaspersky Security Center Linux podem fazer login em qualquer dispositivo onde o Kaspersky Security Center Web Console ou aplicativos OpenAPI estejam instalados. É possível configurar o Servidor de Administração para que os usuários apenas possam se conectar a ele apenas em dispositivos com endereços IP permitidos. Nesse caso, se um invasor tentar se conectar ao Kaspersky Security Center Linux por meio do Web Console Server instalado em um dispositivo que não esteja na lista de permissão, ele não conseguirá fazer o login no Kaspersky Security Center Linux.

Configuração de uma lista de permissão de endereços IP para conexão ao Kaspersky Security Center Web Console

Por padrão, os usuários do Kaspersky Security Center Linux podem se conectar ao Kaspersky Security Center Web Console em qualquer dispositivo. Em um dispositivo com o Kaspersky Security Center Web Console, o firewall (integrado ao sistema ou de terceiros) deve ser configurado para permitir conexões apenas de endereços IP autorizados.

Segurança da conexão com o controlador de domínio durante a sondagem

Para consultar o controlador de domínio, o Servidor de Administração ou um ponto de distribuição Linux tenta se conectar a este domínio via LDAPS. Por padrão, a verificação de certificado não é exigida durante a conexão. Para impor a verificação de certificado, defina o sinalizador `KLNAG_LDAP_TLS_REQCERT` como 1. Você também pode especificar um caminho personalizado para a autoridade de certificação (CA) para acessar a cadeia de certificados, usando a opção `KLNAG_LDAP_SSL_CACERT`.

Contas e autenticação

Antes de seguir estas etapas, crie uma cópia backup dos dados do Servidor de Administração do Kaspersky Security Center Linux usando a tarefa Backup de dados do Servidor de Administração ou o utilitário klbackup e salve a cópia backup em um local seguro. Mantenha a cópia backup dos dados em um local seguro.

Usar a autenticação de dois fatores com o Servidor de Administração

O Kaspersky Security Center Linux usa autenticação de dois fatores ao fazer login no Kaspersky Security Center Web Console com base no padrão RFC 6238 (TOTP: Algoritmo de Senha Avulsa por Tempo Limitado).

Sempre que você fizer login no Kaspersky Security Center Web Console, insira seu nome de usuário, senha e um código de segurança de uso único adicional. Para receber um código de segurança de uso único, é necessário instalar um app autenticador no seu computador ou dispositivo móvel.

Existem autenticadores de software e hardware (tokens) que são compatíveis com o padrão RFC 6238. Exemplos de autenticadores de software incluem o Kaspersky Password Manager for Business, Google Authenticator, Microsoft Authenticator e FreeOTP.

É altamente recomendável não instalar o app autenticador no mesmo dispositivo no qual a conexão com o Servidor de Administração é estabelecida. É possível instalar um app autenticador no seu dispositivo móvel.

Uso da autenticação de dois fatores para um sistema operacional

Para garantir uma proteção abrangente usando a autenticação de dois fatores, é necessário proteger não apenas o Servidor de Administração, mas também o dispositivo no qual ele está instalado.

Ao conectar-se ao dispositivo onde o Servidor de Administração está instalado (por SSH, RDP ou outros protocolos), recomendamos usar a autenticação multifator (MFA) com um token, cartão inteligente ou outro método de autenticação.

Proibição para salvar a senha do administrador

Caso Kaspersky Security Center Web Console seja usado, não recomendamos salvar a senha do administrador no navegador instalado no dispositivo do usuário.

Autenticação de uma conta de usuário interna

Por padrão, a senha de uma conta de usuário interna do Servidor de Administração deve seguir as seguintes regras:

- A senha deve ter de 8 a 256 caracteres.
- A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
  - Letras maiúsculas (A–Z)
  - Letras minúsculas (a-z)
  - Números (0–9)
  - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- A senha não deve conter nenhum espaço em branco, caracteres Unicode ou a combinação dos caracteres "." e "@", quando "." estiver colocado antes de "@".

Por padrão, o número máximo de tentativas permitidas de entrada da senha é de 10. É possível alterar o número permitido de tentativas de inserção de senha.

O usuário do Kaspersky Security Center Linux pode inserir uma senha inválida um número limitado de vezes. Depois que o limite é atingido, a conta de usuário é bloqueada por uma hora.

Configuração das opções para alteração de senha de conta de usuário interna

Recomendamos configurar as seguintes opções para alteração de senha de uma conta de usuário interna:

- Período de rotação de senha
- Horário da advertência prévia sobre a necessidade de alterar a senha
- Valor da opção **O usuário deve alterar a senha no primeiro login**

Proteção da conta contra modificações não autorizadas

Recomendamos ativar uma opção adicional para proteger uma conta de usuário interna do Servidor de Administração contra modificações não autorizadas. Essa proteção deve ser configurada separadamente para cada usuário interno.

Grupo de administração dedicado para Servidor de Administração

Para o Servidor de Administração

Recomendamos criar um grupo de administração dedicado. Conceda direitos de acesso especiais para esse grupo e crie uma política de segurança especial para ele.

Para evitar diminuir intencionalmente o nível de segurança do Servidor de Administração, recomendamos restringir a lista de contas que podem gerenciar o grupo de administração dedicado.

Restrição da atribuição da função de Administrador principal

O usuário criado pelo utilitário kladduser é atribuído com a função de Administrador principal na lista de controle de acesso (ACL) do Servidor de Administração ou do Servidor de Administração virtual. Recomendamos evitar atribuir a função de Administrador principal a um grande número de usuários.

Configuração de direitos de acesso aos recursos do aplicativo

Recomendamos usar a configuração flexível de direitos de acesso aos recursos do Kaspersky Security Center Linux para cada usuário ou grupo de usuários.

O controle de acesso baseado em função permite a criação de funções de usuário padrão com um conjunto predefinido de direitos e atribuição dessas funções aos usuários dependendo do seu escopo de obrigações.

As principais vantagens do modelo de controle de acesso baseado em função:

- Facilidade de administração
- Hierarquia de função
- Abordagem de privilégio mínimo
- Segregação de deveres

É possível atribuir funções internas a determinados profissionais de acordo com suas posições ou criar funções completamente novas.

Ao configurar as funções, observe os privilégios associados com a alteração do estado de proteção do dispositivo do Servidor de Administração e com a instalação remota de software de terceiros:

- Gerenciamento de grupos de administração
- Operações com o Servidor de Administração
- Instalação remota
- Alteração dos parâmetros para armazenamento de eventos e envio de notificações.

  Esse privilégio permite definir as notificações que executam um script ou um módulo executável no dispositivo do Servidor de Administração quando um evento ocorrer.

Conta separada para instalação remota de aplicativos

Além da diferenciação básica de direitos de acesso, recomendamos restringir a instalação remota de aplicativos para todas as contas (exceto para o administrador principal ou outra conta especializada).

Recomendamos o uso de uma conta separada para instalação remota de aplicativos. É possível atribuir uma função ou permissões para a conta separada.

Auditoria periódica de todos os usuários e suas ações

Recomendamos conduzir uma auditoria regular de todos os usuários no dispositivo do Servidor de Administração. Isso permite responder a certos tipos de ameaças de segurança associadas ao possível comprometimento de um dispositivo.

Você também pode rastrear as ações dos usuários, como a conexão ou desconexão do Servidor de Administração, conexão ao Servidor de Administração com um erro e modificação de objetos (para objetos compatíveis com o gerenciamento de revisões).

Gerenciamento da proteção do Servidor de Administração

Seleção de um software de proteção do Servidor de Administração

Dependendo do tipo de implementação do Servidor de Administração e da estratégia de proteção geral, selecione o aplicativo para proteger o dispositivo do Servidor de Administração.

Caso o Servidor de Administração seja implantado em um dispositivo dedicado, recomendamos selecionar o aplicativo Kaspersky Endpoint Security para proteger o dispositivo do Servidor de Administração. Isso permite aplicar todas as tecnologias disponíveis para proteger o dispositivo do Servidor de Administração, inclusive os módulos de análise comportamental.

Caso o Servidor de Administração esteja instalado em um dispositivo existente na infraestrutura e que tenha sido usado anteriormente para outras tarefas, recomendamos considerar o seguinte software de proteção:

- Kaspersky Industrial CyberSecurity for Nodes. Recomendamos instalar esse aplicativo em dispositivos incluídos em uma rede industrial. Kaspersky Industrial CyberSecurity for Nodes é um aplicativo que possui certificados de compatibilidade com diversos fabricantes de softwares industriais.

- Aplicativos de segurança recomendados. Caso o Servidor de Administração esteja instalado em um dispositivo com outro software, recomendamos levar em consideração as recomendações desse fornecedor de software sobre a compatibilidade de produtos de segurança (é possível que já haja recomendações para selecionar uma solução de segurança e talvez seja necessário configurar a zona confiável).

Criação de uma política de segurança separada para o aplicativo de proteção

Recomendamos criar uma política de segurança separada para o aplicativo de proteção do dispositivo do Servidor de Administração. Essa política deve ser diferente da política de segurança para dispositivos clientes. Isso permite especificar as configurações de segurança mais apropriadas para o Servidor de Administração, sem afetar o nível de proteção de outros dispositivos.

Recomendamos dividir os dispositivos em grupos e, em seguida, colocar o dispositivo do Servidor de Administração em um grupo separado para o qual será possível criar uma política de segurança especial.

Módulos de proteção

Caso não haja recomendações especiais do fornecedor do software de terceiros instalado no mesmo dispositivo do Servidor de Administração, recomendamos ativar e configurar todos os módulos de proteção disponíveis (depois de verificar a operação desses módulos de proteção por um determinado período).

Configuração do firewall do dispositivo do Servidor de Administração

No dispositivo do Servidor de Administração, recomendamos configurar o firewall para restringir o número de dispositivos nos quais os administradores poderão se conectar ao Servidor de Administração usando o Kaspersky Security Center Web Console.

Por padrão, o Servidor de Administração usa a porta 13299 para receber conexões do Kaspersky Security Center Web Console. Recomendamos restringir o número de dispositivos nos quais o Servidor de Administração pode ser gerenciado com o uso dessa porta.

Gerenciar a proteção do Agente de Rede

Para impedir que invasores tirem os dispositivos do controle do Servidor de Administração, é altamente recomendável seguir estas práticas:

Usar a senha de desinstalação

Nas configurações do pacote de instalação do Agente de Rede, especifique a senha de desinstalação que será solicitada ao desinstalar o Agente de Rede.

A funcionalidade está disponível somente para o Agente de Rede em dispositivos Windows.

Reforçar a proteção do Agente de Rede

Nas configurações do pacote de instalação do Agente de Rede, ative a opção **Proteger serviço do Agente de Rede contra remoção ou interrupção não autorizada e impedir alterações nas configurações**. Após a instalação do Agente de Rede em um dispositivo gerenciado, o componente não poderá ser desinstalado ou modificado sem os privilégios necessários. O serviço Agente de Rede não pode ser interrompido.

A funcionalidade está disponível somente para o Agente de Rede em dispositivos Windows.

Monitorar o endereço do Servidor de Administração ao qual o Agente de Rede se conecta

Para detectar qualquer redirecionamento não autorizado do Agente de Rede para um Servidor de Administração externo, use o Log de Eventos Kaspersky. O Log de Eventos Kaspersky é uma seção do log de eventos armazenado no sistema operacional dos dispositivos gerenciados. No Windows, é possível visualizar o conteúdo do log usando o Visualizador de Eventos e, no Linux, usando o utilitário journalctl. Quando o Agente de Rede se conecta ao Servidor de Administração, uma ou duas entradas são gravadas no Log de Eventos Kaspersky com as seguintes informações:

- Endereço do Servidor de Administração:
  - **Tentar conectar-se ao Servidor de Administração em <endereço do Servidor de Administração>**.
  - **Conectado ao Servidor de Administração em <endereço do Servidor de Administração>**.
- O endereço do Servidor de Administração e do gateway de conexão ao conectar-se por meio de um gateway:
  - **Tentar conectar-se ao Servidor de Administração em <endereço do Servidor de Administração> via CG <endereço do gateway de conexão>**.
  - **Conectado ao Servidor de Administração em <endereço do Servidor de Administração> via CG <endereço do gateway de conexão>**.

Um evento com o endereço do Servidor de Administração é registrado nos seguintes casos:

- Sempre que o serviço Agente de Rede é reiniciado
- Quando o Agente de Rede se conecta a outro Servidor de Administração
- Uma vez por dia durante a operação normal do dispositivo, mesmo que o serviço Agente de Rede não tenha sido reiniciado e o Agente de Rede não tenha se conectado a outro Servidor de Administração (nesse caso, somente a segunda entrada é publicada novamente no log).

Por conveniência, recomendamos configurar o envio de eventos do Log de Eventos Kaspersky para um sistema SIEM e gerar um alerta caso o endereço do Servidor indicado no evento não corresponda ao endereço atual do seu Servidor.

Gerenciamento de proteção dos dispositivos cliente

Restrição de adição de chaves de licença a pacotes de instalação

Os pacotes de instalação são armazenados na pasta compartilhada do Servidor de Administração, na subpasta Pacotes. Caso uma chave de licença seja adicionada a um pacote de instalação, a chave de licença poderá ser acessada por todos os usuários com direitos de leitura para esta pasta (diretamente ou via Servidor Web integrado no Servidor de Administração).

Para evitar o comprometimento da chave de licença, não recomendamos adicionar as chaves de licença nos pacotes de instalação.

Recomendamos usar a distribuição automática de chaves de licença para dispositivos gerenciados, a implementação pela tarefa adicionar chave de licença para um aplicativo gerenciado e a adição manual de um código de ativação ou arquivo de chave nos dispositivos.

Regras automáticas para migrar os dispositivos entre os grupos de administração

Recomendamos restringir o uso de regras automáticas para dispositivos móveis entre os grupos de administração.

Caso as regras automáticas para mover dispositivos sejam usadas, isso poderá provocar a propagação de políticas que fornecem mais privilégios ao dispositivo movido antes do que ele tinha no momento da realocação.

Além disso, mover um dispositivo cliente para outro grupo de administração pode causar a propagação das configurações da política. Essas configurações da política podem ser indesejáveis para distribuição entre os dispositivos convidados e não confiáveis.

Essa recomendação não se aplica à alocação inicial única de dispositivos para grupos de administração.

Requisitos de segurança para pontos de distribuição e gateways de conexão

Os dispositivos com o Agente de Rede instalado podem atuar como um ponto de distribuição e executar as seguintes funções:

- Distribuir atualizações e pacotes de instalação recebidos do Servidor de Administração para dispositivos clientes dentro do grupo.
- Executar a instalação remota de software de terceiros e aplicativos Kaspersky em dispositivos cliente.
- Faça a sondagem da rede para detectar novos dispositivos e para atualizar as informações sobre os existentes. Um ponto de distribuição pode aplicar os mesmos métodos de localização dos dispositivos que os do Servidor de Administração.

Colocação de pontos de distribuição na rede da organização usados para:

- Reduzir a carga no Servidor de Administração
- Otimizar o tráfego
- Fornecer ao Servidor de Administração o acesso aos dispositivos em partes de difícil acesso de uma rede

Tendo em vista as capacidades disponíveis, recomendamos proteger os dispositivos que funcionam como pontos de distribuição de qualquer tipo de acesso não autorizado (inclusive acesso físico).

Restrição da atribuição automática dos pontos de distribuição

Para simplificar a administração e manter a operacionalidade da rede, recomendamos o uso de atribuição automática de pontos de distribuição. Entretanto, para redes industriais e pequenas redes, recomendamos evitar a atribuição de pontos de distribuição automaticamente, pois, por exemplo, as informações privadas das contas usadas para enviar as tarefas de instalação remota podem ser transferidas para os pontos de distribuição pelo sistema operacional.

Para redes industriais e pequenas redes, é possível atribuir os dispositivos manualmente para atuar como pontos de distribuição.

Também é possível visualizar o Relatório de atividades de pontos de distribuição.

Requisitos de segurança para dispositivos de usuários do Kaspersky Security Center Linux

Requisitos especiais de segurança devem ser aplicados aos dispositivos dos usuários do Kaspersky Security Center Linux. Recomendamos proteger esses dispositivos contra qualquer tipo de acesso não autorizado (inclusive físico).

Os dispositivos de usuários do Kaspersky Security Center Linux incluem:

- Dispositivos com os quais os usuários do Kaspersky Security Center Linux se conectam ao Kaspersky Security Center Web Console usando um navegador.
- Dispositivos usados por aplicativos que se conectam ao Kaspersky Security Center Linux e interagem com o Servidor de Administração via OpenAPI.

Requisitos de segurança para dispositivos com o Kaspersky Security Center Web Console instalado

Dispositivos com o Kaspersky Security Center Web Console instalado são usados para gerenciar o Kaspersky Security Center Linux, portanto, requisitos especiais devem ser aplicados à segurança desses dispositivos. Recomendamos proteger esses dispositivos contra qualquer tipo de acesso não autorizado (inclusive físico).

Configuração da proteção para aplicativos gerenciados

Políticas de aplicativos gerenciados

Recomendamos a criação de uma política para cada tipo de aplicativo e componente usado do Kaspersky Security Center Linux (Agente de Rede, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Agent e outros). Esta política deve ser aplicada em todos os dispositivos gerenciados (o grupo de administração root) ou em um grupo separado para o qual novos dispositivos gerenciados são movidos automaticamente de acordo com as regras de movimentação configuradas.

Especificação da senha para desativar a proteção e desinstalar o aplicativo

É altamente recomendável ativar a proteção por senha para impedir que invasores desativem ou desinstalem os aplicativos de segurança da Kaspersky. Em plataformas nas quais a proteção por senha é compatível, é possível definir a senha, por exemplo, para o Kaspersky Endpoint Security, Agente de Rede e outros aplicativos da Kaspersky. Depois de ativar a proteção por senha, recomendamos bloquear as configurações correspondentes com o fechamento do "cadeado".

Especificação da senha para a conexão manual de um dispositivo cliente ao Servidor de Administração (utilitário klmover)

O utilitário klmover permite conectar manualmente um dispositivo cliente ao Servidor de Administração. O utilitário klmover está localizado na pasta Instalação do Agente de Rede.

Para impedir que intrusos movam dispositivos para fora do controle do Servidor de Administração, é altamente recomendável ativar a proteção por senha para executar o utilitário klmover. Para ativar a proteção por senha, selecione a opção **Usar senha de desinstalação** nas configurações da política do Agente de Rede.

O utilitário klmover requer direitos de administrador local.

Se você perder ou esquecer a senha do Agente de Rede protegido por senha instalado no dispositivo que não está mais sob a gestão do Kaspersky Security Center Linux, não será possível remover o Agente de Rede por meio do utilitário klmover ou da linha de comando. Nesse caso, será necessário reinstalar o sistema operacional no dispositivo com o Agente de Rede instalado e protegido por senha.

A ativação da opção **Usar senha de desinstalação** em dispositivos Windows também ativará a proteção por senha para a ferramenta Cleaner (cleaner.exe).

Usar a Kaspersky Security Network

Em todas as políticas de aplicativos gerenciados e nas propriedades do Servidor de Administração, recomendamos ativar o uso da Kaspersky Security Network (KSN) e aceitar a Declaração da KSN. Durante a atualização ou o upgrade do Servidor de Administração, é possível aceitar a Declaração da KSN atualizada. Em alguns casos, quando o uso de serviços em nuvem for proibido por lei ou por outros regulamentos, é possível desativar a KSN.

Verificação regular de dispositivos gerenciados

Para todos os grupos de dispositivos, recomendamos criar uma tarefa que execute periodicamente uma verificação completa dos dispositivos.

Descoberta de novos dispositivos

Recomendamos definir corretamente as configurações de descoberta de dispositivos: configurar a integração com controladores de domínio e especificar os intervalos de endereços IP para descobrir novos dispositivos.

De acordo com os propósitos de segurança, é possível usar o grupo de administração padrão que inclui todos os novos dispositivos e as políticas padrão que afetam esse grupo.

Manutenção do Servidor de Administração

Cópia de backup de dados do Servidor de Administração

Backup de dados permite restaurar os dados do Servidor de Administração sem perda de dados.

Por padrão, uma tarefa de backup de dados é criada automaticamente após a instalação do Servidor de Administração e é executada periodicamente ao salvar os backups no diretório apropriado.
As configurações da tarefa de backup de dados podem ser alteradas da seguinte forma:

- A frequência de backup aumenta
- Um diretório especial para salvar cópias é especificado
- As senhas para cópias de backup são alteradas

Caso as cópias de backup sejam armazenadas em um diretório especial, diferentemente do diretório padrão, recomendamos limitar a lista de controle de acesso (ACL) para esse diretório. As contas do Servidor de Administração e as contas do banco de dados do Servidor de Administração devem ter acesso de gravação para esse diretório.

Manutenção do Servidor de Administração

A manutenção do Servidor de Administração permite reduzir o volume do banco de dados e aprimorar o desempenho e a confiabilidade da operação do aplicativo. Recomendamos efetuar a manutenção do Servidor de Administração ao menos uma vez por semana.

A manutenção do Servidor de Administração é executada usando uma tarefa dedicada. O aplicativo executa as seguintes ações ao efetuar a manutenção do Servidor de Administração:

- Reorganiza os índices do banco de dados
- Atualiza as estatísticas do banco de dados
- Compacta o banco de dados (caso seja necessário)

Instalação de atualizações do sistema operacional e atualizações de software de terceiros

Recomendamos com ênfase a instalação regular das atualizações de software do sistema operacional e dos softwares de terceiros no dispositivo do Servidor de Administração.

Os dispositivos cliente não requerem uma conexão contínua com o Servidor de Administração, portanto, é seguro reinicializar o dispositivo do Servidor de Administração após a instalação das atualizações. Todos os eventos registrados nos dispositivos clientes durante o tempo de inatividade do Servidor de Administração são enviados para ele após a conexão ser restaurada.

Transferência de eventos para sistemas de terceiros

Monitoramento e relatórios

Para uma resposta oportuna aos problemas de segurança, recomendamos configurar os recursos de monitoramento e relatórios.

Exportação de eventos para os sistemas SIEM

Para a detecção rápida dos problemas de segurança antes que ocorram danos significativos, recomendamos o uso da exportação de eventos em um sistema SIEM.

Notificações por e-mail de eventos de auditoria

O Kaspersky Security Center Linux lhe permite receber informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nestes dispositivos gerenciados. Para uma pronta resposta a emergências, recomendamos configurar o Servidor de Administração para o envio de notificações sobre os eventos de auditoria, eventos críticos, eventos de falha e advertência que ele publica.

Como esses eventos são eventos intrassistema, pode haver um pequeno número deles, o que é bastante pertinente para a correspondência.

Recomendações de segurança para sistemas de informações de terceiros

Recomendações de segurança do CIS Benchmarks

Ao usar versões de sistemas operacionais, plataformas de virtualização ou servidores de banco de dados compatíveis com o Servidor de Administração e o Agente de Rede, recomendamos aplicar as melhores práticas de segurança da informação do Center for Internet Security (CIS), se houver, para aperfeiçoar esses sistemas de informação.

Center for Internet Security (CIS) é uma organização sem fins lucrativos dedicada a melhorar a segurança no campo da tecnologia da informação. Em particular, o CIS desenvolve e distribui padrões de segurança, como CIS Controls e CIS Benchmarks. Esses padrões são um conjunto de recomendações e práticas para garantir a segurança dos sistemas de informação.

O portal do CIS contém recomendações para as versões dos seguintes sistemas de informação suportados pelo Servidor de Administração e pelo Agente de Rede:

- Sistemas operacionais das seguintes famílias:
  - Windows para desktops
  - Windows para servidores
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS

- Plataformas de virtualização VMware
- Servidores de banco de dados:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Recomendações de segurança para o sistema operacional Astra Linux

Ao usar o sistema operacional Astra Linux, é necessário seguir as recomendações de segurança descritas no Red Book para a versão correspondente do Astra Linux.

Recomendações de segurança para o sistema operacional RED OS

Ao usar o sistema RED OS, siga as recomendações de segurança do guia do administrador descritas na documentação oficial do RED OS.

Recomendações para usar aplicativos de segurança da Kaspersky

Uso da senha do KLAdmin no Kaspersky Endpoint Security for Windows

A conta KLAdmin é uma conta de administrador com acesso irrestrito ao Kaspersky Endpoint Security for Windows. A conta KLAdmin tem o direito de executar qualquer ação protegida por senha no Kaspersky Endpoint Security for Windows, incluindo a remoção do aplicativo. As permissões para a conta KLAdmin não podem ser revogadas. É possível definir a senha da conta KLAdmin nas propriedades da política do Kaspersky Endpoint Security for Windows. O administrador do Kaspersky Endpoint Security for Windows é totalmente responsável pelo uso seguro da senha da conta KLAdmin. Caso sua organização tenha a própria política de senha, siga as instruções dessa política. Quanto mais longa e complexa a senha, mais confiável ela é.

Nossas recomendações para proteger a organização contra roubo da senha do KLAdmin são as seguintes:

- **Requisitos gerais**

  Não use o nome da conta ou parte do nome como a senha.

- **Requisitos mínimos de comprimento da senha**

  Crie uma senha com pelo menos 10 caracteres.

- **Requisitos para o uso de vários tipos de caracteres**

  Defina uma senha complexa que contenha caracteres de diferentes categorias: letras maiúsculas e minúsculas, números e caracteres especiais.

- **Requisitos de expiração da senha**

  Defina uma data mínima de expiração da senha de 90 dias. Uma nova senha não deve corresponder a nenhuma das últimas 24 senhas.

Cenário: Autenticação do MySQL Server

Recomendamos usar um certificado TLS para autenticar o servidor MySQL. É possível usar um certificado de uma autoridade de certificação (AC) confiável ou um certificado autoassinado.

O Servidor de Administração é compatível com a autenticação SSL unidirecional e bidirecional para o MySQL.

Ativar a autenticação SSL unidirecional

Siga estas etapas para configurar a autenticação SSL para o MySQL:

1. **Crie um certificado TLS autoassinado para o servidor MySQL**

   Execute o seguinte comando:

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

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

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

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

2. **Crie um arquivo de sinalização do servidor**

   Use o utilitário klscflag para criar o sinalizador do servidor KLSRV_MYSQL_OPT_SSL_CA e especifique o caminho para o certificado como seu valor. O utilitário klscflag está localizado no diretório no qual o Servidor de Administração está instalado. O caminho de instalação padrão é /opt/kaspersky/ksc64/sbin.

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

3. **Configure o banco de dados**

   Especifique os certificados no arquivo my.cnf. Abra o arquivo my.cnf em um editor de texto e adicione as seguintes linhas na seção [mysqld]:

   ```
   [mysqld]
   ```

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

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

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

Ativar a autenticação SSL bidirecional

Siga estas etapas para configurar a autenticação bidirecional SSL para o MySQL:

1. **Crie arquivos de sinalização do servidor**

   Use o utilitário klscflag para criar os sinalizadores do servidor e especifique o caminho para os arquivos do certificado como seus valores:

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

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <caminho para server-cert.pem> -t s
   ```

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

   O utilitário klscflag está localizado no diretório no qual o Servidor de Administração está instalado. O caminho de instalação padrão é /opt/kaspersky/ksc64/sbin.

2. **Especifique a senha (opcional)**

   Caso o server-key.pem exija uma senha, crie um sinalizador KLSRV_MARIADB_OPT_TLS_PASPHRASE e especifique a senha como seu valor:

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

3. **Configure o banco de dados**

   Especifique os certificados no arquivo my.cnf. Abra o arquivo my.cnf em um editor de texto e adicione as seguintes linhas na seção [mysqld]:

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

Cenário: Autenticação TLS bidirecional do PostgreSQL para o banco de dados do Servidor de Administração e o banco de dados do IAM

No Kaspersky Security Center Linux, é possível configurar a criptografia e a validação mútua de certificados entre o servidor PostgreSQL e os clientes, ou seja, o Servidor de Administração e o IAM. Cada banco de dados usa um usuário e um certificado de cliente próprios. Além do TLS, também é usada a autenticação por senha `scram-sha-256`.

A autenticação do servidor PostgreSQL ocorre em etapas:

1. **Preparação do SGBD e criação de funções**

   Execute os seguintes comandos:

   ```
   sudo -u postgres psql
   CREATE DATABASE kav;
   ```

```
CREATE DATABASE iam;
CREATE USER myuserksc WITH PASSWORD '*password*';
ALTER ROLE myuserksc WITH LOGIN CREATEDB;
ALTER DATABASE kav OWNER TO myuserksc;
CREATE USER myuseriam WITH PASSWORD '*password*';
ALTER ROLE myuseriam WITH LOGIN CREATEDB;
ALTER DATABASE iam OWNER TO myuseriam;
```

2. Criação de uma CA própria e de um certificado de servidor (autenticação SSL unidirecional)

`subjectAltName` (SAN) é um parâmetro obrigatório do certificado do servidor. O valor desse parâmetro deve corresponder ao FQDN do host.

Execute os seguintes comandos:

```
sudo openssl req -x509 -nodes -newkey rsa:4096 -keyout
/etc/ssl/private/postgresql_ca.key -out /etc/ssl/certs/postgresql_ca.crt -days 365 -
addext "subjectAltName=DNS:*FQDN*" -subj "/CN=mysrvca"
sudo openssl req -new -nodes -newkey rsa:4096 -keyout
/etc/ssl/private/postgresql_leaf.key -out /tmp/postgresql_leaf.csr -addext
"subjectAltName=DNS:< FQDN >" -subj "/CN=*FQDN*"
sudo openssl x509 -req -in /tmp/postgresql_leaf.csr -CA
/etc/ssl/certs/postgresql_ca.crt -CAkey /etc/ssl/private/postgresql_ca.key -
CAcreateserial -out /etc/ssl/certs/postgresql_leaf.crt -days 365 -sha256 -
copy_extensions copy
sudo cat /etc/ssl/certs/postgresql_leaf.crt /etc/ssl/certs/postgresql_ca.crt | sudo
tee /etc/ssl/certs/postgresql.crt
sudo chmod 600 /etc/ssl/private/postgresql_leaf.key
sudo chown postgres:postgres /etc/ssl/private/postgresql_leaf.key
sudo chmod 644 /etc/ssl/certs/postgresql_leaf.crt
sudo chown ksc:kladmins /etc/ssl/certs/postgresql_ca.crt
sudo chmod 644 /etc/ssl/certs/postgresql_ca.crt
sudo chmod 644 /etc/ssl/certs/postgresql.crt
```

3. Criação da CA do cliente e dos certificados para o banco de dados do Servidor de Administração e o banco de dados do IAM (autenticação SSL bidirecional)

Execute os seguintes comandos:

```
sudo openssl req -x509 -nodes -newkey rsa:4096 -keyout
/etc/ssl/private/postgresql_cli_ca.key -out /etc/ssl/certs/postgresql_cli_ca.crt -days
365 -subj "/CN=myclica"
openssl x509 -in /etc/ssl/certs/postgresql_cli_ca.crt -text -noout
sudo chmod 600 /etc/ssl/private/postgresql_cli_ca.key
sudo chmod 644 /etc/ssl/certs/postgresql_cli_ca.crt
openssl req -new -nodes -newkey rsa:4096 -keyout $HOME/postgresql_cli_myuserksc.key -
out /tmp/postgresql_cli_myuserksc.csr -subj "/CN=myuserksc"
sudo openssl x509 -req -in /tmp/postgresql_cli_myuserksc.csr -CA
/etc/ssl/certs/postgresql_cli_ca.crt -CAkey /etc/ssl/private/postgresql_cli_ca.key -
CAcreateserial -out $HOME/postgresql_cli_myuserksc.crt -days 365
openssl req -new -nodes -newkey rsa:4096 -keyout $HOME/postgresql_cli_myuseriam.key -
out /tmp/postgresql_cli_myuseriam.csr -subj "/CN=myuseriam"
sudo openssl x509 -req -in /tmp/postgresql_cli_myuseriam.csr -CA
/etc/ssl/certs/postgresql_cli_ca.crt -CAkey /etc/ssl/private/postgresql_cli_ca.key -
CAcreateserial -out $HOME/postgresql_cli_myuseriam.crt -days 365
```

4. Copiar certificados de cliente para o Servidor de Administração e o host do IAM e definir permissões

Execute os seguintes comandos:

```
sudo cp $HOME/postgresql_cli_myuserksc.crt   /home/ksc/
sudo cp $HOME/postgresql_cli_myuserksc.key   /home/ksc/
sudo cp $HOME/postgresql_cli_myuseriam.crt   /home/ksciam/
sudo cp $HOME/postgresql_cli_myuseriam.key   /home/ksciam/
sudo chown ksc:kladmins /home/ksc/*.crt /home/ksc/*.key
```

```
sudo chown ksciam:kladmins /home/ksciam/*.crt /home/ksciam/*.key
sudo chmod 644 /home/ksc/*.crt
sudo chmod 600 /home/ksc/*.key
sudo chmod 644 /home/ksciam/*.crt
sudo chmod 600 /home/ksciam/*.key
```

5. **Configuração do PostgreSQL**

   Edite o arquivo postgresql.conf da seguinte forma:

   ```
   listen_addresses = '*'
   ssl = on
   ssl_cert_file = '*path to postgresql.crt*'
   ssl_key_file = '*path to postgresql_leaf.key*'
   ssl_ca_file = '*path to postgresql_cli_ca.crt*'
   ```

   Modifique o arquivo pg_hba.conf da seguinte forma:

   ```
   hostssl    kav    myuserksc    *Administration Server IP address*    scram-sha-256
   clientcert=verify-full
   hostssl    iam    myuseriam    *Administration Server IP address*    scram-sha-256
   clientcert=verify-full
   ```

   Se o Servidor de Administração e o PostgreSQL estiverem no mesmo dispositivo, use o endereço `127.0.0.1/32` e `listen_addresses = 'localhost'`.

   Garanta que o arquivo pg_hba.conf não inclua um registro que comece com `host`.

6. **Reinício do daemon do PostgreSQL**

   Execute o seguinte comando:

   ```
   systemctl restart postgresql
   ```

7. **Especificação do sinalizador do servidor para o Servidor de Administração**

   Use o utilitário klscflag para criar os sinalizadores do servidor e especifique o caminho para os arquivos do certificado como seus valores.

   O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é `/opt/kaspersky/ksc64/sbin/`.

   Execute os seguintes comandos:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v *path to
   postgresql_cli_myuserksc.crt* -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v *path to
   postgresql_cli_myuserksc.key* -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v *path to
   postgresql_ca.crt* -t s
   ```

   Caso o postgres_leaf.key exija uma senha, crie um sinalizador KLSRV_POSTGRES_OPT_TLS_PASPHRASE e especifique a senha como seu valor:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v *pasphrase* -t s
   ```

8. **Configuração do IAM**

   Edite o arquivo iam_config.yaml da seguinte forma:

   ```
   dbms_tl_opt_ssl_ca: "/etc/ssl/certs/postgresql_ca.crt"
   dbms_tl_opt_ssl_verify_server_cn: "1"
   dbms_tl_opt_ssl_cert: "/home/ksc/postgresql_cli_myuseriam.crt"
   dbms_tl_opt_ssl_key:  "/home/ksc/postgresql_cli_myuseriam.key"
   ```

9. **Reinicialização dos serviços do Servidor de Administração**

   Execute o seguinte comando:

   ```
   sudo systemctl restart kl*
   ```

Preparação para implementação

Esta seção descreve como escolher a opção de implementação e a configuração do Kaspersky Security Center Linux, e um DBMS de acordo com as necessidades da sua organização.

Há diversas opções de implementação de componentes do Kaspersky Security Center Linux na rede de uma organização, considerando os seguintes critérios:

- Número total de dispositivos
- As unidades (escritórios locais, filiais) que são separadas de forma organizacional ou geográfica
- Separar as redes conectadas por canais estreitos
- Necessário fornecer acesso à Internet ao Servidor de Administração

Um Servidor de Administração pode ser compatível com até 50 mil dispositivos (com PostgreSQL ou Postgres Pro como DBMS). Se o número total de dispositivos na rede de uma organização exceder 50 mil, múltiplos Servidores de Administração devem ser implementados na rede e combinados em uma hierarquia para o gerenciamento centralizado conveniente.

Se uma organização incluir escritórios locais remotos de larga escala (filiais) com os seus próprios administradores, é útil implementar Servidores de Administração naqueles escritórios. Caso contrário, esses escritórios devem ser visualizados como redes separadas conectadas por canais com baixas taxas de produtividade, consulte o artigo "Configuração padrão: alguns escritórios de grande porte gerenciados por seus próprios administradores".

Ao usar redes desanexadas conectadas com canais estreitos, o tráfego pode ser poupado ao atribuir um ou diversos Agentes de Rede para atuar como pontos de distribuição (consulte tabela para o cálculo do número de pontos de distribuição). Nesse caso, todos os dispositivos em uma rede desanexada recuperam as atualizações desses centros de atualização locais. Os pontos de distribuição reais podem baixar as atualizações do Servidor de Administração (cenário padrão) e de servidores da Kaspersky na Internet (consulte o artigo "Configuração padrão: múltiplos pequenos escritórios remotos").

A seção "Configurações padrão do Kaspersky Security Center" fornece descrições detalhadas das configurações padrão do Kaspersky Security Center Linux. Ao planejar a implementação, selecione a configuração padrão mais adequada, dependendo da estrutura da organização.

Na etapa do planejamento da implementação, a atribuição do certificado especial X.509 ao Servidor de Administração deve considerada. A atribuição do certificado X.509 ao Servidor de Administração pode ser útil nos seguintes casos (lista parcial):

- Inspecionar tráfego da camada do soquete seguro (SSL) por meio de um proxy de terminação SSL ou para usar um proxy reverso
- Integração com a infraestrutura de chaves públicas (PKI) de uma organização
- Especificação dos valores necessários nos campos do certificado
- Fornecer a força de criptografia necessária de um certificado

Selecionar a configuração do Kaspersky Security Center Linux

Esta seção descreve as seguintes configurações padrão usadas para a implementação de componentes do Kaspersky Security Center Linux em uma rede de organização:

- Escritório único
- Alguns escritórios de larga escala que são geograficamente separados e executam por si seus próprios administradores
- Múltiplos pequenos escritórios que são geograficamente separados

Configuração padrão: escritório único

Um ou diversos Servidores de Administração podem ser implementados na rede da organização. O número de Servidores de Administração pode ser selecionado de acordo com o hardware disponível ou o número total de dispositivos gerenciados.

Um Servidor de Administração pode ser compatível com até 50 mil dispositivos (com PostgreSQL ou Postgres Pro como DBMS). Considere a possibilidade de aumentar o número de dispositivos gerenciados no futuro próximo: pode ser útil conectar um número ligeiramente menor de dispositivos em um único Servidor de Administração.

Os Servidores de Administração podem ser implementados na rede interna, ou na DMZ, dependendo de se o acesso à Internet aos Servidores de Administração é necessário.

Se múltiplos servidores forem usados, recomenda-se que você os combine em uma hierarquia. Usar uma hierarquia de Servidor de Administração permite evitar políticas e tarefas duplicadas, tratar todo o conjunto de dispositivos gerenciados como se eles fossem gerenciados por um único Servidor de Administração (ou seja, procura por dispositivos, criação de seleções de dispositivos e criação de relatórios).

Configuração padrão: Alguns escritórios de larga escala executam por si seus próprios administradores

Se uma organização tiver escritórios geograficamente separados em ampla escala, considere a opção de implantar Servidores de Administração em cada um dos escritórios. Um ou vários Servidores de Administração podem ser implementados por escritório, dependendo do número de dispositivos e hardware do cliente disponíveis. Neste caso, cada um dos escritórios pode ser visto como uma "Configuração padrão: Escritório único". Para facilitar a administração, é recomendável combinar todos os Servidores de Administração em uma hierarquia (possivelmente em vários níveis).

Caso alguns funcionários façam movimentações entre os escritórios com seus dispositivos (portáteis), crie perfis de conexão do Agente de Rede na política do Agente de Rede.

Configuração padrão: múltiplos pequenos escritórios remotos

Esta configuração padrão fornece meios para um escritório de sede e muitos pequenos escritórios remotos que podem se comunicar com o escritório via Internet. Cada um destes escritórios remotos pode estar localizados por trás da Network Address Translation (NAT), assim, nenhuma conexão pode ser estabelecida entre dois escritórios remotos, pois eles estão isolados.

Um Servidor de Administração deve ser implementado no escritório sede e um ou múltiplos pontos de distribuição devem ser atribuídos a todos os outros escritórios. Caso os escritórios estejam ligados pela Internet, pode ser útil criar uma tarefa *Baixar atualizações nos repositórios de pontos de distribuição* para os pontos de distribuição para que eles baixem as atualizações diretamente dos servidores Kaspersky, pasta de rede ou local, e não do Servidor de Administração.

Se alguns dispositivos em um escritório remoto não tiverem acesso direto ao Servidor de Administração (por exemplo, o acesso ao Servidor de Administração é fornecido por meio da Internet, mas alguns dispositivos não têm acesso à Internet), os pontos de distribuição devem ser alternados para o modo de gateway de conexão. Neste caso, os Agentes de Rede em dispositivos no escritório remoto serão conectados, para a sincronização adicional, ao Servidor de Administração – mas através do gateway, não diretamente.

Como o Servidor de Administração, muito provavelmente, não conseguirá sondar a rede do escritório remoto, pode ser útil transferir esta função para um ponto de distribuição.

O Servidor de Administração não será capaz de enviar notificações para a porta 15000 UDP em dispositivos gerenciados localizados além da NAT no escritório remoto. Para solucionar este problema, você pode ativar o modo da conexão contínua para o Servidor de Administração nas propriedades dos dispositivos que atuam como pontos de distribuição (caixa de seleção **Não desconectar do Servidor de Administração**). Este modo está disponível se o número total de pontos de distribuição não exceder 300. É possível usar servidores push para garantir que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração. Consulte o seguinte artigo para obter informações: Ativação de um servidor push.

Selecionar uma estrutura para a proteção de uma empresa

A seleção de uma estrutura para a proteção de uma organização é definida pelos seguintes fatores:

- Topologia de rede da organização.
- Estrutura organizacional.
- Número de funcionários responsáveis pela proteção da rede e alocação de suas responsabilidades.
- Recursos de hardware que podem ser alocados para os componentes de gerenciamento da proteção.
- A produtividade dos canais de comunicação que pode ser alocada para manter a operação dos componentes de proteção na rede da organização.
- Limites de tempo para execução de operações administrativas críticas na rede da organização. As operações administrativas críticas incluem, por exemplo, a distribuição das atualizações para os bancos de dados antivírus e a modificação de políticas para dispositivos cliente.

Ao selecionar uma estrutura de proteção, recomenda-se inicialmente estimar a rede existente e os recursos de hardware disponíveis que podem ser usados para a operação de um sistema de proteção centralizado.

Para analisar a rede e infraestrutura de hardware, recomenda-se que você siga o processo abaixo:

1. Definir as configurações seguintes da rede na qual a proteção será implementada:
   - Número de segmentos de rede.
   - A velocidade dos canais de comunicação entre os segmentos de rede individuais.
   - Número de dispositivos gerenciados em cada um dos segmentos da rede.
   - Informação de cada canal de comunicação que pode ser alocada para manter a operação da proteção.
2. Determinar o tempo máximo permitido para a execução das principais operações administrativas para todos os dispositivos gerenciados.
3. Analise as informações das etapas 1 e 2, assim como os dados do teste de carga do sistema de administração. Com base na análise, responda às seguintes perguntas:
   - É possível servir todos os clientes com um único Servidor de Administração ou é necessário uma hierarquia de Servidores de Administração?
   - Qual a configuração de hardware dos Servidores de Administração que é necessária para processar todos os clientes dentro dos limites de tempo especificados no etapa 2?
   - É necessário usar pontos de distribuição para reduzir a carga nos canais de comunicação?

Após obter as respostas para a etapa 3 acima, você pode compilar um conjunto de estruturas permitidas de proteção da organização.

Na rede da organização, você pode usar uma das seguintes estruturas de proteção padrão:

- Um Servidor de Administração. Todos os dispositivos cliente são conectados a um único Servidor de Administração. O Servidor de Administração funciona como um ponto de distribuição.
- Um Servidor de Administração com pontos de distribuição. Todos os dispositivos cliente são conectados a um único Servidor de Administração. Alguns dos dispositivos cliente na rede agem como pontos de distribuição.
- Hierarquia de Servidores de Administração Para cada segmento de rede, um Servidor de Administração individual é alocado e se torna parte de uma hierarquia geral de Servidores de Administração. O Servidor de Administração principal funciona como o ponto de distribuição.
- Hierarquia de Servidores de Administração com pontos de distribuição. Para cada um dos segmentos de rede um Servidor de Administração individual é alocado e se torna parte de uma hierarquia geral de Servidores de Administração. Alguns dos dispositivos cliente na rede agem como pontos de distribuição.

Esquemas típicos para implementação do sistema de proteção

Esta seção descreve os esquemas padrão de implementação de um sistema de proteção em uma rede corporativa usando o Kaspersky Security Center.

O sistema deve ser protegido contra qualquer tipo de acesso não autorizado. Recomendamos que você instale todas as atualizações de segurança disponíveis para o sistema operacional antes de instalar o aplicativo em seu dispositivo e de proteger fisicamente o(s) Servidor(es) de Administração e o(s) ponto(s) de distribuição.

Você pode usar o Kaspersky Security Center para implementar um sistema de proteção em uma rede corporativa por meio dos seguintes esquemas de implementação:

- Implementar um sistema de proteção usando o Kaspersky Security Center Web Console.

  Os aplicativos Kaspersky são automaticamente instalados em dispositivos cliente, os quais, por sua vez, são automaticamente conectados ao Servidor de Administração usando o Kaspersky Security Center.

- Implemente um sistema de proteção manualmente usando os pacotes de instalação independentes gerados pelo Kaspersky Security Center.

  A instalação de aplicativos Kaspersky em dispositivos cliente e na estação de trabalho do administrador é executada manualmente; as configurações para a conexão dos dispositivos cliente ao Servidor de Administração são especificadas durante a instalação do Agente de Rede.

  Este método de implementação é recomendado nos casos quando a instalação remota não for possível.

O Kaspersky Security Center não é compatível com a implementação com o uso das políticas de grupo do Microsoft Active Directory®.

Selecionar um DBMS

A tabela a seguir lista as opções válidas de DBMS, assim como as recomendações e restrições quanto ao seu uso.

Recomendações e restrições no DBMS

DBMS	Recomendações e restrições
MySQL (consulte as versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 20.000 dispositivos.
MariaDB (consulte as versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 20.000 dispositivos.
PostgreSQL, Postgres Pro (ver versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos.
Tantor (ver versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos. O Tantor DBMS é compatível somente com o Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.8).

Para obter informações sobre como instalar o DBMS selecionado, consulte a sua documentação.

Recomendamos desativar a tarefa de Inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados.

Se você decidir instalar o DBMS PostgreSQL ou Postgres Pro, certifique-se de ter especificado uma senha para o superusuário. Se a senha não for especificada, o Servidor de Administração pode não conseguir se conectar ao banco de dados.

Caso o MySQL, MariaDB, PostgreSQL ou Postgres Pro seja instalado, use as configurações recomendadas para garantir que o DBMS funcione corretamente.

Caso um DBMS PostgreSQL, MariaDB ou MySQL seja usado, a guia **Eventos** poderá exibir uma lista incompleta de eventos para o dispositivo cliente selecionado. Isso ocorre quando o DBMS armazena uma quantidade muito grande de eventos. É possível aumentar o número de eventos exibidos com a execução de um dos seguintes procedimentos:

- Remoção de eventos desnecessários.
- Redução do prazo de armazenamento para eventos desnecessários.

Para ver uma lista completa de eventos registrados no Servidor de Administração para o dispositivo, use Relatórios.

Fornecer acesso à Internet ao Servidor de Administração

Os seguintes casos necessitam do acesso à Internet ao Servidor de Administração:

- Atualização regular dos bancos de dados, módulos de software e aplicativos Kaspersky
- Atualizando software de terceiros

  Por padrão, a conexão com a Internet não é necessária para que o Servidor de Administração instale atualizações de software da Microsoft nos dispositivos gerenciados. Por exemplo, os dispositivos gerenciados podem baixar as atualizações de software da Microsoft diretamente dos servidores de Atualizações da Microsoft ou do Windows Server com o Microsoft Windows Server Update Services (WSUS) implementado na rede da sua organização. O Servidor de Administração deve estar conectado à Internet nos seguintes casos:

  - Ao usar o Servidor de Administração como servidor WSUS
  - Para instalar atualizações de software de terceiros que não sejam da Microsoft
- Corrigindo vulnerabilidades de software de terceiros

  Uma conexão com a Internet é necessária para que o Servidor de Administração execute as seguintes tarefas:

  - Para fazer uma lista de correções recomendadas para vulnerabilidades em softwares da Microsoft. A lista é criada e atualizada regularmente por especialistas da Kaspersky.
  - Para corrigir vulnerabilidades em software de terceiros que não sejam software da Microsoft.
- Gerenciar dispositivos (computadores portáteis) de usuários fora do escritório
- Gerenciar dispositivos em escritórios remotos
- Interagir com Servidores de Administração principais ou secundários, sediados em escritórios remotos
- Gerenciamento de Dispositivos Móveis

Esta seção descreve formas típicas para fornecer o acesso ao Servidor de Administração por meio da Internet. Cada um dos casos com enfoque no fornecimento de acesso à Internet para o Servidor de Administração pode necessitar de um certificado dedicado do Servidor de Administração.

Acesso à Internet: Servidor de Administração em uma rede local

Se o Servidor de Administração estiver localizado na rede interna de uma empresa, convém tornar a porta 13000 TCP do Servidor de Administração acessível do exterior por meio do reencaminhamento de porta.

Acesso à Internet: Servidor de Administração em DMZ

Se o Servidor de Administração estiver localizado em DMZ da rede da organização, ele não terá acesso à rede interna da organização. Por isso, as seguintes limitações aplicam-se:

- O Servidor de Administração não pode detectar novos dispositivos.
- O Servidor de Administração não pode executar a implementação inicial do Agente de Rede através da instalação forçada em dispositivos na rede interna da organização.

  Isto somente se aplica à instalação inicial do Agente de Rede. Quaisquer atualizações adicionais do Agente de Rede ou da instalação do aplicativo de segurança pode, no entanto, ser executada pelo Servidor de Administração.

Observe que o Kaspersky Security Center Linux não é compatível com a implementação com o uso de políticas de grupo do Microsoft Windows.

É possível usar os pontos de distribuição localizados na rede da organização. Para executar a implementação inicial em dispositivos sem Agente de Rede, você primeiro instala o Agente de Rede em um dos dispositivos e, a seguir, o atribui o status de ponto de distribuição. Como resultado, a instalação inicial do Agente de Rede em outros dispositivos será executada pelo Servidor de Administração através deste ponto de distribuição.

Para assegurar o envio com êxito de notificações para a porta 15000 UDP em dispositivos gerenciados na rede interna da organização, você precisa cobrir toda a rede com pontos de distribuição. Nas propriedades dos pontos de distribuição que foram atribuídos, selecione a caixa de seleção **Não desconectar do Servidor de Administração**. Como resultado, o Servidor de Administração estabelecerá uma conexão contínua com os pontos de distribuição e eles serão capazes de enviar notificações para a porta 15000 UDP nos dispositivos na rede interna da organização (pode ser uma rede IPv4 ou IPv6).

Instalação

Esta seção descreve a instalação do Kaspersky Security Center Linux e do Kaspersky Security Center Web Console.

Configuração do servidor MariaDB x64 para trabalhar com o Kaspersky Security Center Linux

Para configurar corretamente o servidor MariaDB x64 para uso com o Kaspersky Security Center, é preciso utilizar os parâmetros de servidor padrão, exceto aqueles especificados neste artigo.

Configurações recomendadas para o arquivo my.cnf

Para obter mais detalhes sobre a configuração do DBMS, consulte também o procedimento de configuração da conta. Para obter informações sobre a instalação do DBMS, consulte o procedimento de instalação do DBMS.

Para configurar o arquivo my.cnf:

1. Abra o arquivo my.cnf em um editor de texto.

2. Adicione as seguintes linhas na seção [mysqld] do arquivo 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=< 80% da RAM alocada para o DBMS; consulte a documentação do seu DBMS para obter recomendações >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

   Observe que a memória especificada no valor `innodb_buffer_pool_size` é alocado na inicialização do servidor. Caso o tamanho do banco de dados seja menor que o tamanho do buffer especificado, somente a memória necessária será alocada. Caso o MariaDB 10.4.3 ou anterior seja usado, o tamanho real da memória alocada será aproximadamente 10% maior que o tamanho do buffer especificado. Para obter recomendações sobre a configuração de `innodb_buffer_pool_size` e outras informações adicionais, consulte a documentação do MySQL.

   Recomenda-se usar o valor do parâmetro `innodb_flush_log_at_trx_commit=0`, pois os valores "1" ou "2" afetam negativamente a velocidade de operação do MariaDB. Certifique-se de que o parâmetro `innodb_file_per_table` está definido como `1`.

   Para o MariaDB 10.1, insira adicionalmente as seguintes linhas na seção [mysqld]:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

   Para o MariaDB 10.6, insira adicionalmente as seguintes linhas na seção [mysqld]:

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

Por padrão, os complementos do otimizador `join_cache_incremental`, `join_cache_hashed`, `join_cache_bka` estão ativados. Se esses complementos não estiverem ativados, você deve ativá-los.

Para verificar se os complementos do otimizador estão ativados:

1. No console do cliente MariaDB, execute o comando:

   ```
   SELECT @@optimizer_switch;
   ```

2. Verifique se a saída contém as seguintes linhas:

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

   Se essas linhas estiverem presentes e com os valores `on`, os complementos do otimizador serão ativados.

   Se estas linhas estiverem ausentes ou tiverem valores `off`, você precisa fazer o seguinte:

   a. Abra o arquivo my.cnf em um editor de texto.

   b. Adicione as seguintes linhas ao arquivo my.cnf:

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

Os complementos `join_cache_incremental`, `join_cache_hash`, e `join_cache_bka` estão ativados.

Aumente o limite padrão de arquivos que podem ser abertos (descritores de arquivo) para o serviço MariaDB systemd para garantir a estabilidade sob carga.

Para aumentar o limite de descritores de arquivo:

1. Execute o seguinte comando:

   ```
   sudo systemctl edit mariadb.service
   ```

2. Especifique o limite dos descritores de arquivo no parâmetro `LimitNOFILE` da seção `[Service]`:

   ```
   LimitNOFILE=1048576
   ```

3. Execute o seguinte comando para garantir que os parâmetros sejam especificados corretamente:

   ```
   sudo systemd-analyze verify mariadb.service
   ```

4. Execute o seguinte comando para recarregar o processo do systemd:

   ```
   sudo systemctl daemon-reload
   ```

5. Execute o seguinte comando para reiniciar o serviço MariaDB:

   ```
   sudo systemctl restart mariadb.service
   ```

   O limite de descritores de arquivo foi aumentado.

Configuração do servidor de DBMS baseado em PostgreSQL para trabalhar com o Kaspersky Security Center Linux

Este artigo descreve como configurar um Servidor de Administração implantado em um único dispositivo. Se você estiver usando um cluster de SGBD de alta disponibilidade, leia o artigo Preparar um cluster de SGBD de alta disponibilidade para funcionar com o Kaspersky Security Center Linux.

O Kaspersky Security Center Linux é compatível com SGBD baseado em PostgreSQL. Para configurar um servidor de banco de dados PostgreSQL para funcionar com o Kaspersky Security Center Linux, use as configurações padrão do servidor, exceto as listadas neste artigo.

O caminho padrão para o arquivo de configuração é `/etc/postgresql/<VERSION>/main/postgresql.conf`.
In the ALT Linux operating system, the default path is `/var/lib/pgsql/data/postgresql.conf`

Para preparar o SGBD para a instalação do Kaspersky Security Center Linux:

1. Defina as configurações necessárias do servidor de SGBD de acordo com a documentação do SGBD.

2. Para integrar o SGBD ao Kaspersky Security Center Linux da melhor maneira possível, especifique as seguintes configurações:

   - `max_connections = 151`
   - `shared_buffers = N`

     N = 25% do dimensionamento de RAM estimado para o DBMS. Se o DBMS estiver instalado em um dispositivo junto com o Servidor de Administração, o cálculo deve ser feito com base na RAM alocada para o DBMS, e não na RAM total do dispositivo.

     Se a RAM for inferior a 1 GB, deixe o valor padrão.
   - `temp_buffers = 24MB`
   - `work_mem = 16MB`
   - `maintenance_work_mem = 128MB`
   - `max_stack_depth` = tamanho máximo da pilha (execute o comando '`ulimit -s`' para obter esse valor em KB) menos a margem de segurança de 1 MB
   - `max_parallel_workers_per_gather = 0`
   - `standard_conforming_strings = on`

   Caso use o Postgres Pro 15.7 ou Postgres Pro 15.7.1, desative o parâmetro `enable_compound_index_stats`:

   `enable_compound_index_stats = off`

   Recarregue a configuração ou reinicie o servidor do DBMS após atualizar o arquivo de configuração executando o seguinte comando:

   `sudo systemctl restart postgresql-<version>`

   ou

   `sudo systemctl restart postgresql`

3. Crie bancos de dados e contas de usuário.

   Para obter instruções sobre como criar bancos de dados e configurar contas de usuário para um DBMS baseado em PostgreSQL, consulte o artigo Criação de bancos de dados baseados em PostgreSQL e contas de usuário.

O DBMS está pronto para a instalação do Kaspersky Security Center Linux.

Configuração do servidor MySQL x64 para trabalhar com o Kaspersky Security Center Linux

Para configurar corretamente o servidor MySQL x64 para uso com o Kaspersky Security Center, é preciso utilizar os parâmetros de servidor padrão, exceto os aqueles especificados neste artigo.

Se você usa o servidor MySQL para o Kaspersky Security Center, ative a compatibilidade para armazenamento InnoDB e MEMORY e as codificações UTF-8 e UCS-2.

Configurações recomendadas para o arquivo my.cnf

Para obter mais detalhes sobre a configuração do DBMS, consulte também o procedimento de configuração da conta. Para obter informações sobre a instalação do DBMS, consulte o procedimento de instalação do DBMS.

Para configurar o arquivo my.cnf:

1. Abra o arquivo my.cnf em um editor de texto.

2. Adicione as seguintes linhas na seção `[mysqld` do arquivo my.cnf:

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=< 80% da RAM alocada para o DBMS; consulte a documentação do
seu DBMS para obter recomendações >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (na maioria dos casos, o servidor usa pequenas
transações)
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
```

   Observe que a memória especificada no valor `innodb_buffer_pool_size` é alocado na inicialização do servidor. Caso o tamanho do banco de dados seja menor que o tamanho do buffer especificado, somente a memória necessária será alocada. O tamanho real da memória alocada é aproximadamente 10% maior que o tamanho do buffer especificado. Para obter recomendações sobre a configuração de `innodb_buffer_pool_size` e outras informações adicionais, consulte a documentação do MySQL.

   Recomenda-se usar o valor do parâmetro `innodb_flush_log_at_trx_commit = 0`, pois os valores "1" ou "2" afetam negativamente a velocidade de operação do MySQL. Certifique-se de que o parâmetro `innodb_file_per_table` está definido como `1`.

Preparar um cluster DBMS de alta disponibilidade para funcionar com o Kaspersky Security Center Linux

Este artigo descreve as etapas para preparar um cluster DBMS de alta disponibilidade para o Kaspersky Security Center Linux. Se o Servidor de Administração for implantado em um único dispositivo, consulte o artigo Configurar um servidor DBMS baseado em PostgreSQL para funcionar com o Kaspersky Security Center Linux.

A Kaspersky Security Center Linux é compatível com os seguintes clusters de alta disponibilidade:

- Platform V Pangolin
- Alta disponibilidade integrada do Postgres Pro
- Patroni (com balanceador de carga HAProxy opcional)

Uma configuração mínima recomendada de cluster DBMS de alta disponibilidade deve incluir pelo menos três nós.

Para preparar um cluster DBMS de alta disponibilidade para funcionar com o Kaspersky Security Center Linux:

1. Defina o tipo de replicação como síncrona.

   Se você usar o modelo Patroni versão 3.3.1 ou anterior para PostgreSQL, certifique-se de que o parâmetro `synchronous_standby_names` tenha sido aplicado corretamente.

   Para verificar se a replicação síncrona está sendo usada, execute a seguinte consulta no nó principal:

   `SELECT application_name, client_addr, client_hostname, client_port, sync_state FROM pg_stat_replication;`

   Se a coluna `sync_state` exibir valores diferentes de `sync` ou `potential` para qualquer nó, o cluster usará a replicação assíncrona, que não é compatível. Para resolver esse problema, execute um dos seguintes procedimentos:

   Atualize o Patroni para a versão 3.3.2 ou mais recente.

   No arquivo de configuração do Patroni, localize a sub-seção `dcs` da seção `bootstrap` e defina o parâmetro `synchronous_mode` para `true`:

   ```
   bootstrap:
   dcs:
   <...>
   synchronous_mode: true
   ```

2. Em cada nó do cluster de DBMS, configure o arquivo de configuração seguindo as etapas 1 e 2 das instruções Como configurar um servidor de DBMS baseado em PostgreSQL para funcionar com o Kaspersky Security Center Linux.

3. Crie bancos de dados e contas de usuário de acordo com as instruções do artigo Como criar bancos de dados baseados em PostgreSQL e contas de usuário.

4. Configure a descoberta dos nós do cluster de DBMS de uma das seguintes maneiras:

   - Especifique manualmente todos os nós do cluster de DBMS durante a instalação do Kaspersky Security Center Linux.

   - Para a descoberta automática dos nós do cluster, especifique apenas o nome DNS ou o endereço IP do nó de controle ou do nó de réplica durante a instalação do Kaspersky Security Center Linux.

     Para fazer isso:

     a. Em todos os nós do cluster de DBMS de alta disponibilidade, adicione a seguinte linha ao arquivo de configuração `postgresql`:

     `log_hostname=1`

     b. Depois de editar o arquivo de configuração, reinicie o serviço de cluster DBMS em todos os nós de cluster DBMS de alta disponibilidade.

     c. Certifique-se de que o usuário do banco de dados tenha o privilégio `pg_read_all_stats`.

     Você pode conceder esse privilégio executando o seguinte comando:

     `GRANT pg_read_all_stats TO "<kscdbadmin>";`

     Em que `<kscdbadmin>` é o nome do usuário do banco de dados.

     O nome de usuário do banco de dados do Servidor de Administração é especificado durante a instalação do Kaspersky Security Center Linux.

     d. Configure o balanceador de carga para o banco de dados do IAM.

O cluster DBMS de alta disponibilidade está pronto para funcionar com o Kaspersky Security Center Linux.

Instalação do Kaspersky Security Center Linux

Este procedimento descreve como instalar o Kaspersky Security Center Linux.

Antes de instalar o aplicativo, siga estas etapas:

- Planeje a implementação do Kaspersky Security Center Linux de acordo com as recomendações do cenário Introdução.

  Se você cumpriu os pré-requisitos e concluiu as etapas 1 a 4 do cenário, prossiga com a instalação do Servidor de Administração do Kaspersky Security Center Linux.

  > Caso o sistema operacional RED OS 7.3.4 ou posterior ou MSVSPHERE 9.2 ou posterior seja usado, instale o pacote libxcrypt-compat para a função correta do Servidor de Administração.

- Instale o DBMS para o Kaspersky Security Center Linux. Você pode escolher qualquer DBMS compatível.

  Se a sua distribuição Linux não incluir um DBMS compatível, você poderá instalar o DBMS a partir de um repositório de pacotes de terceiros do fornecedor ou de outra fonte confiável.

Depois de instalar o DBMS, siga as instruções correspondentes:

- Configuração do servidor de DBMS baseado em PostgreSQL para trabalhar com o Kaspersky Security Center Linux
- Configuração do servidor MariaDB x64 para trabalhar com o Kaspersky Security Center Linux
- Configuração do servidor MySQL x64 para trabalhar com o Kaspersky Security Center Linux

- Certifique-se de que o servidor DNS esteja disponível na rede.

  Certifique-se de que os endereços FQDN e os nomes DNS dos componentes de servidor do Kaspersky Security Center Linux sejam convertidos corretamente em endereços IP nos sistemas operacionais dos componentes do aplicativo e nos dispositivos de rede.

- Baixe o arquivo de instalação com a localização necessária no site da Kaspersky.

  Escolha o arquivo de instalação que corresponde à distribuição Linux instalada no dispositivo: ksc64_<version_number>_amd64.deb or ksc64-<version_number>.x86_64.rpm.

  > O idioma do Servidor de Administração instalado depende da localização do pacote de distribuição baixado.

Para instalar o Kaspersky Security Center Linux:

1. Crie um grupo de segurança para os serviços do Kaspersky Security Center, um usuário sem privilégios para iniciar os serviços do Servidor de Administração e um usuário sem privilégios para iniciar os serviços do IAM.

   Esses usuários devem ser membros do grupo de segurança do Kaspersky Security Center.

   Para isso, execute os seguintes comandos em sequência (neste exemplo, o grupo de segurança é "kladmins", o usuário para executar os serviços do Servidor de Administração é "ksc" e o usuário para iniciar os serviços do IAM é "ksciam"):

   ```
   sudo adduser ksc
   sudo groupadd kladmins
   sudo gpasswd -a ksc kladmins
   sudo usermod -g kladmins ksc
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

2. Se necessário, aumente o limite padrão de arquivos que podem ser abertos (descritores de arquivo) para as contas usadas para a função dos serviços do Servidor de Administração.

   Para isso, abra o arquivo /etc/security/limits.conf e especifique os limites flexíveis e rígidos dos descritores de arquivo da seguinte forma:

   ```
   ksc soft nofile <max_number_of_opened_files>
   ksc hard nofile <max_number_of_opened_files>
   ```

   Por padrão, os limites dos descritores de arquivo são especificados durante a instalação. O limite flexível de arquivos é de 32.768 arquivos, e o limite rígido de arquivos é de 131.072 arquivos.

3. Execute a instalação do Kaspersky Security Center Linux.

   Dependendo da sua distribuição Linux, execute um dos seguintes comandos:

   ```
   sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
   ```

```
sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm
```

4. Execute o script de configuração inicial do Kaspersky Security Center Linux:

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

5. Leia o Contrato de Licença do Usuário Final (EULA) e a Política de Privacidade. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite os seguintes valores:

   a. Digite `y` (sim), se você entende e aceita integralmente os termos do EULA. Digite `n` (não) se você não aceita os termos do EULA. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos do EULA.

   b. Digite `y` se você entende e aceita os termos da Política de Privacidade e se concorda que seus dados serão tratados e transmitidos (inclusive para países terceiros), conforme descrito na Política de Privacidade. Digite `n` (não) se você não aceita os termos da Política de Privacidade. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos da Política de Privacidade.

6. Quando for solicitado, digite as seguintes configurações:

   a. Selecione o **Standard** como um modo de instalação do Servidor de Administração.

   b. Digite o FQDN ou o nome DNS do Servidor de Administração. Esse nome será usado por outros dispositivos para se conectar com o Servidor de Administração.

   c. Digite o número da porta SSL do Servidor de Administração. O número da porta padrão é 13000.

   d. Avalie o número aproximado de dispositivos que você deseja gerenciar:

   - Se você tem de 1 a 100 dispositivos gerenciados, digite 1.
   - Se você tem de 101 a 1000 dispositivos gerenciados, digite 2.
   - Se você tem mais de 1000 dispositivos gerenciados, digite 3.

   Essa configuração é utilizada para o atraso aleatório automático do início de uma tarefa para aprimorar uma carga de rede. A lista abaixo mostra o intervalo usado para calcular o atraso:

   - 1 a 100 dispositivos gerenciados, valor 1. O atraso não é utilizado.
   - 101 a 1000 dispositivos gerenciados, valor 2. O atraso é de 5 minutos.
   - Mais de 1000 dispositivos gerenciados, valor 3. O atraso é de 10 minutos.

   e. Digite o nome do grupo de segurança criado na etapa 1 (no exemplo, o grupo é `kladmins`).

   f. Digite o nome do usuário que iniciará o serviço do Servidor de Administração criado na etapa 1 (no exemplo, o usuário é `ksc`).

   O usuário deve ser membro do grupo de segurança especificado na etapa 8e.

   g. Digite o nome do usuário que iniciará outros serviços (no exemplo, o grupo é `kladmins`).

   O usuário deve ser membro do grupo de segurança especificado na etapa 8e.

h. Selecione o DBMS que foi instalado para funcionar com o Kaspersky Security Center Linux:

- Caso tenha instalado o MySQL ou o MariaDB, digite 1.
- Se você instalou um DBMS baseado em PostgreSQL, digite 2.

i. Digite o nome DNS ou endereço IP do dispositivo no qual o banco de dados do Servidor de Administração está instalado. Para a instalação local do DBMS, especifique 127.0.0.1.

Para usar um cluster de failover de alta disponibilidade, execute uma das seguintes ações:

- Insira os nomes DNS ou endereços IP e portas de todos os nós no seguinte formato:
  `<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;`
- Especifique somente o nome DNS ou o endereço IP do nó principal ou do nó de réplica.

j. Digite o número da porta do banco de dados. Esta porta é usada para comunicação com o Servidor de Administração. Esta etapa será ignorada se você inserir nomes DNS ou endereços IP e portas de todos os nós de cluster de alta disponibilidade na etapa 8i.

Por padrão, as seguintes portas são usadas:

- Porta `3306` para MySQL ou MariaDB
- Porta `5432` para PostgreSQL ou Postgres Pro

k. Insira o nome do banco de dados do Servidor de Administração (no exemplo dos artigos, o banco de dados `kav`) que você criou seguindo as instruções: Criação de bancos de dados e contas de usuário baseados em PostgreSQL ou Configuração do servidor MariaDB x64 para funcionar com o Kaspersky Security Center Linux.

l. Insira o nome da conta do administrador do banco de dados usada para acessar o banco de dados do Servidor de Administração (no exemplo dos artigos da etapa 8k, `kscdbadmin`).

m. Insira a senha da conta de administrador do banco de dados usada para acessar o banco de dados do Servidor de Administração.

n. Se você instalou um banco de dados baseado em PostgreSQL, poderá especificar o esquema do banco de dados a ser usado pelo Servidor de Administração. Para fazer isso, especifique o nome do esquema.

> O nome do esquema diferencia maiúsculas de minúsculas: use apenas letras minúsculas.

Se você não quiser usar um esquema personalizado, pressione ENTER. Nesse caso, será usado o esquema padrão selecionado no DBMS.

o. Insira o FQDN ou o nome DNS do servidor IAM. Se você não especificar esta variável, o nome DNS do dispositivo com o Servidor de Administração instalado será utilizado.

Insira o valor especificado na etapa 8b.

p. Insira o nome da conta que iniciará o serviço IAM criado na etapa 1. O usuário deve pertencer ao grupo de segurança especificado na etapa 8e (no exemplo da etapa 1, `ksciam`).

q. Selecione o DBMS que foi instalado para funcionar com o serviço IAM:

- Caso tenha instalado o MySQL ou o MariaDB, digite 1.
- Caso tenha instalado o PostgreSQL ou o Postgres Pro, digite 2.

r. Insira o endereço do IAM DBMS a ser usado pelo serviço IAM.

Para usar um cluster de alta disponibilidade, execute uma das seguintes ações:

- Insira os nomes DNS ou endereços IP e portas de todos os nós no seguinte formato:
  `<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;`
- Informe apenas o nome DNS ou o endereço IP do balanceador de carga.

s. Insira o número da porta do IAM DBMS. Esta porta é usada para a comunicação com o serviço IAM. Esta etapa será ignorada se você inserir nomes DNS ou endereços IP e portas de todos os nós de cluster de alta disponibilidade na etapa 8r.

Por padrão, as seguintes portas são usadas:

- Porta 3306 para MySQL ou MariaDB.
- Porta 5432 para PostgreSQL ou Postgres Pro.

t. Insira o nome do banco de dados do IAM a ser usado pelo serviço do IAM (no exemplo, `iam`).

u. Insira o nome de usuário da conta de administrador do banco de dados usada para acessar o banco de dados (no exemplo, `iamdbadmin`).

v. Insira a senha da conta de administrador do banco de dados usada para acessar o banco de dados do IAM.

Aguarde que os serviços sejam adicionados e inicializados automaticamente:

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

w. Se você instalou o PostgreSQL ou o Postgres Pro, poderá especificar o esquema do banco de dados a ser usado pelo IAM. Para fazer isso, especifique o nome do esquema.

Se você não quiser usar um esquema personalizado, pressione ENTER. Nesse caso, é usado o esquema 'public'.

> O nome do esquema diferencia maiúsculas de minúsculas: use apenas letras minúsculas.
> Não especifique os nomes de esquema reservados do IAM: client, iam, ksc, locker, pat, scope, voltron.

x. Crie uma conta que agirá como um administrador do Servidor de Administração. Digite o nome de usuário e senha.

A senha deve estar em conformidade com as seguintes regras:

- A senha de usuário não pode ter menos de 8 nem mais de 256 caracteres.
- A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
  - Letras maiúsculas (A–Z)
  - Letras minúsculas (a-z)
  - Números (0–9)
  - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Se você ignorar esta etapa, poderá usar o seguinte comando para criar um novo usuário mais tarde:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p
```

O usuário será adicionado e o Kaspersky Security Center Linux estará instalado.

Prossiga para a instalação do Kaspersky Security Center Web Console.

Se o Servidor de Administração não tiver acesso ao repositório de pacotes de distribuição de aplicativos para instalação remota, baixe as dependências necessárias para criar pacotes de instalação para instalar aplicativos em dispositivos Windows da seguinte maneira:

1. Crie o sinalizador RIUtilsArchiveDirUsed executando o seguinte comando:

   `/opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1`

2. Execute o seguinte comando para reiniciar o serviço do Servidor de Administração:

   `systemctl restart kladminserver_srv.service`

3. Baixe os módulos adicionais, "Arquivos para instalação remota via Kaspersky Security Center", no site da Kaspersky.

   Os arquivos baixados têm os seguintes nomes:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Não renomeie os arquivos comprimidos.

4. Coloque os arquivos no diretório /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

O Servidor de Administração agora tem as dependências necessárias.

Verificação de serviço

Use os comandos a seguir para verificar se o serviço está sendo executando ou não:

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

Instalação do Kaspersky Security Center Linux no modo silencioso

É possível instalar o Kaspersky Security Center Linux em dispositivos Linux usando um arquivo de resposta para executar uma instalação no modo silencioso, ou seja, sem a participação do usuário. O arquivo de resposta contém um conjunto personalizado de parâmetros de instalação: variáveis e seus respectivos valores.

Antes da instalação:

- Instale o DBMS para o Kaspersky Security Center Linux. Você pode escolher qualquer DBMS compatível. Para obter informações sobre como instalar o DBMS selecionado, consulte a sua documentação.

  Caso a distribuição do sistema operacional baseado em Linux não contenha um DBMS compatível, será possível instalar o DBMS por meio de um repositório de pacotes de terceiros.

  Depois de instalar o DBMS, siga as instruções correspondentes:

  - Configurar o servidor PostgreSQL ou Postgres Pro para uso com o Kaspersky Security Center Linux

    Configuração das contas DBMS para que elas funcionem com o PostgreSQL e o Postgres Pro

    Se você quiser que o Servidor de Administração descubra automaticamente os endereços dos nós de cluster, basta especificar o nome DNS ou o endereço IP do nó de controle ou do nó de réplica durante a instalação. Para isso, certifique-se de ter concluído a etapa 2 das instruções em Preparação de um cluster DBMS de alta disponibilidade para uso com o Kaspersky Security Center Linux.

  - Configuração do servidor MariaDB x64 para uso com o Kaspersky Security Center Linux

    Configuração da conta DBMS para uso com MySQL e MariaDB

  - Configuração do servidor MySQL x64 para uso com o Kaspersky Security Center Linux

    Configuração da conta DBMS para uso com MySQL e MariaDB

- Certifique-se de que o dispositivo com o DBMS instalado não tenha contas de usuário DBMS com os seguintes nomes:
  - client
  - iam
  - ksc

- locker
- pat
- scope
- voltron

- Verifique e confirme se o dispositivo no qual deseja instalar o Kaspersky Security Center Linux está executando em uma das distribuições Linux compatíveis.

  Caso o sistema operacional RED OS 7.3.4 ou posterior ou MSVSPHERE 9.2 ou posterior seja usado, instale o pacote libxcrypt-compat para a função correta do Servidor de Administração.

- Baixe o arquivo de instalação com a localização necessária no site da Kaspersky. Escolha o arquivo de instalação que corresponde à distribuição Linux instalada no seu dispositivo: ksc64_[version_number]_amd64.deb ou ksc64-[version_number].x86_64.rpm.

Para instalar o Kaspersky Security Center Linux no modo silencioso:

1. Leia o Contrato de Licença do Usuário Final. Siga as etapas abaixo somente se entender e aceitar os termos do Contrato de Licença do Usuário Final.

2. Crie um grupo "kladmins" e contas sem privilégios "ksc" e "ksciam" que devem ser membros do grupo "kladmins". Para fazer isso, execute sequencialmente os seguintes comandos em uma conta com privilégios de raiz:

   `adduser ksc`

   `groupadd kladmins`

   `gpasswd -a ksc kladmins`

   `usermod -g kladmins ksc`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

3. No servidor DBMS, crie um banco de dados para o IAM. O nome do banco de dados deve ser diferente daquele instalado para uso com o Kaspersky Security Center Linux. O Servidor de Administração não faz a remoção automática do banco de dados do IAM ao desinstalar ou mover o servidor para outro dispositivo. É necessário fazer a remoção manual do banco de dados.

   - Para PostgreSQL, execute o seguinte comando:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Para MariaDB, execute o seguinte comando:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. Crie o arquivo de resposta (no formato TXT) e adicione a ele uma lista de variáveis no formato `VARIABLE_NAME=variable_value`. Adicione cada variável em uma linha separada. O arquivo de resposta deve incluir as variáveis listadas na tabela abaixo.

5. Defina o valor da variável de ambiente `KLAUTOANSWERS` no ambiente raiz, ou no ambiente do usuário, que contém o nome completo do arquivo de resposta, incluindo o caminho, por exemplo, com o seguinte comando:

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. Execute a instalação do Kaspersky Security Center Linux no modo silencioso e, dependendo da sua distribuição Linux, execute um dos seguintes comandos:

   No ambiente raiz:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
yum install /<path>/ksc64-[version_number].x86_64.rpm -y
```

   No ambiente do usuário:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
sudo -E yum install /<path>/ksc64-[version_number].x86_64.rpm -y
```

7. Crie um usuário para trabalhar com o Kaspersky Security Center Web Console. Para fazer isso, execute o seguinte comando em uma conta com privilégios de root e especifique uma senha com pelo menos 8 caracteres:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

8. Instale o Kaspersky Security Center Web Console.

Variáveis do arquivo de resposta usadas como parâmetros de instalação do Kaspersky Security Center Linux no modo silencioso

Nome da variável	Necessário	Descrição	Valores possíveis
`EULA_ACCEPTED`	Sim	Confirma que entende e aceita por completo os termos do Contrato de Licença de Usuário Final.	1
`PP_ACCEPTED`	Sim	Confirme que entende e aceita os termos da Política de Privacidade.	1
`KLSRV_UNATT_SERVERADDRESS`	Sim	O nome DNS do Servidor de Administração ou o endereço IP estático.	Nome DNS ou endereço IP
`KLSRV_UNATT_PORT_SRV`	Não	O número da porta do Servidor de Administração. Configuração opcional. O valor padrão é 14000.	Número da porta
`KLSRV_UNATT_PORT_SRV_SSL`	Não	O número da porta SSL do Servidor de Administração. Configuração opcional. O valor padrão é 13000.	Número da porta
`KLSRV_UNATT_PORT_KLOAPI`	Não	O número da porta para uso com o OpenAPI. Essa porta também é usada para receber conexões do Kaspersky Security Center Web Console. Configuração opcional. O valor padrão é 13299.	Número da porta

KLSRV_UNATT_PORT_GUI	Não	O número da porta para uso com o utilitário klakaut. Configuração opcional. O valor padrão é 13291. O utilitário klakaut e seu sistema de Ajuda estão localizados na pasta de instalação do Kaspersky Security Center Linux. Esta porta é fechada por padrão. Caso queira utilizar o utilitário klakaut para automatizar a operação do Kaspersky Security Center Linux, abra a porta 13291 através do utilitário klscflag.	Número da porta
KLSRV_UNATT_NETRANGETYPE	Não	O número aproximado de dispositivos que o usuário deseja gerenciar. Essa configuração é usada para otimizar a carga da rede. Configuração opcional. O valor padrão é 1.	1 para 1 a 100 dispositivos gerenciados. 2 para 101 a 1000 dispositivos gerenciados. 3 para mais de 1000 dispositivos gerenciados.
KLSRV_UNATT_DBMS_TYPE	Sim	O tipo de sistema de gerenciamento de banco de dados: MySQL (MariaDB) ou Postgres.	mysql ou postgres
KLSRV_UNATT_DBMS_INSTANCE	Sim	O endereço do servidor de banco de dados. Para usar um cluster do Postgres, um cluster de alta disponibilidade integrado do PostgreSQL ou um cluster do Platform V Pangolin DBMS, insira os nomes DNS ou os endereços IP e as portas de todos os nós no seguinte formato: <fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>; Como alternativa, caso queira usar um cluster DBMS do Platform V Pangolin, basta especificar apenas o nome DNS ou o endereço IP do nó principal, ou do nó de réplica, ao especificar o endereço do DBMS.	Nome DNS ou endereço IP estático do servidor de banco de dados.
KLSRV_UNATT_DBMS_PORT	Sim	Porta do servidor de banco de dados. O valor padrão para o MySQL (MariaDB) é 3306; o valor padrão do Postgres é 5432.	3306 ou 5432
KLSRV_UNATT_DB_NAME	Sim	O nome do banco de dados. O nome do banco de dados deve ser diferente do nome do banco de dados do IAM especificado na variável KLSRV_UNATT_DB_IAM_NAME.	kav
KLSRV_UNATT_DBMS_LOGIN	Sim	O nome de usuário de quem tem acesso ao banco de dados.	
KLSRV_UNATT_DBMS_PASSWORD	Sim	A senha de um usuário que tem acesso ao banco de dados.	
KLSRV_UNATT_DBMS_SCHEMA	Não	O esquema personalizado do DBMS. Se você não especificar um esquema personalizado, o Servidor de Administração usará um esquema padrão. O nome do esquema diferencia maiúsculas de minúsculas: use apenas letras minúsculas. Somente será possível especificar um esquema personalizado se o PostgreSQL ou o Postgres Pro for usado como DBMS. Caso contrário, a variável será ignorada.	database_schema

KLSRV_UNATT_IAM_ADDRESS	Sim	Os navegadores do usuário serão redirecionados para esse endereço pelo OpenIDConnect. Insira o FQDN do Servidor IAM. Você deve usar o nome DNS do Servidor de Administração que foi especificado no parâmetro KLSRV_UNATT_SERVERADDRESS.	FQDN
KLSRV_UNATT_KLIAMUSER	Sim	O nome da conta para iniciar o serviço IAM. A conta deve ser membro do grupo de segurança especificado na variável KLSRV_UNATT_KLADMINSGROUP.	ksciam
KLSRV_UNATT_DBMS_IAM_TYPE	Sim	O tipo de sistema de gerenciamento de banco de dados do IAM: MySQL (MariaDB) ou Postgres.	mysql ou postgres
KLSRV_UNATT_DBMS_IAM_INSTANCE	Sim	O endereço do servidor do banco de dados do IAM. Para usar um cluster do Postgres, um cluster de alta disponibilidade integrado do PostgreSQL ou um cluster do Platform V Pangolin DBMS, insira os nomes DNS ou os endereços IP e as portas de todos os nós no seguinte formato: <fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>; Como alternativa, caso queira usar um cluster DBMS do Platform V Pangolin, basta especificar apenas o nome DNS ou o endereço IP do nó principal, ou do nó de réplica, ao especificar o endereço do DBMS.	Endereço IP
KLSRV_UNATT_DBMS_IAM_PORT	Sim	A porta do servidor do banco de dados do IAM. O valor padrão para o MySQL (MariaDB) é 3306; o valor padrão do Postgres é 5432.	3306 ou 5432
KLSRV_UNATT_DBMS_IAM_LOGIN	Sim	O nome de usuário de um usuário que tem acesso ao banco de dados do IAM. Se o tipo de banco de dados do IAM for o MySQL (MariaDB) e tiver ambas as seguintes configurações: • gtid_mode=ON • gtid_purged=ON|AUTO certifique-se de que o usuário especificado tenha um dos seguintes privilégios de DBMS: • RELOAD • FLUSH_TABLES	
KLSRV_UNATT_DBMS_IAM_PASSWORD	Sim	A senha de um usuário que tem acesso ao banco de dados do IAM.	
KLSRV_UNATT_DBMS_IAM_SCHEMA	Não	O esquema personalizado do DBMS. Se você não especificar um esquema personalizado, o IAM usará um esquema público. Somente será possível especificar um esquema personalizado se o PostgreSQL ou o Postgres Pro for usado como DBMS. Caso contrário, a variável será ignorada. O nome do esquema diferencia maiúsculas de minúsculas: use apenas letras minúsculas. Não especifique os nomes de esquema reservados do IAM: client, iam, ksc, locker, pat, scope, voltron.	database_schema

KLSRV_UNATT_DB_IAM_NAME	Sim	O nome do banco de dados do IAM. O nome do banco de dados do IAM deve ser diferente do nome do banco de dados especificado na variável KLSRV_UNATT_DB_NAME. Especifique um banco de dados vazio criado manualmente.	iamdb
KLSRV_UNATT_KLADMINSGROUP	Sim	O nome do grupo de segurança para serviços.	kladmins
KLSRV_UNATT_KLSRVUSER	Sim	O nome da conta para iniciar o serviço do Servidor de Administração. A conta deve ser membro do grupo de segurança especificado na variável KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Sim	O nome da conta para iniciar outros serviços. A conta deve ser membro do grupo de segurança especificado na variável KLSRV_UNATT_KLADMINSGROUP.	ksc
Caso o Servidor de Administração seja implementado como um Cluster de failover da Kaspersky Security Center Linux, o arquivo de resposta deverá incluir as seguintes variáveis adicionais:			
KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT	Não	Configuração do cluster de failover. Caso o parâmetro seja omitido no arquivo de resposta, será usado o valor padrão. Valores possíveis: 0 – Cluster de failover cujos nós estão localizados em um único data center (valor padrão). 2 – Cluster de failover distribuído geograficamente cujos nós estão localizados em data centers diferentes.	0 ou 2
KLFOC_UNATT_NODE	Sim	O número do nó (1 ou 2).	1 ou 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Sim	O ponto de montagem do compartilhamento de estado.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Sim	O ponto de montagem do compartilhamento de dados.	
KLFOC_UNATT_CONN_MODE	Sim	O modo de conectividade do cluster de failover.	VirtualAdapter ou ExternalLoadBalancer
Caso a variável KLFOC_UNATT_CONN_MODE tenha o valor VirtualAdapter, o arquivo de resposta deve incluir as seguintes variáveis adicionais:			
KLFOC_UNATT_CONN_MODE_VA_NAME	Sim	O nome do adaptador de rede virtual.	
KLFOC_UNATT_CONN_MODE_VA_IPV4	Uma destas variáveis é necessária	O endereço IP do adaptador de rede virtual.	Endereço IP
KLFOC_UNATT_CONN_MODE_VA_IPV6		O endereço IPv6 do adaptador de rede virtual.	Endereço IPv6

Se o Servidor de Administração não tiver acesso ao repositório de pacotes de distribuição de aplicativos para instalação remota, baixe as dependências necessárias para criar pacotes de instalação para instalar aplicativos em dispositivos Windows da seguinte maneira:

1. Crie o sinalizador RIUtilsArchiveDirUsed executando o seguinte comando:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Execute o seguinte comando para reiniciar o serviço do Servidor de Administração:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Baixe os módulos adicionais, "Arquivos para instalação remota via Kaspersky Security Center", no site da Kaspersky.

   Os arquivos baixados têm os seguintes nomes:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Não renomeie os arquivos comprimidos.

4. Coloque os arquivos no diretório /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

O Servidor de Administração agora tem as dependências necessárias.

Instalação do Kaspersky Security Center Linux no Astra Linux no modo de ambiente de software fechado

Esta seção descreve como instalar o Kaspersky Security Center Linux no sistema operacional Astra Linux Special Edition.

Antes da instalação:

- Instale um DBMS.
- Baixar a chave do aplicativo kaspersky_astra_pub_key.gpg.
- Baixe o arquivo de instalação ksc64_[version_number]_amd64.deb do site da Kaspersky.

Em uma conta com privilégios de raiz, execute os comandos fornecidos nesta instrução com alta integridade e zero confidencialidade.

Para instalar o Kaspersky Security Center Linux em um dispositivo que executa o Astra Linux Special Edition (atualização 1.7.2), o Astra Linux Special Edition (atualização 1.6) ou o Astra Linux Special Edition RUSB.10015-01 (atualização 1.8):

1. Abra o arquivo `/etc/digsig/digsig_initramfs.conf` e especifique a seguinte configuração:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Na linha de comando, execute o seguinte comando para instalar o pacote de compatibilidade:

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

3. Crie um diretório para a chave do aplicativo:

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

4. Coloque a chave do aplicativo no diretório criado na etapa anterior:

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

5. Atualize a imagem inicial do sistema de arquivos RAM para todos os kernels do sistema:

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

   Reinicialize o sistema.

6. Crie um grupo 'kladmins' e contas sem privilégios 'ksc' e 'ksciam'. As contas devem ser membros do grupo 'kladmins'. Para fazer isso, execute os seguintes comandos em sequência:

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

7. Execute a instalação do Kaspersky Security Center Linux:

```
# apt install /<path>/ksc64_[ número_da_versão ]_amd64.deb
```

8. Execute a configuração do Kaspersky Security Center Linux:

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

9. Leia o Contrato de Licença do Usuário Final (EULA) e a Política de Privacidade. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite os seguintes valores:

   a. Digite `y` (sim), se você entende e aceita integralmente os termos do EULA. Digite `n` (não) se você não aceita os termos do EULA. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos do EULA.

   b. Digite `y` se você entende e aceita os termos da Política de Privacidade e se concorda que seus dados serão tratados e transmitidos (inclusive para países terceiros), conforme descrito na Política de Privacidade. Digite `n` (não) se você não aceita os termos da Política de Privacidade. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos da Política de Privacidade.

10. Quando for solicitado, digite as seguintes configurações:

    a. Digite o FQDN ou o nome DNS do Servidor de Administração.

    b. Digite o número da porta do Servidor de Administração. O número da porta padrão é 14000.

    c. Digite o número da porta SSL do Servidor de Administração. O número da porta padrão é 13000.

    d. Avalie o número aproximado de dispositivos que você deseja gerenciar:

       - Se você tem de 1 a 100 dispositivos gerenciados, digite 1.
       - Se você tem de 101 a 1000 dispositivos gerenciados, digite 2.
       - Se você tem mais de 1000 dispositivos gerenciados, digite 3.

       Essa configuração é utilizada para o atraso aleatório automático do início de uma tarefa para aprimorar uma carga de rede. A lista abaixo mostra o intervalo usado para calcular o atraso:

       - 1 a 100 dispositivos gerenciados, valor 1. O atraso não é utilizado.
       - 101 a 1000 dispositivos gerenciados, valor 2. O atraso é de 5 minutos.
       - Mais de 1000 dispositivos gerenciados, valor 3. O atraso é de 10 minutos.

    e. Digite o nome do grupo de segurança para serviços. Por padrão, é usado o grupo 'kladmins'.

f. Digite o nome da conta e inicie o serviço do Servidor de Administração. A conta deve ser membro do grupo de segurança digitado. Por padrão, é usada a conta ksc.

g. Digite o nome da conta para iniciar outros serviços. A conta deve ser membro do grupo de segurança digitado. Por padrão, é usada a conta ksc.

h. Selecione o DBMS que foi instalado para funcionar com o Kaspersky Security Center Linux:

- Caso tenha instalado o MySQL ou o MariaDB, digite 1.
- Caso tenha instalado o PostgreSQL ou o Postgres Pro, digite 2.

i. Digite o endereço IP do dispositivo no qual o banco de dados está instalado.

j. Digite o número da porta do banco de dados. Esta porta é usada para comunicação com o Servidor de Administração. Por padrão, as seguintes portas são usadas:

- Porta 3306 para MySQL ou MariaDB.
- Porta 5432 para PostgreSQL ou Postgres Pro.

k. Digite o nome do banco de dados.

l. Insira o login da conta de administrador do banco de dados usado para acessar o banco de dados.

m. Insira a senha da conta de administrador do banco de dados usada para acessar o banco de dados.

n. Insira o FQDN ou o nome DNS do servidor IAM.

Insira o valor especificado na etapa 10a.

o. Insira o nome da conta para iniciar o serviço kliam. A conta deve ser membro do grupo de segurança digitado.

p. Selecione o DBMS que foi instalado para funcionar com o serviço IAM:

- Caso tenha instalado o MySQL ou o MariaDB, digite 1.
- Caso tenha instalado o PostgreSQL ou o Postgres Pro, digite 2.

q. Insira o endereço DBMS a ser usado pelo serviço IAM.

r. Digite o número da porta do banco de dados. Esta porta é usada para a comunicação com o serviço IAM. Por padrão, as seguintes portas são usadas:

- Porta 3306 para MySQL ou MariaDB.
- Porta 5432 para PostgreSQL ou Postgres Pro.

s. Insira o nome do banco de dados a ser usado pelo serviço IAM. O nome do banco de dados usado pelo serviço do IAM deve ser diferente do banco de dados usado pelo Servidor de Administração.

t. Insira o login da conta raiz do banco de dados usada para acessar o banco de dados do IAM.

u. Insira a senha da conta raiz do banco de dados usada para acessar o banco de dados do IAM.

Aguarde que os serviços sejam adicionados e inicializados automaticamente:

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

v. Crie uma conta que agirá como um administrador do Servidor de Administração. Digite o nome de usuário e senha.

A senha deve estar em conformidade com as seguintes regras:

- A senha do usuário deve ter no mínimo 8 e no máximo 256 caracteres.
- A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
  - Letras maiúsculas (A–Z)
  - Letras minúsculas (a-z)
  - Números (0–9)
  - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

O Kaspersky Security Center Linux é instalado e o usuário é adicionado.

Para baixar as dependências necessárias para criar pacotes de instalação do aplicativo para dispositivos Windows:

1. Crie o sinalizador RIUtilsArchiveDirUsed executando o seguinte comando:

   `/opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1`

2. Execute o seguinte comando para reiniciar o serviço do Servidor de Administração:

   `systemctl restart kladminserver_srv.service`

3. Baixe os módulos adicionais, "Arquivos para instalação remota via Kaspersky Security Center", no site da Kaspersky.

   Os arquivos baixados têm os seguintes nomes:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Não renomeie os arquivos comprimidos.

4. Coloque os arquivos no diretório /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

O Servidor de Administração agora tem as dependências necessárias.

Verificação de serviço

Use os comandos a seguir para verificar se o serviço está sendo executando ou não:

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

Instalar o Kaspersky Security Center Web Console

Esta seção descreve como instalar o Kaspersky Security Center Web Console Server (também mencionado como Kaspersky Security Center Web Console) em dispositivos que executam o sistema operacional Linux. Antes da instalação, é necessário instalar um DBMS e o Servidor de Administração do Kaspersky Security Center Linux.

Caso o Kaspersky Security Center Web Console seja instalado no Astra Linux no modo de ambiente de software fechado, siga as instruções específicas para o Astra Linux.

Use um dos seguintes arquivos de instalação que corresponda à distribuição Linux instalada em seu dispositivo:

- Para Debian: ksc-web-console-<número da compilação>.x86_64.deb
- Para sistemas operacionais baseados em RPM: ksc-web-console-<número da compilação>.x86_64.rpm

Para receber o arquivo de instalação, baixe-o do site da Kaspersky.

Para instalar o Kaspersky Security Center Web Console:

1. Certifique-se de que o dispositivo no qual você quer instalar o Kaspersky Security Center Web Console está executando uma das distribuições Linux compatíveis.
2. Leia o Contrato de Licença do Usuário Final. Caso o kit de distribuição do Kaspersky Security Center Linux não inclua um arquivo TXT com o texto do EULA, é possível baixá-lo pelo site da Kaspersky. Se você não aceitar os termos do Contrato de Licença, não instale o aplicativo.
3. Crie um arquivo de resposta que contenha parâmetros para conectar o Kaspersky Security Center Web Console ao Servidor de Administração: `/etc/ksc-web-console-setup.json`.

   Exemplo de um arquivo de resposta que contém o conjunto mínimo de parâmetros

O conjunto de parâmetros do arquivo de resposta depende da versão do Servidor de Administração ao qual o Kaspersky Security Center Web Console se conecta:

- Servidor de Administração versão 16 ou posterior

  Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 16 ou posterior:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Servidor de Administração versão 15.4 ou posterior

  Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 15.4 ou anterior:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

É possível instalar o Kaspersky Security Center Web Console no mesmo dispositivo que o Servidor de Administração ou em um dispositivo diferente. Se o Kaspersky Security Center Web Console for instalado em um dispositivo diferente, o endereço do Kaspersky Security Center Web Console (especificado por `address`) e o endereço do Servidor de Administração (especificado por `iamHost` ou `kscHost`) serão diferentes. Se o Kaspersky Security Center Web Console for instalado no mesmo dispositivo que o Servidor de Administração, esses parâmetros terão os mesmos valores.

O valor `iamHost` deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Para obter informações detalhadas, consulte o artigo: Parâmetros de instalação do Kaspersky Security Center Web Console.

Você pode adicionar vários Servidores de Administração de versões diferentes à lista de servidores confiáveis. Nesse caso, os Servidores podem usar métodos de autenticação diferentes.

Recomendamos que os números de porta acima de 1024 sejam especificados. Se você quiser que o Kaspersky Security Center Web Console funcione em portas abaixo de 1024, após a instalação, certifique-se de ter o utilitário setcap e execute o seguinte comando:

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

Se você não tiver o utilitário setcap, é possível instalá-lo. **Clique neste link para visualizar os comandos.**

Para os sistemas operacionais Debian e Ubuntu, execute um dos seguintes comandos:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Para o SUSE Linux Enterprise Server e o Red Hat Enterprise Linux, execute o comando:

- `sudo zypper install libcap-progs`

Ao instalar o Kaspersky Security Center Web Console no sistema operacional ALT Linux, é necessário especificar um número de porta diferente de 8080, pois essa porta é usada pelo sistema operacional.

Kaspersky Security Center Web Console não pode ser atualizado usando o mesmo arquivo de instalação .rpm. Caso queira alterar as configurações em um arquivo de resposta e usar esse arquivo para reinstalar o aplicativo, primeiro remova o aplicativo e, em seguida, instale-o novamente com o novo arquivo de resposta.

4. Em uma conta com privilégios de raiz, use a linha de comando para executar o arquivo de configuração com a extensão .deb ou .rpm, dependendo da sua distribuição Linux.

   - Para instalar ou atualizar o Kaspersky Security Center Web Console a partir de um arquivo .deb, execute o seguinte comando:
     `sudo apt-get install ksc-web-console-<número da compilação>.x86_64.deb`
   - Para instalar o Kaspersky Security Center Web Console a partir de um arquivo .rpm, execute os seguintes comandos:
     `sudo yum install ksc-web-console-<número da compilação>.x86_64.rpm`

     ou

     `sudo alien -i ksc-web-console-<número da compilação>.x86_64.rpm`
   - Para atualizar de uma versão anterior do Kaspersky Security Center Web Console, execute um dos seguintes comandos:
     - Para os dispositivos que executam sistema operacional baseado em RPM:
       `sudo yum install ksc-web-console-<número da compilação>.x86_64.rpm`
     - Para os dispositivos com sistema operacional baseado em Debian:
       `sudo apt-get install ksc-web-console-<número da compilação>.x86_64.deb`

   Essa ação inicia a descompactação do arquivo de configuração. Espere até que a instalação seja concluída. Kaspersky Security Center Web Console está instalado no seguinte diretório: /var/opt/kaspersky/ksc-web-console.

5. Reinicie os serviços do Kaspersky Security Center Web Console executando o seguinte comando:
   `sudo systemctl restart KSC*`

Quando a instalação estiver concluída, você poderá usar o navegador para abrir e fazer login no Kaspersky Security Center Web Console.

Se o certificado comum do Servidor de Administração for substituído por outro certificado de um backup ou substituído usando o utilitário klsetsrvcert, será necessário remover e reinstalar o Kaspersky Security Center Web Console. Caso contrário, o login no Web Console será restrito.
Se, após a reinstalação, você não conseguir fazer login no Web Console, verifique a configuração do Servidor IAM.

Parâmetros de instalação do Kaspersky Security Center Web Console

Para instalar o Kaspersky Security Center Web Console Server em dispositivos que executam o Linux, você deve criar um arquivo de resposta, um arquivo .json que contém parâmetros para conectar o Kaspersky Security Center Web Console ao Servidor de Administração. Você deve nomear esse arquivo ksc-web-console-setup.json e colocá-lo no seguinte diretório: /etc/ksc-web-console-setup.json.

O conjunto de parâmetros do arquivo de resposta depende da versão do Servidor de Administração ao qual o Kaspersky Security Center Web Console se conecta.

- Servidor de Administração versão 16 ou posterior

  O Servidor de Administração versão 16 ou posterior inclui o Identity and Access Manager (IAM), que fornece autenticação do domínio com conexão única (SSO) no Kaspersky Security Center Web Console. Para que o Kaspersky Security Center Web Console se conecte ao Servidor de Administração, o arquivo de resposta deve conter os parâmetros para a interação com o componente de IAM, mesmo se você não usar conexão única (SSO).

  Exemplo do arquivo de resposta para a instalação do Web Console que se conectará ao Servidor de Administração versão 16 ou posterior. Neste exemplo, o Web Console e o Servidor de Administração são instalados em dispositivos diferentes:

```
{
    "webConsoleAddress": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
    "iamHost": "ksc16.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
    "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "internalCertsTTLDays": 1095,
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

Exemplo do arquivo de resposta para a instalação do Web Console que se conectará ao Servidor de Administração versão 15.4 ou anterior:

Os parâmetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`,, `natsMessageQueueAccount`, `certPath` e `keyPath` são opcionais. Você pode omitir esses parâmetros no arquivo de resposta.

Se você quiser utilizar um certificado personalizado, especifique os parâmetros `certPath` e `keyPath`. Se você não especificar os parâmetros ou especificar apenas um, o navegador da Web continuará informando que a conexão não é privada.

Por motivos de segurança, qua não recomenda especificar os parâmetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` e `natsMessageQueueAccount`.
Se você decidir especificar esses parâmetros, verifique se as contas de usuário que você está configurando pertencem ao mesmo grupo de segurança. Se esses parâmetros não forem definidos, o instalador do Kaspersky Security Center Web Console criará um grupo de segurança padrão e, em seguida, contas de usuário com nomes padrão dentro desse grupo.
Os parâmetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` e `natsMessageQueueAccount` não devem ser usados separadamente uns dos outros: especifique os valores para todos esses parâmetros ou não especifique nenhum deles.

É possível instalar o Kaspersky Security Center Web Console no mesmo dispositivo que o Servidor de Administração ou em um dispositivo diferente. Se o Kaspersky Security Center Web Console for instalado em um dispositivo diferente, o endereço do Kaspersky Security Center Web Console (especificado por `webConsoleAddress`) e o endereço do Servidor de Administração (especificado por `iamHost` ou `kscHost`) serão diferentes. Se o Kaspersky Security Center Web Console for instalado no mesmo dispositivo que o Servidor de Administração, esses parâmetros terão os mesmos valores.

O valor `iamHost` deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Recomendamos que os números de porta acima de 1024 sejam especificados. Caso queira que o Kaspersky Security Center Web Console funcione em portas abaixo de 1024, execute o seguinte comando após a instalação:

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

Se você não tiver o utilitário setcap, é possível instalá-lo. **Clique neste link para visualizar os comandos**.

Para os sistemas operacionais Debian e Ubuntu, execute um dos seguintes comandos:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Para o SUSE Linux Enterprise Server e o Red Hat Enterprise Linux, execute o comando:

- `sudo zypper install libcap-progs`

Ao instalar o Kaspersky Security Center Web Console no sistema operacional ALT Linux, é necessário especificar um número de porta diferente de 8080, pois essa porta é usada pelo sistema operacional.

A tabela abaixo descreve os parâmetros que podem ser especificados em um arquivo de resposta.

Parâmetros para instalar o Kaspersky Security Center Web Console em dispositivos que executam o Linux

Configuração	Descrição	Valores disponíveis
`webConsoleAddress`	Endereço do dispositivo (FQDN ou nome do host) em que o Kaspersky Security Center Web Console está instalado (necessário). Se você instalar o Kaspersky Security Center Web Console no servidor do Kaspersky Security Center, use o endereço especificado ao instalar o Kaspersky Security Center Linux. Se você instalar o Kaspersky Security Center Web Console em um dispositivo diferente, especifique o endereço do dispositivo (FQDN ou nome do host) que será utilizado pelo navegador para se conectar ao servidor do Kaspersky Security Center Web Console.	Valor da sequência de caracteres. Exemplo: `"ksc.example.com"`
`port`	Porta usada pelo Kaspersky Security Center Web Console para receber conexões de navegadores da Web (necessário).	Valor numérico. O valor recomendado é 8080 (exceto par operacional ALT Linux).
`defaultLangId`	Idioma da interface do usuário (por padrão, `1033`). Se necessário, você pode alterar o idioma da interface do Kaspersky Security Center Web Console.	Código numérico do idioma: • Alemão: `1031` • Inglês: `1033` • Espanhol: `1034` • Espanhol (México): `2058` • Francês: `1036` • Italiano: `1040` • Japonês: `1041` • Cazaque: `1087` • Polonês: `1045` • Português (Brasil): `1046` • Russo: `1049` • Turco: `1055` • Chinês simplificado: `2052` • Chinês tradicional: `1028` Se nenhum valor for especificado, o idiom US) será utilizado.
`enableLog`	Ativar ou não ativar o registro de rastreamento do Kaspersky Security Center Web Console. Recomendamos que você altere o valor padrão dos parâmetros somente se solicitado por um especialista do Suporte Técnico da Kaspersky.	Valor booleano: • `true`. O registro está ativado. • `false`. O registro está desativado (s padrão).

Configuração	Descrição	Valores disponíveis
`trusted`	Lista de endereços de Servidores de Administração confiáveis aos quais o Kaspersky Security Center Web Console pode se conectar. Você pode adicionar vários Servidores de Administração de versões diferentes à lista de servidores confiáveis. Para o Servidor de Administração versão 16 ou posterior: • Nome do Servidor de Administração que será exibido na janela de login. • `iamHost` é o endereço (FQDN ou nome do host) do Servidor de Administração, que inclui o componente de IAM (iniciando com a Kaspersky Security Center Linux versão 16) e ao qual o Kaspersky Security Center Web Console se conecta. O valor `iamHost` deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` • `iamOAuthPort` é a porta utilizada para trocar tokens de autenticação por meio do protocolo de autenticação OpenID Connect (o valor padrão é 4444). Esta porta é utilizada tanto para a comunicação entre o Kaspersky Security Center Web Console Server e o Servidor de Administração, quanto entre o navegador (utilizado com o Kaspersky Security Center Web Console) e o Servidor de Administração. • `iamProxyPort` é a porta usada para conectar o Kaspersky Security Center Web Console Server ao Servidor de Administração (o valor padrão é 9050). • `iamCertPath` é o caminho para o certificado IAM. O certificado IAM é criado automaticamente na primeira vez que você executa o Servidor de Administração. O certificado está localizado no dispositivo no qual o Servidor de Administração está instalado. O caminho padrão para o certificado: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem. O certificado IAM autoassinado é rotacionado automaticamente. • `iamPATPath` é o caminho para o token usado para o registro do Kaspersky Security Center Web Console como um cliente OAuth no IAM. Este arquivo é gerado automaticamente na primeira vez que você executa o Servidor de Administração. O token está localizado no dispositivo no qual o Servidor de Administração está instalado. O caminho padrão para o token: /var/opt/kaspersky/klnagent_srv/iam/initial_token.txt. A validade do token é indefinida e não requer rotação. • `kscPort` é a porta usada para conectar o Kaspersky Security Center Web Console ao Servidor de Administração via OpenAPI (o valor padrão é 13299). • `kscCertPath` é o caminho para o certificado do Servidor de Administração. O certificado está localizado no dispositivo no qual o Servidor de Administração está instalado. O caminho padrão para o certificado é: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer.	Uma seção do arquivo JSON no seguinte `"trusted": { "Administration Server v16": { "iamHost": "ksc-iam.example.com", "iamOAuthPort": 4444, "iamProxyPort": 9050, "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_c "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initia "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ }, "Administration Server v15.4": { "kscHost": "ksc.example.com", "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ } }` Você pode especificar qualquer nome do Administração em vez de `Administrati v16` e `Administration Server v15.4`

Configuração	Descrição	Valores disponíveis
	Para o Servidor de Administração versão 15.4 ou anterior: • Nome do Servidor de Administração que será exibido na janela de login. • `kscHost` é o endereço (FQDN ou nome do host) do Servidor de Administração ao qual o Kaspersky Security Center Web Console se conecta. • `kscPort` é a porta OpenAPI que é utilizada para conectar o Kaspersky Security Center Web Console Server ao Servidor de Administração (o valor padrão é 13299). • `kscCertPath` é o caminho para o certificado do Servidor de Administração. O certificado está localizado no dispositivo no qual o Servidor de Administração está instalado. O caminho padrão para o certificado é: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer. Ao instalar o Kaspersky Security Center Web Console em um dispositivo diferente daquele em que o Servidor de Administração está instalado, copie do dispositivo com o Servidor de Administração instalado para o dispositivo de destino o arquivo de certificado do Servidor de Administração (especificado por `kscCertPath`), o arquivo de certificado do IAM (especificado por `iamCertPath`) e o arquivo de token (especificado por `iamPATPath`). Especifique o caminho local para esses arquivos no arquivo de resposta para o instalador do Web Console.	
`acceptEula`	Se você aceita ou não os termos do Contrato de Licença do Usuário Final (EULA). O arquivo que contém os termos do EULA é baixado junto com o arquivo de instalação.	Valor booleano: • `true` – Confirmo que li, entendi e ac integralmente os termos e condições Contrato de Licença do Usuário Fina • `false` – Eu não aceito os termos do Licença (selecionado por padrão). Caso nenhum valor seja especificado, o ir Kaspersky Security Center Web Console e perguntará se você concorda ou não er seus termos.
`certDomain`	Se você quiser gerar um novo certificado autoassinado, use este parâmetro para especificar o FQDN para conectar o navegador ao Kaspersky Security Center Web Console.	Valor da sequência de caracteres.
`certPath`	Use este parâmetro para indicar o caminho do certificado personalizado do Kaspersky Security Center Web Console que seja confiável em sua infraestrutura e atenda aos requisitos para certificados personalizados. Você pode especificar apenas uma chave privada (`keyPath`) para um certificado ou para uma cadeia de certificados.	Valor da sequência de caracteres. Certificados criptografados não são com Kaspersky Security Center Web Console No dispositivo onde o Kaspersky Security Console será instalado, informe o caminh certificado no formato de codificação PE Exemplo: `/root/server.crt`
`keyPath`	Use o parâmetro para especificar o caminho para a chave privada associada ao certificado personalizado do Kaspersky Security Center Web Console especificado no parâmetro `certPath`.	Valor da sequência de caracteres. O arquivo com a chave privada não deve criptografado. No dispositivo onde o Kaspersky Security Console será instalado, informe o caminh chave no formato de codificação PEM. Exemplo: `/root/key-without-passph`
`webConsoleAccount`	Nome da conta sob a qual o serviço do Kaspersky Security Center Web Console é executado.	Valor da sequência de caracteres no segu `"<nome do grupo>:<nome de usuár` Exemplo: `"Group1:User1"`. Se nenhum valor for especificado, o insta Kaspersky Security Center Web Console nova conta com o nome padrão `user_management_%uid%`.

Configuração	Descrição	Valores disponíveis
`managementServiceAccount`	Nome da conta sob a qual o Serviço de gerenciamento do Kaspersky Security Center Web Console é executado.	Valor da sequência de caracteres no segu `"< nome do grupo >:< nome de usuár` Exemplo: `"Group1:User2"`. Se nenhum valor for especificado, o insta Kaspersky Security Center Web Console nova conta com o nome padrão `user_nc`
`serviceWebConsoleAccount`	Nome da conta sob a qual o serviço do Kaspersky Security Center Web Console é executado.	Valor da sequência de caracteres no segu `"< nome do grupo >:< nome de usuár` Exemplo: `"Group1:User3"`. Se nenhum valor for especificado, o insta Kaspersky Security Center Web Console nova conta com o nome padrão `user_svc_nodejs_%uid%`.
`pluginAccount`	Nome da conta sob a qual o serviço de Plug-ins de produto do Kaspersky Security Center é executado.	Valor da sequência de caracteres no segu `"< nome do grupo >:< nome de usuár` Exemplo: `"Group1:User4"`. Se nenhum valor for especificado, o insta Kaspersky Security Center Web Console nova conta com o nome padrão `user_web_plugin_%uid%`.
`natsMessageQueueAccount`	Nome da conta utilizada para executar o serviço NATS do Kaspersky Security Center Web Console.	Valor da sequência de caracteres no segu `"< nome do grupo >:< nome de usuár` Exemplo: `"Group1:User6"`. Se nenhum valor for especificado, o insta Kaspersky Security Center Web Console nova conta com o nome padrão `user_message_queue_%uid%`.
`internalCertsTTLDays`	Prazo de validade dos certificados internos do Kaspersky Security Center Web Console.	Configuração opcional. O valor padrão é

Instalação do Kaspersky Security Center Web Console no Astra Linux no modo de ambiente de software fechado

Esta seção descreve como instalar o Kaspersky Security Center Web Console Server (também mencionado como Kaspersky Security Center Web Console) no sistema operacional Astra Linux Special Edition. Antes da instalação, é necessário instalar um DBMS e o Servidor de Administração do Kaspersky Security Center Linux.

Para instalar o Kaspersky Security Center Web Console:

1. Certifique-se de que o dispositivo no qual você quer instalar o Kaspersky Security Center Web Console está executando uma das distribuições Linux compatíveis.

2. Leia o Contrato de Licença do Usuário Final. Caso o kit de distribuição do Kaspersky Security Center Linux não inclua um arquivo TXT com o texto do EULA, é possível baixá-lo pelo site da Kaspersky. Se você não aceitar os termos do Contrato de Licença, não instale o aplicativo.

3. Crie um arquivo de resposta que contenha parâmetros para conectar o Kaspersky Security Center Web Console ao Servidor de Administração: `/etc/ksc-web-console-setup.json`.

   Exemplo de um arquivo de resposta que contém o conjunto mínimo de parâmetros

O conjunto de parâmetros do arquivo de resposta depende da versão do Servidor de Administração ao qual o Kaspersky Security Center Web Console se conecta:

- Servidor de Administração versão 16 ou posterior

  Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 16 ou posterior:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Servidor de Administração versão 15.4 ou posterior

  Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 15.4 ou anterior:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

É possível instalar o Kaspersky Security Center Web Console no mesmo dispositivo que o Servidor de Administração ou em um dispositivo diferente. Se o Kaspersky Security Center Web Console for instalado em um dispositivo diferente, o endereço do Kaspersky Security Center Web Console (especificado por `address`) e o endereço do Servidor de Administração (especificado por `iamHost` ou `kscHost`) serão diferentes. Se o Kaspersky Security Center Web Console for instalado no mesmo dispositivo que o Servidor de Administração, esses parâmetros terão os mesmos valores.

O valor `iamHost` deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Para obter informações detalhadas, consulte o artigo: Parâmetros de instalação do Kaspersky Security Center Web Console.

Você pode adicionar vários Servidores de Administração de versões diferentes à lista de servidores confiáveis. Nesse caso, os Servidores podem usar métodos de autenticação diferentes.

4. Abra o arquivo `/etc/digsig/digsig_initramfs.conf` e especifique a seguinte configuração:

```
DIGSIG_ELF_MODE=1
```

5. Na linha de comando, execute o seguinte comando para instalar o pacote de compatibilidade:

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

6. Crie um diretório para a chave do aplicativo:

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

7. Coloque a chave do aplicativo `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` no diretório criado na etapa anterior:

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

Se o kit de distribuição do Kaspersky Security Center Linux não incluir a chave do aplicativo kaspersky_astra_pub_key.gpg, você poderá baixá-lo clicando no link: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Atualize os discos RAM:

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

Reinicialize o sistema.

9. Em uma conta com privilégios de raiz, use a linha de comando para executar o arquivo de instalação. Para receber o arquivo de instalação, baixe-o do site da Kaspersky.

- Para instalar ou atualizar o Kaspersky Security Center Web Console, execute o seguinte comando:

```
sudo apt-get install ksc-web-console-<número da compilação>.x86_64.deb
```

- Para atualizar de uma versão anterior do Kaspersky Security Center Web Console, execute o seguinte comando:

```
sudo apt-get install ksc-web-console-<número da compilação>.x86_64.deb
```

Essa ação inicia a descompactação do arquivo de configuração. Espere até que a instalação seja concluída. Kaspersky Security Center Web Console está instalado no seguinte diretório: `/var/opt/kaspersky/ksc-web-console`.

10. Reinicie os serviços do Kaspersky Security Center Web Console executando o seguinte comando:

```
sudo systemctl restart KSC*
```

Quando a instalação estiver concluída, você poderá usar o navegador para abrir e fazer login no Kaspersky Security Center Web Console.

Instalação do Kaspersky Security Center Linux com um script

O script `ksc_fast_install.py` permite implementar o Kaspersky Security Center Linux e executar a configuração inicial de seus componentes: Servidor de Administração e Web Console, incluindo DBMS e pacotes de suporte necessários.

O script lê os parâmetros do arquivo de parâmetro. Os valores padrão dos parâmetros são usados. Se necessário, você pode alterar os valores.

Como funciona o script

Durante a execução, o script:

- Verifica se as condições são atendidas:
  - Você tem os direitos necessários para a execução do script.
  - O script é compatível com o sistema operacional e o DBMS.
  - Os EULAs e a Política de Privacidade são aceitos.

    Se você não os aceitar no arquivo de parâmetro, será solicitado que os aceite após executar o script.
  - Requisitos de hardware para o Servidor de Administração e o Web Console.

    Os requisitos são definidos no Guia de dimensionamento.
- Instala o DBMS (se ainda não estiver instalado) e configura seus parâmetros
- Cria bancos de dados do Kaspersky Security Center, configura credenciais do SO
- Instala o Servidor de Administração, Web Console
- Fornece login e senha para entrar no Web Console.

  Antes de fechar o terminal da linha de comando, salve as credenciais de uma forma prática. Se você perder as credenciais, será necessário adicionar uma nova conta de usuário executando o comando:
  `` `/opt/kaspersky/ksc64/sbin/kladduser -n <user>` ``

Se uma ou mais condições não forem atendidas ou ocorrer um erro, o script será encerrado e uma notificação correspondente será exibida.

O script não inclui ações para proteção do sistema. Para reduzir o risco de comprometimento do Kaspersky Security Center, considere as recomendações do Guia de proteção.
O método de instalação baseado em script é aplicável para implementar o Kaspersky Security Center Linux versão 16.3 e posteriores em um dispositivo sem o Kaspersky Security Center Linux.
É necessário o Python 3.6 ou posterior para executar o script.

A implementação só é possível se o dispositivo atual não tiver o Kaspersky Security Center Linux instalado.

Não é possível usar o script para atualizar o Kaspersky Security Center Linux para uma nova versão nem quando um cluster de failover do Kaspersky Security Center Linux estiver implementado.

O script `ksc_fast_install.py` é compatível com a instalação do Kaspersky Security Center Linux nas versões de sistemas operacionais com DBMSs descritos na tabela.

Operating system version	DBMS
Ubuntu Server 26.04 LTS	PostgreSQL 18 MySQL 8.4 (compilação 8.4.10)
RED OS 8	PostgreSQL 16 MariaDB 10.11 (compilação 10.11.18)
Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.8.5)	PostgreSQL 15 MariaDB 10.11 (compilação 10.11.13)
CentOS Stream 10	PostgreSQL 18 MariaDB 10.11 (compilação 10.11.13)

O esquema de banco de dados personalizado não é compatível com o script.

Como executar a implementação por meio do script

Pré-requisitos

Antes de executar o script:

- Atualize seu sistema operacional executando um dos comandos: `dnf update` ou `apt update`
- Obtenha os privilégios de superusuário executando o comando: `sudo -i`
- Permita a execução do script executando o comando: `chmod +x ./ksc_fast_install.py`
- Confira se o repositório do seu sistema operacional contém o DBMS compatível executando o comando: `sudo apt policy postgresql`

Para implementar o Kaspersky Security Center Linux executando o script:

1. No site da Kaspersky, baixe os seguintes itens:
   - Pacotes de distribuição .deb ou .rpm para o Servidor de Administração e o Web Console.
   - O arquivo "Script de instalação do KSC".

   > Ao usar o script, selecione os pacotes de distribuição do Servidor de Administração e do Web Console compatíveis com o gerenciador de pacotes do seu sistema operacional.

A compactação inclui os seguintes arquivos:

- Arquivo de script `ksc_fast_install.py`.
- Arquivo de parâmetro.

  O nome do arquivo padrão é `params.txt`. Se quiser renomear o arquivo, certifique-se de especificar o novo nome por meio do parâmetro `--params` ao executar o script no terminal da linha de comando.
- Arquivo com o EULA e a Política de Privacidade do Servidor de Administração.
- Arquivo com o EULA do Kaspersky Security Center Web Console.
- Arquivos com somas de hash dos EULAs.

2. Coloque todos os arquivos baixados no mesmo diretório local.
3. Se necessário, configure o arquivo de parâmetro.

   Clique aqui para visualizar o exemplo de arquivo de parâmetro com a descrição de seus parâmetros

```
# Required parameters:

#klfi_server_eula_accepted=N

#klfi_nwc_eula_accepted=N

#klfi_pp_accepted=N

# Optional parameters:

#klfi_klserver_db=KAV

#klfi_klserver_dbuser=klserver

#klfi_klserver_address=

#klfi_kliam_db=KAV_IAM

#klfi_kliam_dbuser=kliam

#klfi_kliam_address=

#klfi_sys_group_kladmin=kladmins

#klfi_sys_user_klserver=klsrvuser

#klfi_sys_user_kliam=kliamuser

#klfi_sys_user_svc=klsvcuser

#klfi_nwc_port=8080

#klfi_display_name=

#klfi_netsize=M
```

Os parâmetros `klfi_server_eula_accepted=N`, `klfi_nwc_eula_accepted=N` e `klfi_pp_accepted=N` são obrigatórios e estão sempre presentes no arquivo de parâmetros. Os outros parâmetros são opcionais.

Para os parâmetros obrigatórios:

- Se você alterar o valor padrão sem remover o comentário de uma linha, será necessário aceitar o EULA e a Política de Privacidade.
- Se você especificar um valor diferente de `Y` ou `N`, será necessário aceitar o EULA e a Política de Privacidade, independentemente de ter removido o comentário da linha.
- Se você remover o comentário da linha sem alterar o valor padrão `N`, o script não funcionará.
- Se você remover o comentário da linha e definir o valor `Y`, o script não fará nenhuma solicitação.

Parâmetro e seu valor padrão	Descrição do parâmetro e outros valores possíveis (se houver)
`klfi_server_eula_accepted=N`	Contrato de Licença de Usuário Final do Servidor de Administração. Valores possíveis: • EULA do `Y` aceito. • Eula do `N` não aceito.
`klfi_nwc_eula_accepted=N`	Contrato de Licença de Usuário Final do Kaspersky Security Center Web Console. Valores possíveis: • EULA do `Y` aceito. • Eula do `N` não aceito.
`klfi_pp_accepted=N`	Política de Privacidade. Valores possíveis: • Política de Privacidade do `Y` aceita. • Política de Privacidade do `N` não aceita.
`klfi_klserver_db=KAV`	O nome do banco de dados do Servidor de Administração. O nome deve ser diferente daquele do banco de dados do IAM especificado no parâmetro `klfi_kliam_db`.
`klfi_kliam_db=KAV_IAM`	O nome do banco de dados do IAM. O nome deve ser diferente daquele do banco de dados do Servidor de Administração especificado no parâmetro `klfi_klserver_db`.
`klfi_klserver_dbuser=klserver`	Nome do usuário do banco de dados do Servidor de Administração.
`klfi_kliam_dbuser=kliam`	Nome do usuário do banco de dados do IAM.
`klfi_klserver_address=FQDN`	O FQDN do Servidor de Administração ou o nome do dispositivo atual. Se o valor do parâmetro não for especificado, o script definirá automaticamente o FQDN ou o nome do dispositivo em que você executa o script. Se o script não conseguir definir os valores, a instalação será concluída com um erro.
`klfi_kliam_address=FQDN`	O FQDN do Servidor IAM ou o nome do dispositivo atual. Se o valor do parâmetro não for especificado, o script definirá automaticamente o FQDN ou o nome do dispositivo em que você executa o script. Se o script não conseguir definir os valores, a instalação será concluída com um erro.
`klfi_sys_group_kladmin=kladmins`	O nome do grupo de segurança para serviços.
`klfi_sys_user_klserver=klsrvuser`	O nome da conta para iniciar o serviço do Servidor de Administração.
`klfi_sys_user_kliam=kliamuser`	O nome da conta para iniciar o serviço IAM.
`klfi_sys_user_svc=klsvcuser`	O nome da conta para iniciar outros serviços.
`klfi_nwc_port=8080`	Porta para conexão com o Kaspersky Security Center Web Console.

`klfi_display_name=FQDN`	Nome do Servidor de Administração que será exibido na janela de login.

`klfi_netsize=M`	O número aproximado de dispositivos que o usuário deseja gerenciar.
	Cada estimativa considera os recursos necessários para executar os aplicativos da Kaspersky. O cálculo abrange a operação simultânea do Servidor de Administração, do Agente de Rede, do Kaspersky Security Center Web Console e do Kaspersky Endpoint Security for Linux em um único dispositivo.
	O armazenamento das cópias de backup do Servidor de Administração não está incluído nesses cálculos. Use um recurso de arquivo externo como ponto de montagem para armazenar cópias de backup em um dispositivo separado ou aumente o espaço disponível em disco para incluir o armazenamento de cópias de backup.
	Qua recomendamos adicionar mais 4–6 GB de RAM e 20 GB de espaço livre em disco para a instalação do sistema operacional.
	Estimativa de recursos de hardware por tamanho da rede:
	• `S` – 1 a 1.000 dispositivos gerenciados.
	  • CPU – 8 núcleos
	  • RAM – 16 GB
	  • Espaço disponível em disco para o diretório `/var` – 70 GB, 300 IOPS ou mais
	• `M` – 1.001 a 10.000 dispositivos gerenciados.
	  • CPU – 12 núcleos
	  • RAM – 24 GB
	  • Espaço disponível em disco para o diretório `/var` – 340 GB, 300 IOPS ou mais
	• `L` – 10.001 a 30.000 dispositivos gerenciados.
	  • CPU – 20 núcleos
	  • RAM – 40 GB
	  • Espaço disponível em disco para o diretório `/var` – 490 GB, 300 IOPS ou mais
	• `XL` – 30.001 a 50.000 dispositivos gerenciados.
	  • CPU – 28 núcleos
	  • RAM – 54 GB
	  • Espaço disponível em disco para o diretório `/var` – 640 GB, 300 IOPS ou mais

Há comentários nas linhas do arquivo de parâmetros. Se quiser configurar os valores, remova o símbolo *#* no início da linha da qual deseja remover o comentário.

Os parâmetros `klfi_server_eula_accepted`, `klfi_nwc_eula_accepted` e `klfi_pp_accepted` são obrigatórios, e o valor padrão deles é `N`. Se você executar o script sem alterar esses valores no arquivo de configurações, será solicitado que aceite o Contrato de Licença de Usuário Final e a Política de Privacidade.

4. Execute o script.

Após a execução do script, é exibida uma notificação sobre a implementação bem-sucedida dos componentes do Kaspersky Security Center Linux, assim como o login e a senha para entrar no Web Console.

Se as condições para a instalação baseada em script não forem atendidas, parâmetros desconhecidos forem especificados no arquivo de parâmetro ou se um parâmetro for repetido várias vezes, o script retornará um erro e uma notificação correspondente será exibida.

Se o script detectar incorretamente RAM insuficiente durante a etapa de descoberta de recursos, desative o uso de RAM dinâmica durante a instalação.

Se ocorrer um erro ao instalar os componentes do Kaspersky Security Center Linux ou o DBMS, o script reverterá as alterações e será encerrado.

Reversão da instalação malsucedida

Se ocorrer um erro durante a instalação dos componentes do Kaspersky Security Center Linux ou do DBMS, a reversão será executada automaticamente pelo script. O componente ou o DBMS instalado antes da ocorrência do erro será excluído.

A atualização de pacotes do sistema operacional e a instalação de pacotes de suporte não serão revertidas.

Se você encerrar o script manualmente, as etapas concluídas com sucesso não serão revertidas. Na próxima vez que você executar o script (usando o comando `python3 ksc_fast_install.py`), a instalação será retomada a partir da etapa em que foi interrompida. Se você não quiser retomar a instalação, execute o script com a opção `rollback`: `python3 ksc_fast_install.py rollback.`. Isso faz com que o script reverta todas as ações executadas antes de ser interrompido.

Implementação do cluster de failover do Kaspersky Security Center Linux

Um cluster de failover do Kaspersky Security Center Linux garante a alta disponibilidade do Kaspersky Security Center Linux e minimiza o tempo de inatividade do Servidor de Administração em caso de falha. O cluster de failover é baseado em duas instâncias idênticas do Kaspersky Security Center Linux, instaladas em dois computadores. Uma das instâncias funciona como o nó ativo e a outra, como o nó passivo. O nó ativo gerencia a proteção dos dispositivos clientes, enquanto o passivo está preparado para assumir todas as funções do nó ativo caso o nó ativo falhe. Quando ocorre uma falha, o nó passivo torna-se ativo e o nó ativo torna-se passivo.

O cluster de failover do Kaspersky Security Center Linux é compatível com duas configurações:

- Cluster de failover cujos nós estão localizados em um único data center.
- Cluster de failover distribuído geograficamente cujos nós estão localizados em data centers diferentes.

Em um cluster de failover do Kaspersky Security Center Linux, todos os seus serviços são gerenciados automaticamente. Não tente reiniciar os serviços manualmente.

Utilize o recurso syslog para a resolução de problemas.

Condições de alternância

O cluster de failover alterna o gerenciamento de proteção dos dispositivos clientes do nó ativo para o nó passivo se qualquer um dos seguintes eventos ocorrer no nó ativo:

- O nó ativo foi interrompido devido a uma falha de software ou hardware.
- O nó ativo foi temporariamente interrompido por atividades de manutenção.
- Pelo menos um dos serviços (ou processos) do Kaspersky Security Center Linux falhou ou foi encerrado acidentalmente. Os serviços do Kaspersky Security Center Linux são os seguintes: klnagent_klfoc, kladminserver_klfoc, klactprx_klfoc, klwebsrv_klfoc.
- A conexão de rede entre o nó ativo e o armazenamento no servidor de arquivos foi interrompida ou encerrada (somente para o cluster localizado em um único data center).

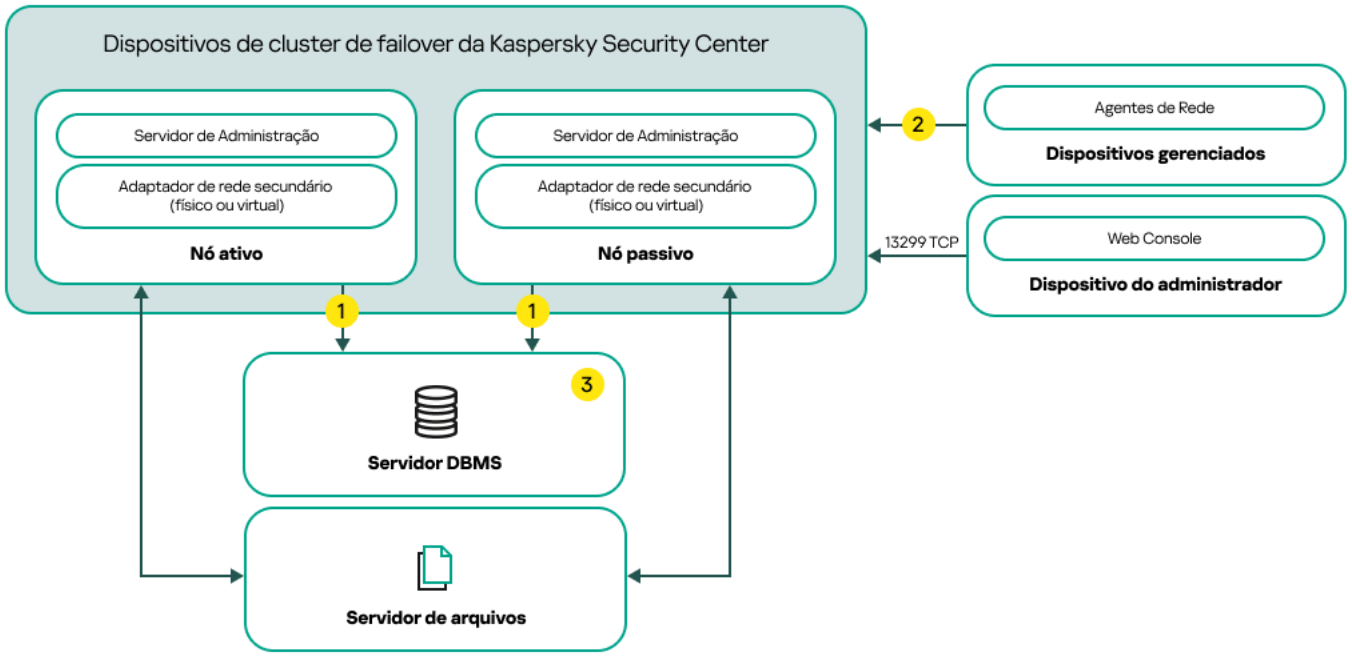
Cluster de failover do Kaspersky Security Center Linux. Esquemas de implementação

É possível escolher um dos seguintes esquemas para implementar o cluster de failover do Kaspersky Security Center Linux:

- Cluster de failover da Kaspersky Security Center Linux implementado em um único data center:
  - Um esquema que usa um adaptador de rede secundário e um DBMS instalado em um dispositivo dedicado.
  - Um esquema que usa um balanceador de carga de terceiros e um DBMS instalado em um dispositivo dedicado.
- Cluster de failover da Kaspersky Security Center Linux distribuído geograficamente implementado em vários data centers.

Cluster de failover do Kaspersky Security Center Linux

Um esquema que usa um adaptador de rede secundário e um DBMS instalado em um dispositivo dedicado



Um esquema que usa um adaptador de rede secundário e um DBMS instalado em um dispositivo dedicado.

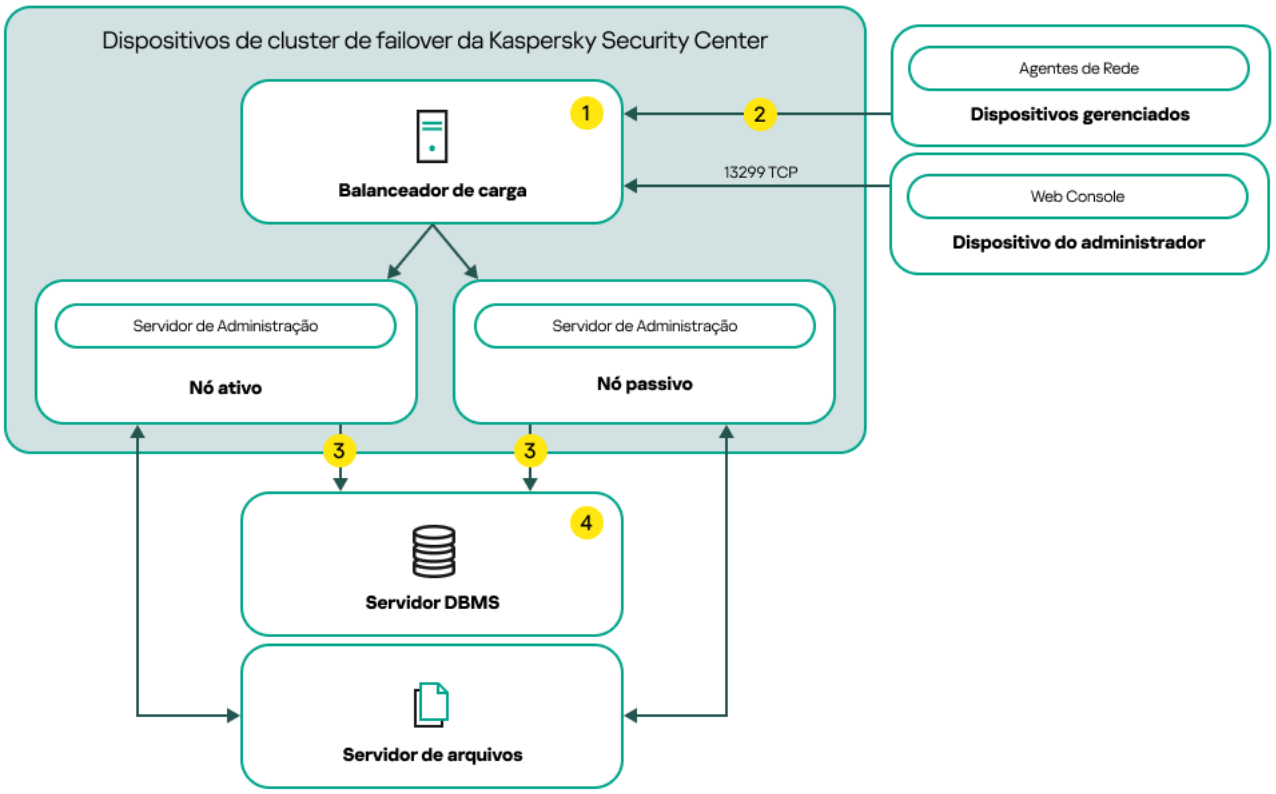
Legenda do esquema:

1 O Servidor de Administração envia dados para o banco de dados. Abra as portas necessárias no dispositivo no qual o banco de dados está localizado, por exemplo, a porta 3306 para o MySQL Server ou a porta 5432 para PostgreSQL ou Postgres Pro. Consulte a documentação do DBMS para obter informações relevantes.

2 Abra as seguintes portas nos dispositivos com o Servidor de Administração para conectar aos dispositivos gerenciados: TCP 13000, UDP 13000 e TCP 17000.

3 Um dispositivo com Sistema de Gerenciamento de Banco de Dados (DBMS). Se você usa o MariaDB Galera Cluster como um DBMS, não é necessário um dispositivo dedicado para essa finalidade. Instale o MariaDB Galera Cluster em cada um dos nós.

Um esquema que usa um balanceador de carga de terceiros e um DBMS instalado em um dispositivo dedicado



Um esquema que usa um balanceador de carga de terceiros e um DBMS instalado em um dispositivo dedicado.

Legenda do esquema:

1 No dispositivo do balanceador de carga, abra todas as portas do Servidor de Administração: TCP 13000, UDP 13000, TCP 13299 e TCP 17000.

> Caso deseje usar o utilitário klakaut para automação, você também deve abrir a porta TCP 13291.

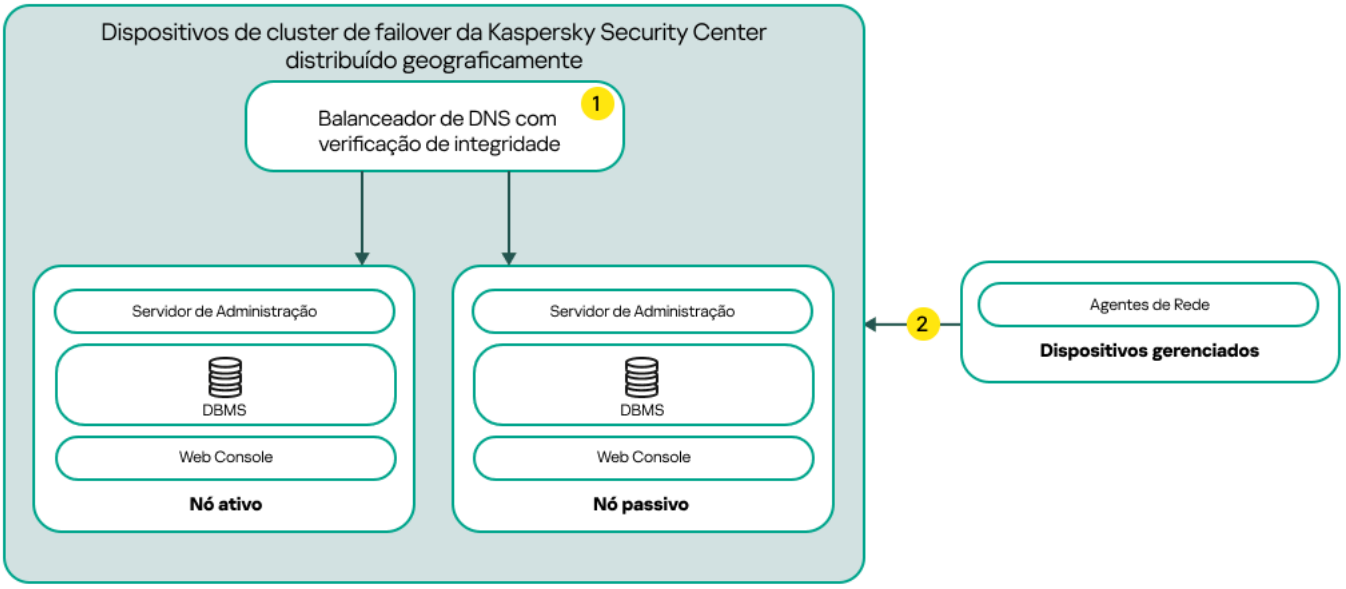
2 Abra as seguintes portas nos dispositivos com o Servidor de Administração para conectar aos dispositivos gerenciados: TCP 13000, UDP 13000 e TCP 17000.

3 O Servidor de Administração envia dados para o banco de dados. Abra as portas necessárias no dispositivo no qual o banco de dados está localizado, por exemplo, a porta 3306 para o MySQL Server ou a porta 5432 para PostgreSQL ou Postgres Pro. Consulte a documentação do DBMS para obter informações relevantes.

4 Um dispositivo com Sistema de Gerenciamento de Banco de Dados (DBMS). Se você usa o MariaDB Galera Cluster como um DBMS, não é necessário um dispositivo dedicado para essa finalidade. Instale o MariaDB Galera Cluster em cada um dos nós.

Cluster de failover da Kaspersky Security Center Linux distribuído geograficamente

Esse esquema de implementação permite fornecer alta disponibilidade a todos os componentes. Nesse esquema, o Servidor de Administração, o DBMS e o Kaspersky Security Center Web Console são instalados em ambos os nós de cluster.



Esquema de implementação do cluster de failover da Kaspersky Security Center Linux distribuído geograficamente

1 Balanceador de DNS com verificação de integridade que deve ser implementado no seu lado antes da instalação do cluster de failover da Kaspersky Security Center Linux distribuído geograficamente.

O balanceador de DNS verifica periodicamente o status dos nós de cluster. Ao acessar o cluster por seu nome de domínio, o balanceador de DNS sempre retorna o endereço IP do nó ativo.

2 Abra as seguintes portas nos dispositivos com o Servidor de Administração para conectar aos dispositivos gerenciados: TCP 13000, UDP 13000 e TCP 17000.

Cluster de failover do Kaspersky Security Center Linux

Esta seção contém informações gerais sobre o cluster de failover da Kaspersky Security Center Linux implementado em um único data center, bem como instruções para preparar e implementar o cluster de failover do Kaspersky Security Center Linux na sua rede.

Cenário: implantação de um cluster de failover do Kaspersky Security Center Linux

Um cluster de failover do Kaspersky Security Center Linux garante a alta disponibilidade do Kaspersky Security Center Linux e minimiza o tempo de inatividade do Servidor de Administração em caso de falha. O cluster de failover é baseado em duas instâncias idênticas do Kaspersky Security Center Linux, instaladas em dois computadores. Uma das instâncias funciona como o nó ativo e a outra, como o nó passivo. O nó ativo gerencia a proteção dos dispositivos clientes, enquanto o passivo está preparado para assumir todas as funções do nó ativo caso o nó ativo falhe. Quando ocorre uma falha, o nó passivo torna-se ativo e o nó ativo torna-se passivo.

A implementação dos aplicativos da Kaspersky é feita em fases:

Recomenda-se seguir a sequência de etapas descritas neste cenário.

1. **Verificando os requisitos de hardware**

   Certifique-se de ter hardware que atenda aos requisitos para o cluster de failover.

2. **Escolhendo o esquema de implementação**

   Escolha o esquema de implementação. Isso afeta os próximos estágios da implementação.

3. **Preparação de contas de usuário para os serviços do Kaspersky Security Center Linux**

   Execute as seguintes etapas no nó ativo, no nó passivo e no servidor de arquivos:

   1. Crie um grupo `kladmins`. Execute os seguintes comandos:

      ```
      sudo groupadd kladmins
      ```

      ```
      sudo groupmod -g <novo_GID> kladmins
      ```

      Certifique-se de que o grupo tenha o mesmo GID nos três dispositivos. Execute o seguinte comando:

      ```
      getent group kladmins
      ```

      Se o GID não corresponder, você poderá utilizar o seguinte comando para especificá-lo:

      ```
      sudo groupmod -g <novo_GID> kladmins
      ```

   2. Crie uma conta de usuário `ksc`. Atribua contas de usuário ao grupo `kladmins`. Execute os seguintes comandos:

      ```
      sudo adduser ksc
      ```

      ```
      sudo usermod -u <novo_GID> ksc
      ```

      ```
      sudo gpasswd -a ksc kladmins
      ```

      ```
      sudo usermod -g kladmins ksc
      ```

      Certifique-se de que a conta de usuário tenha o mesmo UID nos três dispositivos. Execute o seguinte comando:

      ```
      getent passwd ksc
      ```

      Se o UID não corresponder, você poderá utilizar o seguinte comando para especificá-lo:

      ```
      sudo usermod -u <novo_GID> ksc
      ```

   3. Crie uma conta de usuário `rightless`. Atribua contas de usuário ao grupo `kladmins`. Execute os seguintes comandos:

      ```
      sudo adduser rightless
      ```

      ```
      sudo usermod -u <novo_GID> rightless
      ```

      ```
      sudo gpasswd -a rightless kladmins
      ```

      ```
      sudo usermod -g kladmins rightless
      ```

      Certifique-se de que a conta de usuário tenha o mesmo UID nos três dispositivos. Execute o seguinte comando:

      ```
      getent passwd rightless
      ```

      Se o UID não corresponder, você poderá utilizar o seguinte comando para especificá-lo:

`sudo usermod -u <novo_GID> rightless`

4. Crie uma conta de usuário `ksciam`. Atribua contas de usuário ao grupo `kladmins`. Execute os seguintes comandos:

   `sudo adduser ksciam`

   `sudo usermod -u <novo_GID> ksciam`

   `sudo gpasswd -a ksciam kladmins`

   `sudo usermod -g kladmins ksciam`

   Certifique-se de que a conta de usuário tenha o mesmo UID nos três dispositivos. Execute o seguinte comando:

   `getent passwd kliam`

   Se o UID não corresponder, você poderá utilizar o seguinte comando para especificá-lo:

   `sudo usermod -u <novo_GID> ksciam`

5. Se necessário, aumente o limite padrão de arquivos que podem ser abertos (descritores de arquivo) para as contas utilizadas para a função dos serviços do Kaspersky Security Center Linux. Para isso, abra o arquivo /etc/security/limits.conf e especifique os limites flexíveis e rígidos dos descritores de arquivo da seguinte forma:

   `ksc soft nofile <número_máximo_de_arquivos_abertos>`

   `ksc hard nofile <número_máximo_de_arquivos_abertos>`

   Por padrão, os limites dos descritores de arquivo são especificados durante a instalação. O limite flexível de arquivos é de 32.768 arquivos, e o limite rígido de arquivos é de 131.072 arquivos.

4 Preparação do servidor de arquivos

Prepare o servidor de arquivos para funcionar como um componente do cluster de failover do Kaspersky Security Center Linux. Verifique e confirme se o servidor de arquivos atende aos requisitos de hardware e software, crie duas pastas compartilhadas para os dados do Kaspersky Security Center Linux e configure as permissões para acessar as pastas compartilhadas.

Instruções: Preparando um servidor de arquivos para o cluster de failover do Kaspersky Security Center Linux

5 Instalação do DBMS

Instale o DBMS para o Kaspersky Security Center Linux. Você pode escolher qualquer DBMS compatível. Para obter informações sobre como instalar o DBMS selecionado, consulte a sua documentação.

Caso a distribuição do sistema operacional baseado em Linux não contenha um DBMS compatível, será possível instalar o DBMS por meio de um repositório de pacotes de terceiros.

Depois de instalar o DBMS, siga as instruções correspondentes:

- Configurar o servidor PostgreSQL ou Postgres Pro para uso com o Kaspersky Security Center Linux
- Configuração do servidor MariaDB x64 para uso com o Kaspersky Security Center Linux

Crie manualmente um banco de dados para o IAM. O Servidor de Administração não remove automaticamente o banco de dados do IAM quando o servidor é desinstalado ou movido para outro dispositivo. Você deve remover o banco de dados manualmente.

- Para PostgreSQL, execute o seguinte comando:

  `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"`

- Para MariaDB, execute o seguinte comando:

  `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

No dispositivo com o DBMS instalado, configure a conexão com os dispositivos que funcionarão como nós ativos e passivos.

6. **Preparação de nós ativos e passivos**

   Prepare dois dispositivos com hardware e software idênticos para funcionarem como nós ativos e passivos.

   Instruções: Preparando nós para o cluster de failover do Kaspersky Security Center Linux

7. **Instalação do Kaspersky Security Center Linux**

   Instale o Kaspersky Security Center Linux no modo de cluster de failover em ambos os nós.

   Primeiro, é necessário instalar o Kaspersky Security Center Linux no dispositivo que será o nó ativo e depois instalá-lo no nó passivo.

   Instruções: Instalando o Kaspersky Security Center Linux nos nós de cluster de failover da Kaspersky Security Center Linux.

8. **Instalar o Kaspersky Security Center Web Console**

   Instalar o Kaspersky Security Center Web Console em um dispositivo separado que não seja um nó de cluster.

   Especifique o cluster de failover como o endereço do Servidor de Administração no arquivo de resposta.

   O certificado do Servidor de Administração está localizado no seguinte caminho: /mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer

   Copie o arquivo do certificado para o dispositivo no qual o Kaspersky Security Center Web Console está sendo instalado. Especifique o caminho local para o certificado no arquivo de resposta.

9. **Como testar o cluster de failover**

   Verifique se você configurou o cluster de failover corretamente e se ele funciona corretamente. Por exemplo, é possível executar o seguinte comando para iniciar a troca para o nó passivo:

   `/opt/kaspersky/ksc64/sbin/klfoc -failover --stp klfoc`

   Utilize o seguinte comando para verificar se o serviço de gerenciamento de cluster de failover está `Active: active (running)` em ambos os nós:

   `systemctl status klfocsvc_klfoc`

   Utilize os seguintes comandos para verificar se outros serviços de cluster de failover estão `Active: active (running)` no nó ativo. No nó passivo, esses serviços de cluster de failover devem estar `Active: inactive (dead)` ou `Active: failed (Result: signal)`.

   - `systemctl status klnagent_klfoc`
   - `systemctl status kladminserver_klfoc`
   - `systemctl status klactprx_klfoc`
   - `systemctl status klwebsrv_klfoc`

O cluster de failover do Kaspersky Security Center Linux é implementado.

Cluster de failover do Kaspersky Security Center Linux. Requisitos de hardware e software

Recomendamos que, após instalar o Servidor de Administração em um dispositivo, você instale o Kaspersky Endpoint Security for Linux nesse dispositivo.
Para a instalação simultânea, é necessário ter no mínimo 300 IOPS, além de acrescentar aos requisitos do Servidor de Administração 1,5 GB de RAM e 15% à CPU.
Para obter os requisitos de hardware do Kaspersky Endpoint Security, consulte a Ajuda do Kaspersky Endpoint Security for Linux.

Para obter informações sobre as configurações de segurança necessárias para trabalhar com o Kaspersky Security Center Linux, consulte a Ajuda do Kaspersky Endpoint Security for Linux.

Para implementar um cluster de failover do Kaspersky Security Center Linux, é necessário ter o seguinte hardware:

- Dois dispositivos com hardware e software idênticos. Esses dispositivos atuarão como nós ativos e passivos.

  Configuração mínima para nós ativos e passivos

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	6 GB
Espaço em disco	10 GB, 150 IOPS ou superior
Controlador de interface de rede	1 Gbps

  Ocorre falha na implementação do cluster de failover se você tiver os pacotes arping e iputils-arping ou somente o pacote arping instalado. Antes de implementar um cluster de failover, certifique-se de ter apenas o pacote iputils-arping instalado em ambos os nós.

  Você pode consultar os requisitos de dimensionamento dos nós ativos e passivos, de acordo com o número de dispositivos gerenciados, no artigo Requisitos de hardware para o SGBD e o Servidor de Administração.

- Um dispositivo no qual você deseja instalar o Kaspersky Security Center Linux Web Console.

  Configuração do dispositivo para até 10 administradores de sistema

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	4 GB
Espaço em disco	40 GB, 150 IOPS ou superior

  Configuração do dispositivo para mais de 10 administradores de sistema

Hardware	Valor
CPU	4 cores, 2.500 MHz
RAM	8 GB
Espaço em disco	40 GB, 150 IOPS ou superior

- Um servidor de arquivos compatível com o protocolo CIFS/SMB, versão 2.0 ou posterior. Você deve fornecer um dispositivo dedicado que funcionará como um servidor de arquivos.

  Configuração de um servidor de arquivo

Hardware	Valor
CPU	4 cores, 2.500 MHz
RAM	32 GB
Espaço em disco	500 GB, 500 IOPS ou superior
Controlador de interface de rede	10 Gbps

  Certifique-se de ter alta largura de banda de rede entre o servidor de arquivos e os nós ativos e passivos.

- Um dispositivo com Sistema de Gerenciamento de Banco de Dados (DBMS). Se você usa o MariaDB Galera Cluster como um DBMS, não é necessário um dispositivo dedicado para essa finalidade.

- Um dispositivo balanceador de carga. Usado em um esquema de implementação de cluster de failover do Kaspersky Security Center Linux que utiliza um balanceador de carga de terceiros e o DBMS instalado em um dispositivo dedicado.

  Configuração do dispositivo para um balanceador de carga Nginx

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	4 GB

Preparação de um servidor de arquivos para um cluster de failover do Kaspersky Security Center Linux

Um servidor de arquivos funciona como um componente necessário de um cluster de failover do Kaspersky Security Center Linux.

Para preparar um servidor de arquivos:

1. Certifique-se de que o servidor de arquivos atenda aos requisitos de hardware e software.

2. Instalar e configurar um servidor NFS:

   - O acesso ao servidor de arquivos deve ser ativado para os dois nós nas configurações do servidor NFS.
   - O protocolo NFS deve ter a versão 4.0 ou 4.1.
   - Requisitos mínimos para o kernel do Linux:
     - 3.19.0-25, if you use NFS 4.0
     - 4.4.0-176, caso use NFS 4.1

   Dependendo de sua distribuição Linux, instale o pacote nfs-utils ou o pacote nfs-kernel-server ao executar o comando correspondente:

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

3. No servidor de arquivos, crie duas pastas e compartilhe-as usando o NFS. Uma delas é usada para manter informações sobre o estado do cluster de failover. A outra é usada para armazenar os dados e configurações do Kaspersky Security Center Linux. O usuário especificará caminhos para as pastas compartilhadas ao configurar a instalação do Kaspersky Security Center Linux.

   Assegure-se de que as seguintes pastas não existam:

   - `/mnt/KlFocStateShare`
   - `/mnt/KlFocDataShare_klfoc`

   Se alguma dessas pastas existir, exclua-a recursivamente.

   Execute os seguintes comandos:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 770 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo systemctl start nfs-server
   ```

   Ative a inicialização automática executando o seguinte comando:

   ```
   sudo systemctl enable rpcbind
   ```

   É possível especificar pastas personalizadas, mas, por conveniência, recomendamos utilizar os nomes de pasta sugeridos ao usar a Ajuda.

4. Reinicie o servidor de arquivos.

O servidor de arquivos está preparado. Para implantar o cluster de failover do Kaspersky Security Center Linux, siga as instruções adicionais neste cenário.

Preparação de nós para um cluster de failover do Kaspersky Security Center Linux

Antes de continuar, assegure-se de ter concluído as etapas anteriores no Cenário: Implementação do cluster de failover da Kaspersky.

Prepare dois dispositivos para funcionarem como nós ativos e passivos do cluster de failover do Kaspersky Security Center Linux.

Configuração de pastas compartilhadas

Para configurar pastas comuns:

1. Dependendo de sua distribuição Linux, instale o pacote nfs-utils ou o pacote nfs-kernel-server em cada nó ao executar o comando correspondente:

   ```
   yum install nfs-utils
   ```

`apt install nfs-kernel-server`

2. Crie pontos de montagem executando os seguintes comandos:

   `mkdir -p /mnt/KlFocStateShare`

   `mkdir -p /mnt/KlFocDataShare_klfoc`

3. Corresponda os pontos de montagem e as pastas compartilhadas:

   `sudo sh -c "echo <servidor de arquivos>:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"`

   `sudo sh -c "echo <servidor de arquivos>:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"`

   Em que `{servidor de arquivos}` é o FQDN do servidor de arquivos com pastas compartilhadas.

4. Monte as pastas compartilhadas executando os seguintes comandos:

   `mount /mnt/KlFocStateShare`

   `mount /mnt/KlFocDataShare_klfoc`

5. Certifique-se de que as permissões para acessar as pastas compartilhadas pertençam a ksc:kladmins.

   Execute o seguinte comando:

   `ls -la /mnt/`

Configuração dos adaptadores de rede

Um adaptador de rede secundário pode ser físico ou virtual. Se você escolher um esquema de implementação com um adaptador de rede secundário, execute o procedimento correspondente em ambos os nós:

- Utilize um adaptador de rede secundário virtual baseado em um adaptador de rede físico (a tecnologia MACVLAN):

  1. Install the iputils-arping package. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:

     - `yum install iputils`

     ou

     - `apt install iputils-arping`

  2. Para garantir que o NetworkManager seja usado para gerenciar o adaptador de rede físico, execute o seguinte comando:

     `nmcli device status`

     Se a saída do comando mostrar o adaptador de rede físico como não sendo gerenciado, configure o NetworkManager para gerenciar o adaptador de rede físico. As etapas de configuração exatas dependem da sua distribuição Linux.

  3. Para identificar as interfaces, execute o seguinte comando:

     `ip a`

4. Para criar um perfil de configuração, execute o seguinte comando:

   `nmcli connection add type macvlan dev <interface física> mode bridge ifname <interface virtual> ipv4.addresses <máscara do endereço> ipv4.method manual autoconnect no`

- Utilize um adaptador de rede secundário físico ou crie um dispositivo TAP virtual usando um hipervisor. Nesse cenário, desabilite o software NetworkManager.

  1. Conecte o adaptador de rede secundário a um nó.

  2. Install the iputils-arping package. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:

     - `yum install iputils`

     ou

     - `apt install iputils-arping`

  3. Para excluir a conexão do NetworkManager para a interface de destino, execute o seguinte comando:

     `nmcli con del <nome da conexão>`

     Para verificar as conexões com a interface de destino, execute o seguinte comando:

     `nmcli con show`

  4. Edite o arquivo NetworkManager.conf. Localize a seção de arquivo-chave e atribua a interface de destino ao parâmetro `unmanaged-devices`:

     `[keyfile]`

     `unmanaged-devices=interface-name:<nome da interface>`

  5. Reinicie o NetworkManager:

     `systemctl reload NetworkManager`

     Para garantir que a interface de destino não seja mais gerenciada, execute o seguinte comando:

     `nmcli dev status`

Configuração do balanceador de carga

Se você escolheu um esquema de implementação com um balanceador de carga, siga as instruções abaixo para configurá-lo.

Para configurar o balanceador de carga:

1. Prepare um dispositivo dedicado baseado em Linux com nginx ou outro balanceador de carga instalado.

2. Configure o balanceamento de carga. Defina o nó ativo como o servidor principal e o nó passivo como um servidor de backup.

3. No servidor nginx, abra todas as portas do Servidor de Administração de acordo com o seguinte artigo: Portas utilizadas pelo Kaspersky Security Center Linux.

Para implantar o cluster de failover do Kaspersky Security Center Linux, siga as instruções adicionais do cenário.

A disponibilidade dos nós de cluster de failover deve ser determinada pela disponibilidade das portas de conexão principais ao Servidor de Administração. O nó passivo não aceita nenhuma conexão externa até que ocorra uma troca.

Instalação do Kaspersky Security Center Linux nos nós do cluster de failover do Kaspersky Security Center Linux

Antes de continuar, assegure-se de ter concluído as etapas anteriores no Cenário: Implementação do cluster de failover da Kaspersky.

Este procedimento descreve como instalar o Kaspersky Security Center Linux nos nós de cluster de failover da Kaspersky Security Center Linux. A Kaspersky Security Center Linux é instalada separadamente em ambos os nós de cluster de failover da Kaspersky Security Center Linux. Primeiro, você instala o aplicativo no nó ativo e, em seguida, no passivo. Ao instalar, você escolhe qual nó ficará ativo e qual será passivo.

Dependendo da distribuição Linux instalada no seu dispositivo, você deve usar um dos seguintes arquivos de instalação:

- ksc64_[número_da_versão]_amd64.deb
- ksc64-[número_da_versão].x86_64.rpm

Para receber o arquivo de instalação, baixe-o do site da Kaspersky.

Se você usar o RED OS versão 7.3.4 ou mais recente ou o MSVSPHERE versão 9.2 ou mais recente, será necessário instalar o pacote libxcrypt-compat em ambos os nós.

Instalação no nó ativo

Para instalar o Kaspersky Security Center Linux no nó ativo:

1. Verifique e confirme se o dispositivo no qual deseja instalar o Kaspersky Security Center Linux está executando em uma das distribuições Linux compatíveis.
2. Caso um adaptador de rede secundário seja usado, insira o nome dele quando for solicitado. Você pode inserir o seguinte comando para exibir todas as interfaces de rede:

   ```
   ip addr
   ```

3. Execute a instalação do Kaspersky Security Center Linux. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:
   - `sudo apt-get install /<path>/ksc64_<número_da_versão>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<número_da_versão>.x86_64.rpm`
4. Execute a configuração do Kaspersky Security Center Linux:

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

5. Leia o Contrato de Licença do Usuário Final (EULA) e a Política de Privacidade. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite os seguintes valores:

   a. Digite `y` (sim), se você entende e aceita integralmente os termos do EULA. Digite `n` (não) se você não aceita os termos do EULA. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos do EULA.

   b. Digite `y` se você entende e aceita os termos da Política de Privacidade e se concorda que seus dados serão tratados e transmitidos (inclusive para países terceiros), conforme descrito na Política de Privacidade. Digite `n` (não) se você não aceita os termos da Política de Privacidade. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos da Política de Privacidade.

6. Selecione o **Nó de cluster primário** como um modo de instalação do Servidor de Administração.

7. Quando for solicitado, especifique as seguintes configurações:

   a. Insira o caminho local para o ponto de montagem do compartilhamento de estado:
   `/mnt/KlFocStateShare`

   b. Insira o caminho local para o ponto de montagem do compartilhamento de dados:
   `/mnt/KlFocDataShare_klfoc`

   c. Escolha o modo de conectividade do cluster de failover: por meio de um adaptador de rede secundário ou de um balanceador de carga externo.

   d. Caso um adaptador de rede secundário seja usado, insira o nome dele.

   e. Insira o FQDN ou o nome DNS do adaptador de rede secundário ou o FQDN ou o nome DNS do balanceador de carga externo.

   f. Digite o número da porta SSL do Servidor de Administração. O número da porta padrão é 13000.

   g. Avalie o número aproximado de dispositivos que você deseja gerenciar:

      - Se você tem de 1 a 100 dispositivos gerenciados, digite 1.
      - Se você tem de 101 a 1000 dispositivos gerenciados, digite 2.
      - Se você tem mais de 1000 dispositivos gerenciados, digite 3.

      Essa configuração é utilizada para o atraso aleatório automático do início de uma tarefa para aprimorar uma carga de rede. A lista abaixo mostra o intervalo usado para calcular o atraso:

      - 1 a 100 dispositivos gerenciados, valor 1. O atraso não é utilizado.
      - 101 a 1000 dispositivos gerenciados, valor 2. O atraso é de 5 minutos.
      - Mais de 1000 dispositivos gerenciados, valor 3. O atraso é de 10 minutos.

   h. Digite o nome do grupo de segurança para serviços. Por padrão, é usado o grupo 'kladmins'.

   i. Digite o nome da conta e inicie o serviço do Servidor de Administração. A conta deve ser membro do grupo de segurança digitado. Por padrão, é usada a conta ksc.

   j. Digite o nome da conta para iniciar outros serviços. A conta deve ser membro do grupo de segurança digitado. Por padrão, é usada a conta ksc.

k. Selecione o DBMS que foi instalado para funcionar com o Kaspersky Security Center Linux:

- Caso tenha instalado o MySQL ou o MariaDB, digite 1.
- Caso tenha instalado o PostgreSQL ou o Postgres Pro, digite 2.

l. Digite o nome DNS ou endereço IP do dispositivo no qual o banco de dados está instalado.

m. Digite o número da porta do banco de dados. Esta porta é usada para comunicação com o Servidor de Administração. Por padrão, as seguintes portas são usadas:

- Porta 3306 para MySQL ou MariaDB.
- Porta 5432 para PostgreSQL ou Postgres Pro.

n. Digite o nome do banco de dados.

o. Insira o login da conta de administrador do banco de dados usado para acessar o banco de dados.

p. Insira a senha da conta de administrador do banco de dados usada para acessar o banco de dados.

q. Insira o FQDN ou o nome DNS do servidor IAM.

Insira o valor especificado na etapa 7e.

r. Insira o nome da conta para iniciar o serviço IAM. A conta deve ser membro do grupo de segurança digitado. Por padrão, é usada a conta ksciam.

s. Selecione o DBMS que foi instalado para funcionar com o serviço IAM:

- Caso tenha instalado o MySQL ou o MariaDB, digite 1.
- Caso tenha instalado o PostgreSQL ou o Postgres Pro, digite 2.

t. Insira o endereço do IAM DBMS a ser usado pelo serviço IAM.

u. Insira o número da porta do IAM DBMS. Esta porta é usada para a comunicação com o serviço IAM. Por padrão, as seguintes portas são usadas:

- Porta 3306 para MySQL ou MariaDB.
- Porta 5432 para PostgreSQL ou Postgres Pro.

v. Insira o nome do banco de dados do IAM a ser usado pelo serviço do IAM. O nome do banco de dados usado pelo serviço do IAM deve ser diferente do banco de dados usado pelo Servidor de Administração.

w. Insira o login da conta do banco de dados usada para acessar o banco de dados do IAM.

x. Insira a senha da conta do banco de dados usada para acessar o banco de dados do IAM.

8. Aguarde que os serviços sejam adicionados e inicializados automaticamente:

- klfocsvc_klfoc
- kladminserver_klfoc

- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_klfoc

9. Crie uma conta que agirá como um administrador do Servidor de Administração. Digite o nome de usuário e senha. A senha de usuário não pode ter menos de 8 nem mais de 256 caracteres.

   Se você ignorar esta etapa, poderá criar a conta mais tarde executando o seguinte comando:

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <senha>`

O usuário é adicionado e o Kaspersky Security Center Linux é instalado no nó primário.

Instalação no nó secundário (passivo)

Para instalar o Kaspersky Security Center Linux no nó secundário:

1. Verifique e confirme se o dispositivo no qual deseja instalar o Kaspersky Security Center Linux está executando em uma das distribuições Linux compatíveis.

2. Execute a instalação do Kaspersky Security Center Linux. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:

   - `sudo apt-get install /<path>/ksc64_<número_da_versão>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<número_da_versão>.x86_64.rpm`

3. Execute a configuração do Kaspersky Security Center Linux:

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

4. Leia o Contrato de Licença do Usuário Final (EULA) e a Política de Privacidade. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite os seguintes valores:

   a. Digite `y` (sim), se você entende e aceita integralmente os termos do EULA. Digite `n` (não) se você não aceita os termos do EULA. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos do EULA.

   b. Digite `y` se você entende e aceita os termos da Política de Privacidade e se concorda que seus dados serão tratados e transmitidos (inclusive para países terceiros), conforme descrito na Política de Privacidade. Digite `n` (não) se você não aceita os termos da Política de Privacidade. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos da Política de Privacidade.

5. Selecione o **Nó de cluster secundário** como um modo de instalação do Servidor de Administração.

6. Quando for solicitado, insira o caminho local para o ponto de montagem do compartilhamento de estado: `/mnt/KlFocStateShare`

O Kaspersky Security Center Linux é instalado no nó secundário.

Verificação de serviço

Use o seguinte comando para verificar se o serviço de gerenciamento de cluster de failover está com o status `Active: active (running)`:

```
systemctl status klfocsvc_klfoc
```

Use os seguintes comandos para verificar se outros serviços do cluster de failover estão com o status `Active: inactive (dead)`:

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

Agora, é possível testar o cluster de failover do Kaspersky Security Center Linux para verificar se ele foi configurado e funciona corretamente.

Iniciando e interrompendo nós de cluster manualmente

Pode ser necessário interromper todo o cluster de failover da Kaspersky Security Center Linux ou desvincular temporariamente um dos nós de cluster para manutenção. Nesse caso, siga as instruções nesta seção. Não tente iniciar ou interromper os serviços ou processos relacionados ao cluster de failover usando qualquer outro meio. Isso pode causar a perda de dados.

Iniciando e interrompendo todo o cluster de failover para manutenção

Para iniciar ou interromper todo o cluster de failover:

No nó ativo, execute um dos seguintes comandos:

- Para interromper o cluster, execute: `/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- Para iniciar o cluster, execute: `/opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc`

O cluster de failover é iniciado ou interrompido, de acordo com o comando executado.

Mantendo um dos nós

Para manter um dos nós:

1. No nó ativo, interrompa o cluster de failover usando o comando `klfoc -stopcluster --stp klfoc`.
2. No nó que deseja manter, acesse /opt/kaspersky/ksc64/sbin.
3. Abra a linha de comando e desvincule o nó do cluster executando o comando `detach_node.sh`.

4. No nó ativo, inicie o cluster de failover usando o comando `klfoc -startcluster --stp klfoc`.
5. Execute as atividades de manutenção.
6. No nó ativo, interrompa o cluster de failover usando o comando `klfoc -stopcluster --stp klfoc`.
7. No nó que foi mantido, acesse /opt/kaspersky/ksc64/sbin.
8. Abra a linha de comando e vincule o nó ao cluster executando o comando `attach_node.sh`.
9. No nó ativo, inicie o cluster de failover usando o comando `klfoc -startcluster --stp klfoc`.
10. Para garantir que o nó atual esteja ativo, execute os seguintes comandos para verificar se os serviços são executados:

    `systemctl status klnagent_klfoc.service`

    `systemctl status kladminserver_klfoc.service`

    `systemctl status klactprx_klfoc.service`

    `systemctl status klwebsrv_klfoc.service`

    `systemctl status kliam_klfoc.service`

    Esses serviços são executados no nó ativo e não no nó passivo.

O nó é mantido e conectado ao cluster de failover.

Reinstalar um nó de cluster de failover

Para reinstalar um nó de cluster de failover:

1. Crie um backup do Servidor de Administração.
2. Alterne o nó ativo para o modo de manutenção.
3. Se for necessário manter o sistema operacional atual, execute as seguintes etapas.

   Se você quiser substituir o dispositivo ou o sistema operacional, ignore esta etapa.

   a. Para interromper o cluster de failover, execute o seguinte comando:
   `klfoc -stopcluster --stp klfoc`

   b. Para forçar a interrupção dos serviços de cluster de failover, execute os seguintes comandos:
   `sudo systemctl stop klfocsvc_klfoc`
   `systemctl status kl*klfoc*`

   c. Para desmontar diretórios de cluster de failover, execute os seguintes comandos:
   `sudo umount /mnt/KlFocDataShare_klfoc`
   `sudo umount /mnt/KlFocStateShare`

   d. Para desinstalar o Kaspersky Security Center Linux, execute um dos seguintes comandos, dependendo da sua distribuição Linux:

   - `sudo dpkg --remove ksc64`

ou

- `sudo yum remove ksc64`

e. Execute todas as etapas das seguintes instruções para o nó passivo:

1. Preparação de nós para um cluster de failover do Kaspersky Security Center Linux.
2. Instalação do Kaspersky Security Center Linux nos nós de cluster de failover da Kaspersky Security Center Linux.

4. Saia do modo de manutenção. Continue da etapa 6 (interromper o cluster de failover) das instruções Iniciar e interromper nós de cluster manualmente.

Instalação do Kaspersky Security Center Web Console conectado com o Servidor de Administração instalado nos nós do cluster de failover do Kaspersky Security Center Linux

Esta seção descreve como instalar o Kaspersky Security Center Web Console Server (doravante também chamado de Kaspersky Security Center Web Console), que se conecta com o Servidor de Administração instalado em nós do cluster de failover do Kaspersky Security Center Linux. Antes de instalar o Kaspersky Security Center Web Console, instale um DBMS e um Servidor de Administração do Kaspersky Security Center Linux em nós de cluster de failover da Kaspersky Security Center Linux.

> O Kaspersky Security Center Web Console não é compatível com a instalação em nós de cluster. Recomendamos instalar o Kaspersky Security Center Web Console em um servidor separado.

Para instalar o Kaspersky Security Center Web Console que se conecta com o Servidor de Administração instalado nos nós de cluster de failover da Kaspersky Security Center Linux:

1. Execute a etapa 1 e 2 da instalação do Kaspersky Security Center Web Console.
2. Na etapa 3, no arquivo de resposta, especifique o parâmetro de instalação `trusted` para permitir que o Kaspersky Security Center Web Console se conecte ao cluster de failover do Kaspersky Security Center Linux.

   Componentes do **parâmetro de instalação** `trusted`

   Se você se conectar ao Cluster de failover da Kaspersky Security Center Linux usando autenticação do domínio com SSO, especifique o parâmetro de instalação confiável da seguinte forma: Se você conectar o Kaspersky Security Center Web Console ao Servidor de Administração versão 16 ou posterior, será usada a autenticação do domínio com conexão única (SSO) fornecida pelo Identity and Access Manager (IAM). Nesse caso, especifique o parâmetro de instalação `trusted` da seguinte forma:

```
"trusted":  {
  "<Nome do Servidor de Administração>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<pasta de dados compartilhada>/iam/main_certificate.pem",
    "iamPATPath": "<pasta de dados compartilhada>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<pasta de dados compartilhada>/1093/cert/klserver.cer"
  }
}
```

onde:

- O < `nome do Servidor de Administração` > é o nome do cluster de failover do Kaspersky Security Center Linux a ser exibido na janela de login do Kaspersky Security Center Web Console.

- `iamHost` é o endereço do dispositivo onde o Servidor de Administração e o IAM estão instalados. Se você criou um adaptador de rede secundário ao preparar os nós de cluster, use o FQDN ou o nome do host do adaptador como o endereço do Cluster de failover da Kaspersky Security Center Linux. Caso contrário, especifique o FQDN ou o nome do host do balanceador de carga de terceiros em uso.

  O valor `iamHost` deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado:

  ```
  grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
  ```

- `iamOAuthPort` é a porta utilizada para trocar tokens de autenticação por meio do protocolo de autenticação OpenID Connect (o valor padrão é 4444). Esta porta é utilizada tanto para a comunicação entre o Kaspersky Security Center Web Console Server e o Servidor de Administração, quanto entre o navegador (utilizado com o Kaspersky Security Center Web Console) e o Servidor de Administração.

- `iamProxyPort` é a porta usada para conectar o Kaspersky Security Center Web Console Server ao Servidor de Administração (o valor padrão é 9050).

- `iamCertPath` é o caminho para o certificado IAM. O certificado IAM é criado automaticamente na primeira vez que você executa o Servidor de Administração. O certificado está localizado no dispositivo no qual o Servidor de Administração está instalado. O caminho padrão para o certificado é: < `pasta de dados compartilhada` >`/iam/main_certificate.pem`. O certificado está localizado no armazenamento de dados compartilhado do cluster de failover do Kaspersky Security Center Linux. O certificado IAM autoassinado é rotacionado automaticamente.

- `iamPATPath` é o caminho para o token usado para o registro do Kaspersky Security Center Web Console como um cliente OAuth no IAM. Este arquivo é gerado automaticamente na primeira vez que você executa o Servidor de Administração. O token está localizado no dispositivo no qual o Servidor de Administração está instalado. O caminho padrão para o token é: <pasta de dados compartilhada>/iam/initial_token.txt. O token está localizado no armazenamento de dados compartilhado do cluster de failover do Kaspersky Security Center Linux. A validade do token é indefinida e não requer rotação.

- `kscPort` é a porta OpenAPI que o Kaspersky Security Center Web Console usa para se conectar ao Servidor de Administração (o valor padrão é 13299).

- `kscCertPath` é o certificado do Servidor de Administração localizado no armazenamento de dados compartilhado do cluster de failover do Kaspersky Security Center Linux. O caminho padrão para o arquivo de certificado é: < `pasta de dados compartilhada` >`\1093\cert\klserver.cer`.

  Copie o arquivo de certificado do Servidor de Administração (especificado por `kscCertPath`), o arquivo de certificado IAM (especificado por `iamCertPath`) e o arquivo de token (especificado por `iamPATPath`) do armazenamento de dados compartilhado para o dispositivo no qual o Kaspersky Security Center Web Console será instalado. Especifique o caminho local para o certificado do Servidor de Administração.

Se você conectar o Kaspersky Security Center Web Console ao Servidor de Administração versão 15.4 ou anterior, será usada a autenticação especificando o nome e a senha do usuário do domínio ou do usuário interno. Nesse caso, especifique o parâmetro de instalação confiável, conforme a seguir:

```
"trusted":  {
  "<Nome do Servidor de Administração>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<pasta de dados compartilhada>/1093/cert/klserver.cer"
  }
}
```

onde:

- O < `nome do Servidor de Administração` > é o nome do cluster de failover do Kaspersky Security Center Linux a ser exibido na janela de login do Kaspersky Security Center Web Console.
- `kscHost` é o endereço do Servidor de Administração (FQDN ou nome do host). Se você criou um adaptador de rede secundário ao preparar os nós de cluster, use o endereço desse adaptador como o endereço do cluster de failover da Kaspersky Security Center Linux. Caso contrário, especifique o endereço do balanceador de carga de terceiros em uso.
- `kscPort` é a porta OpenAPI utilizada pelo Kaspersky Security Center Web Console para se conectar ao Servidor de Administração (o valor padrão é 13299).
- `kscCertPath` é o certificado do Servidor de Administração localizado no armazenamento de dados compartilhado do cluster de failover do Kaspersky Security Center Linux. O caminho padrão para o arquivo de certificado é: < `pasta de dados compartilhada` >`\1093\cert\klserver.cer`. Copie o arquivo de certificado do armazenamento de dados compartilhado para o dispositivo onde o Kaspersky Security Center Web Console foi instalado. Especifique o caminho local para o certificado do Servidor de Administração.

3. Continue com o padrão de instalação do Kaspersky Security Center Web Console.

Quando a instalação estiver concluída, você poderá usar o navegador para abrir e fazer login no Kaspersky Security Center Web Console.

Cluster de failover da Kaspersky Security Center Linux distribuído geograficamente

Esta seção contém informações gerais sobre o cluster de failover da Kaspersky Security Center Linux distribuído geograficamente, bem como instruções para preparar e implementar o cluster de failover distribuído geograficamente na sua rede para as seguintes configurações:

- Nós de cluster que executam o Ubuntu com o DBMS do PostgreSQL
- Nós de cluster que executam o SberLinux com o DBMS do Platform V Pangolin

Cluster distribuído geograficamente que executa o Ubuntu com o DBMS do PostgreSQL

Seguindo este cenário, você pode preparar sua infraestrutura e implementar um cluster de failover da Kaspersky Security Center Linux distribuído geograficamente.

Pré-requisitos

- Implemente um balanceador de DNS altamente disponível com verificação de integridade.
- Os nós de cluster ativos e passivos devem ser dois dispositivos com configurações de hardware e software idênticas.
  - Requisitos de hardware:
    - CPU: 16 núcleos, 2500 MHz
    - RAM – 32 GB
    - Espaço em disco: 500 GB com 300 IOPS ou superior
    - Controlador de interface de rede: 1 Gbps
  - Requisitos de software:
    - Sistema operacional: Ubuntu Server 24.04 LTS (Noble Numbat) de 64 bits
    - DBMS: PostgreSQL 17 de 64 bits

Fases

O cluster de failover da Kaspersky Security Center Linux implementado em um único data center não pode ser atualizado para um cluster de failover distribuído geograficamente.

A implementação do cluster de failover da Kaspersky Security Center Linux distribuído geograficamente ocorre em etapas:

1. **Preparar um sistema de arquivos de nós de cluster de failover**

   Prepare o sistema de arquivos em ambos os nós de cluster. A preparação inclui a criação de volumes lógicos LVM e a configuração de diretórios como pontos de montagem.

2. **Configurar um sistema de arquivos de cluster replicado**

   Instale os utilitários DRBD e configure os recursos DRBD para a replicação de dados entre nós de cluster de failover. Depois disso, crie um sistema de arquivos replicado no nó do cluster ativo.

3. **Instalar e configurar o Corosync e o Pacemaker nos nós de cluster de failover**

   Instale o Corosync e o Pacemaker para fornecer comunicação de cluster e gerenciamento de recursos para alta disponibilidade.

4. **Instalação e configuração do DBMS do PostgreSQL**

   Instale e configure o PostgreSQL nos nós de cluster.

5. **Instalação da Kaspersky Security Center Linux nos nós de cluster de failover**

   Instale a Kaspersky Security Center Linux nos nós de cluster e configure a criptografia entre os nós de cluster.

6 **Instalação do Kaspersky Security Center Web Console nos nós de cluster de failover**

Instale o Kaspersky Security Center Web Console em ambos os nós de cluster de failover para fornecer alta disponibilidade.

Preparação de um sistema de arquivos de nós de cluster

A primeira etapa na preparação para a implementação do cluster de failover da Kaspersky Security Center Linux distribuído geograficamente é a configuração do sistema de arquivos em ambos os nós de cluster. A preparação inclui a criação de volumes lógicos LVM e a configuração de diretórios como pontos de montagem. Execute o procedimento abaixo em ambos os nós de cluster.

Para preparar um sistema de arquivos de nós de cluster:

1. Crie um volume lógico LVM para os dados e o banco de dados do Servidor de Administração:

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Crie um volume lógico LVM separado para armazenar o arquivo de resposta:

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   onde:

   - `volume group name` é o nome do grupo de volumes usado pelo LVM.
   - `klfocdata` e `klfocstate` são nomes de volumes lógicos. Esses volumes lógicos são criados dentro desse grupo de volumes.

     Recomendamos usar esses nomes de volume para fins de consistência, embora você possa especificar nomes personalizados, se necessário.
   - `volume size` é o tamanho do volume. Recomendamos alocar pelo menos 500 GB para os dados e o banco de dados do Servidor de Administração. O volume para armazenar o arquivo de resposta requer uma pequena quantidade de espaço.

2. Crie diretórios a serem usados como pontos de montagem para os volumes lógicos.

   - Para os dados e o banco de dados do Servidor de Administração:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Para o arquivo de resposta:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

Recomendamos usar os diretórios `/mnt/KlFocDataShare_klfoc` e `/mnt/KlFocStateShare_klfoc` para manter a consistência, embora você possa informar nomes personalizados, se necessário.

O sistema de arquivos dos nós de cluster é preparado. Depois disso, você deve configurar um sistema de arquivos de cluster replicado.

Configurar um sistema de arquivos de cluster replicado

Instalar e configurar o DRBD

O *DRBD* é um software de terceiros usado para replicação de dados (especificamente para os volumes de dados e pontos de montagem preparados na etapa anterior).

Depois de preparar o sistema de arquivos dos nós de cluster, você deve instalar os utilitários DRBD e configurar os recursos DRBD para a replicação de dados entre os nós de cluster. Execute o procedimento abaixo em ambos os nós de cluster.

Para instalar e configurar o DRBD em nós de cluster:

1. Instale os utilitários DRBD:

   ```
   apt update
   apt install -y drbd-utils
   ```

   Recomendamos usar o DRBD versão 9.2.6 ou posterior, pois ele fornece criptografia de tráfego integrada.

   O tráfego DRBD também pode ser criptografado usando sua própria solução VPN.

2. Crie arquivos de configuração de recurso DRBD para cada volume lógico criado durante a preparação de um sistema de arquivos (`klfocdata` e `klfocstate`).

   Todos os arquivos de configuração devem ser colocados em `/etc/drbd.d/`.

   - Recurso `klfocdata` (Dados e banco de dados do Servidor de Administração)

     Use a replicação assíncrona (protocolo A) para o recurso klfocdata. Configure todos os outros parâmetros de acordo com seu ambiente.

     Exemplo de arquivo de configuração:

     ```
     resource klfocdata {
         protocol A;
         net {
             after-sb-0pri    discard-least-changes;
             after-sb-1pri    call-pri-lost-after-sb;
             after-sb-2pri    call-pri-lost-after-sb;
         }
         syncer {
             rate 110M;
         }
         # Hostname of the active node
         on db1 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
         # Hostname of the passive node
         on db2 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
     }
     ```

   - Recurso `klfocstate` (o arquivo de resposta)

     Use a replicação síncrona (protocolo C) para criar o recurso klfocstate. Configure todos os outros parâmetros de acordo com seu ambiente.

Exemplo de arquivo de configuração:

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Inicialize os metadados do DRBD para ambos os recursos:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Inicie o DRBD em todos os recursos configurados:

```
drbdadm up all
```

O DRBD é instalado e configurado em ambos os nós de cluster.

Criar um sistema de arquivos replicado no nó de cluster ativo

Depois de instalar e configurar o DRBD em ambos os nós de cluster, crie um sistema de arquivos replicado no nó de cluster ativo. Execute o procedimento abaixo no nó de cluster ativo.

Para criar um sistema de arquivos replicado no nó de cluster ativo:

1. Promova ambos os recursos DRBD para a função Principal:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Formate os dispositivos DRBD para preparar os volumes replicados para uso nos nós de cluster:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Configure os parâmetros do sistema de arquivos:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Monte os dispositivos DRBD nos diretórios criados anteriormente:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

Se o serviço multipathd estiver instalado, ele deve ser configurado para ignorar dispositivos `/dev/drbd*` em ambos os nós de cluster.

5. Verifique o status da replicação:

```
drbdadm status
```

A saída da configuração correta do sistema de arquivos:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Um sistema de arquivos replicado no nó de cluster ativo é configurado. Depois disso, você deve instalar e configurar o Corosync e o Pacemaker nos nós de cluster.

Instalação e configuração do Corosync e o Pacemaker nos nós de cluster

O Corosync e o Pacemaker fornecem comunicação de cluster e gerenciamento de recursos para alta disponibilidade. Eles garantem que os serviços sejam movidos automaticamente para um nó íntegro em caso de falha, minimizando o tempo de inatividade.

Para instalar e configurar o Corosync e o Pacemaker nos nós de cluster:

1. Instale os pacotes necessários em ambos os nós de cluster:

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. Configure o Corosync e o Pacemaker em ambos os nós de cluster de acordo com a documentação oficial. Isso inclui a ativação do início automático, a geração e distribuição da chave de autenticação e a configuração de permissões de acesso para o arquivo authkey.

Para garantir que as configurações estejam corretas, execute o seguinte comando em um dos nós de cluster:

```
crm status
```

A saída esperada deve mostrar o status do cluster e listar todos os nós ativos para confirmar que o Corosync está executando corretamente e que os nós estão se comunicando.

3. Em ambos os nós de cluster, defina as configurações básicas do cluster do Pacemaker:

```
crm configure property stonith-enabled="false"
crm configure property symmetric-cluster="false"
crm configure rsc_defaults resource-stickiness="110"
crm configure rsc_defaults migration-threshold=3
crm configure property no-quorum-policy=ignore
```

4. Em ambos os nós de cluster, desative a inicialização de scripts que serão gerenciados pelo Corosync:

```
systemctl disable drbd.service
```

5. Em um dos nós de cluster, crie os recursos baseados em DRBD no Pacemaker.

- Recurso DRBD para klfocdata

  a. Crie um recurso de cluster para o volume DRBD `klfocdata`, permitindo que o cluster gerencie seu estado e monitore sua integridade automaticamente:

  ```
  crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Crie um recurso gerenciado por cluster `ms_drbd_klfocdata` com base no recurso criado `drbd_klfocdata`:

  ```
  crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. Crie um ponto de montagem para o volume DRBD `fs_klfocdata`, especificando o dispositivo, o diretório de destino, o tipo de sistema de arquivos e as opções de montagem:

  ```
  crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
  ```

- Recurso DRBD para klfocstate

  a. Crie um recurso de cluster para o volume DRBD `klfocstate`, permitindo que o cluster gerencie seu estado e monitore sua integridade automaticamente:

  ```
  crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Crie um recurso ms_drbd_klfocstate gerenciado por cluster com base no recurso `drbd_klfocstate` criado:

  ```
  crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

c. Crie um ponto de montagem para o volume DRBD `fs_klfocstate`, especificando o dispositivo, o diretório de destino, o tipo de sistema de arquivos e as opções de montagem:

```
crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
```

6. Defina a ordem de montagem dos recursos cujos DRBDs estão no estado Primary. Dê a este recurso o nome `cluster_resources`:

```
crm configure colocation cluster_resources inf: fs_klfocdata ms_drbd_klfocdata:Master ms_drbd_klfocstate:Master
```

7. Configure o grupo de recursos e serviços `group_klfoc`:

```
crm configure group group_klfoc fs_klfocdata fs_klfocstate
```

8. Configure o grupo de recursos `group_klfoc` para que seja iniciado após os recursos DRBD correspondentes. Dê a esta regra o nome `all_after_drbd`:

```
crm configure order all_after_drbd inf: ms_drbd_klfocdata:promote group_klfoc:start
```

9. Defina a preferência de inicialização dos recursos primários e secundários: prioridade 100 para `node1` e 50 para `node2`:

```
crm configure location loc_klfocdata_one ms_drbd_klfocdata 100: db1 # hostname of the first cluster node
crm configure location loc_klfocdata_two ms_drbd_klfocdata 50: db2 # hostname of the second cluster node
crm configure location loc_klfocstate_one ms_drbd_klfocstate 100: db1 # hostname of the first cluster node
crm configure location loc_klfocstate_two ms_drbd_klfocstate 50: db2 # hostname of the second cluster node
crm configure location loc_group_one group_klfoc 100: db1 # hostname of the first cluster node
crm configure location loc_group_two group_klfoc 50: db2 # hostname of the second cluster node
```

10. Em ambos os nós de cluster, desative a inicialização automática do serviço DRBD:

```
systemctl disable drbd.service
```

O Corosync e o Pacemaker são instalados e configurados nos nós de cluster. Depois disso, você deve instalar o DBMS e criar o banco de dados do Servidor de Administração e do IAM.

Instalação e configuração do DBMS do PostgreSQL

Depois de instalar e configurar o Corosync e o Pacemaker nos nós de cluster, você deve instalar o DBMS em ambos os nós.

Para instalar e configurar o DBMS:

1. Em ambos os nós de cluster, instale o PostgreSQL 17 x64 ou posterior.

   Consulte a documentação do PostgreSQL para obter informações sobre como fazer a instalação.

2. Os nós de cluster com o DBMS instalado não podem ter contas de usuário DBMS com os seguintes nomes:

   - client
   - iam

- ksc
- locker
- pat
- scope
- voltron

3. Em ambos os nós de cluster, pare o DBMS e, em seguida, desative a inicialização automática do serviço DBMS:

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. No nó de cluster ativo, copie o diretório DBMS para o diretório `/mnt/KlFocDataShare_klfoc/dbms`:

```
rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
```

5. No nó de cluster ativo, copie os arquivos de configuração do PostgreSQL para o diretório `/mnt/KlFocDataShare_klfoc/dbms`:

```
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
```

6. Em ambos os nós de cluster, abra o arquivo de configuração `/etc/postgresql/17/main/postgresql.conf` e, em seguida, defina o diretório `/mnt/KlFocDataShare_klfoc/dbms` como o diretório de dados do banco de dados.

   Especifique também os caminhos para os arquivos de configuração (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` e `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) e remova o parâmetro `include_dir`:

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

7. No arquivo de configuração `/etc/postgresql/17/main/postgresql.conf`, ajuste a configuração do DBMS para atender aos requisitos da Kaspersky Security Center Linux.

8. Crie e configure contas para trabalhar com o PostgreSQL.

9. Crie o recurso de serviço PostgreSQL:

```
crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
psql="/usr/bin/psql" \
pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
config="/etc/postgresql/17/main/postgresql.conf" \
socketdir="/var/run/postgresql" \
op start timeout=60s \
op stop timeout=60s \
op monitor interval=30s timeout=60s
```

10. Adicione o recurso PostgreSQL ao grupo de clusters `group_klfoc`:

```
crm configure edit group_klfoc
```

11. Adicione o nome do `klfocsvc_dbms` recurso PostgreSQL ao final da lista, por exemplo:

```
group group_klfoc {
...
klfocsvc_dbms
}
```

12. No nó de cluster ativo, no servidor DBMS, crie um banco de dados para o IAM. O nome do banco de dados deve ser diferente daquele instalado para uso com o Kaspersky Security Center Linux. O Servidor de Administração não faz a remoção automática do banco de dados do IAM ao desinstalar ou mover o servidor para outro dispositivo. É necessário remover o banco de dados manualmente:

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

O DBMS é instalado e configurado. O banco de dados do Servidor de Administração e do IAM são criados. Depois disso, você deve instalar a Kaspersky Security Center Linux nos nós de cluster.

Instalação da Kaspersky Security Center Linux nos nós de cluster de failover distribuídos geograficamente

O Kaspersky Security Center Linux é instalado nos nós de cluster de failover distribuídos geograficamente por meio de um arquivo de resposta no modo silencioso, ou seja, sem a participação do usuário. O arquivo de resposta contém um conjunto personalizado de parâmetros de instalação: variáveis e seus respectivos valores.

Pré-requisitos:

- Execute todas as etapas preparatórias:
  - Preparação de um sistema de arquivos de nós de cluster
  - Configurar um sistema de arquivos de cluster replicado
  - Instalação e configuração do Corosync e o Pacemaker nos nós de cluster
  - Instalação e configuração do DBMS do PostgreSQL
- Os nós de cluster devem executar o Ubuntu Server 24.04 LTS (Noble Numbat) x64.
- Baixe o arquivo de instalação `ksc64_[version_number]_amd64.deb` do site da Kaspersky.

Instalação no nó ativo

Para instalar a Kaspersky Security Center Linux no nó ativo no modo silencioso:

1. Leia o Contrato de Licença do Usuário Final. Siga as etapas abaixo somente se entender e aceitar os termos do Contrato de Licença do Usuário Final.

2. Crie o grupo `kladmins` e as contas sem privilégios `ksc` e `ksciam` que devem ser membros do grupo `kladmins`. Para fazer isso, execute sequencialmente os seguintes comandos em uma conta com privilégios de raiz:

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

3. No diretório `/mnt/KlFocDataShare_klfoc/`, crie um diretório para os arquivos do Kaspersky Security Center Linux:

```
mkdir /mnt/KlFocDataShare_klfoc/ksc/
```

4. Crie o arquivo de resposta (no formato TXT) e adicione a ele uma lista de variáveis no formato VARIABLE_NAME=variable_value. Adicione cada variável em uma linha separada.

   Na lista de parâmetros usados para a instalação da Kaspersky Security Center Linux no modo silencioso, especifique os seguintes parâmetros necessários para a implementação do cluster distribuído geograficamente:

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     Defina o valor `2` para implantar o cluster distribuído geograficamente.

   - `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` e `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

     O balanceador de DNS com verificação de integridade já deve estar implementado. Os valores desses parâmetros devem ser idênticos e definidos para o FQDN do balanceador de DNS.

5. Defina o valor da variável de ambiente `KLAUTOANSWERS` no ambiente raiz, ou no ambiente do usuário, que contém o nome completo do arquivo de resposta, incluindo o caminho, por exemplo, com o seguinte comando:

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. Inicie a instalação do Kaspersky Security Center Linux no modo silencioso executando os seguintes comandos:

   - No ambiente raiz:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

   - No ambiente do usuário:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

7. Desative a inicialização automática do serviço klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

8. Após a instalação da Kaspersky Security Center Linux, pare o nó de cluster ativo.

9. Mova todos os recursos de cluster para o nó passivo.

   Você pode usar o comando `crm node standby` (e reativá-lo com `crm node online`).

Instalação no nó passivo

Para instalar a Kaspersky Security Center Linux no nó passivo:

1. Execute a instalação do Kaspersky Security Center Linux:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

2. Execute a configuração do Kaspersky Security Center Linux:

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

3. Leia o Contrato de Licença do Usuário Final (EULA) e a Política de Privacidade. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite os seguintes valores:

   - Digite `y` (sim), se você entende e aceita integralmente os termos do EULA. Digite `n` (não) se você não aceita os termos do EULA. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos do EULA.

   - Digite `y` se você entende e aceita os termos da Política de Privacidade e se concorda que seus dados serão tratados e transmitidos (inclusive para países terceiros), conforme descrito na Política de Privacidade. Digite n se você não aceita os termos da Política de Privacidade. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos da Política de Privacidade.

4. Selecione o nó de cluster passivo como um modo de instalação do Servidor de Administração.

5. Quando for solicitado, insira o caminho local para o ponto de montagem do compartilhamento de estado: `/mnt/KlFocStateShare_klfoc`.

6. Desative a inicialização automática do serviço klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Crie o recurso de serviço `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Adicione o recurso `klfocsvc_klfoc` para o grupo `group_klfoc`:

```
crm configure edit group_klfoc
```

9. Anexe `klfocsvc_klfoc` no final da linha de grupo, por exemplo:

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Verifique se todos os recursos estão no estado iniciado no nó ativo.

```
crm status
```

Configuração da criptografia entre nós de cluster

Para configurar a criptografia entre nós de cluster,

Se você instalou o DRBD versão 9.2.6 ou posterior durante a configuração de um sistema de arquivos de cluster replicado, configure a criptografia entre nós de cluster de acordo com a documentação oficial do DRBD.

Como alternativa, você pode criptografar o tráfego entre os nós de cluster usando sua própria solução de VPN.

O cluster de failover da Kaspersky Security Center Linux distribuído geograficamente é instalado. Depois disso, você deve instalar o Kaspersky Security Center Web Console em ambos os nós de cluster.

Cluster distribuído geograficamente que executa o SberLinux com o DBMS do Platform V Pangolin

Seguindo este cenário, você pode preparar sua infraestrutura e implementar um cluster de failover do Kaspersky Security Center Linux distribuído geograficamente.

Pré-requisitos

- Implemente um balanceador de DNS altamente disponível com verificação de integridade.
- Os nós de cluster ativos e passivos devem ser dois dispositivos com configurações de hardware e software idênticas.
  - Requisitos de hardware:
    - CPU: 16 núcleos, 2500 MHz
    - RAM – 32 GB
    - Espaço em disco: 500 GB com 300 IOPS ou superior
    - Controlador de interface de rede: 1 Gbps

- Requisitos de software:
  - Sistema operacional: Platform V SberLinux OS Server (SLO) 9.5.1 64 bits
  - DBMS: Platform V Pangolin 6.5.1 64 bits

Fases

O cluster de failover da Kaspersky Security Center Linux implementado em um único data center não pode ser atualizado para um cluster de failover distribuído geograficamente.

A implementação do cluster de failover da Kaspersky Security Center Linux distribuído geograficamente ocorre em etapas:

1. **Preparar um sistema de arquivos de nós de cluster de failover**

   Prepare o sistema de arquivos em ambos os nós de cluster. A preparação inclui a criação de volumes lógicos LVM e a configuração de diretórios como pontos de montagem.

2. **Configurar um sistema de arquivos de cluster replicado**

   Instale os utilitários DRBD e configure os recursos DRBD para a replicação de dados entre nós de cluster de failover. Depois disso, crie um sistema de arquivos replicado no nó do cluster ativo.

3. **Instalar e configurar o Corosync e o Pacemaker nos nós de cluster de failover**

   Instale o Corosync e o Pacemaker para fornecer comunicação de cluster e gerenciamento de recursos para alta disponibilidade.

4. **Instalação e configuração do DBMS do Platform V Pangolin**

   Instale e configure o Platform V Pangolin nos nós de cluster.

5. **Instalação da Kaspersky Security Center Linux nos nós de cluster de failover**

   Instale a Kaspersky Security Center Linux nos nós de cluster e configure a criptografia entre os nós de cluster.

6. **Instalação do Kaspersky Security Center Web Console nos nós de cluster de failover**

   Instale o Kaspersky Security Center Web Console em ambos os nós de cluster de failover para fornecer alta disponibilidade.

Preparação de um sistema de arquivos de nós de cluster

A primeira etapa na preparação para a implementação do cluster de failover da Kaspersky Security Center Linux distribuído geograficamente é a configuração do sistema de arquivos em ambos os nós de cluster. A preparação inclui a criação de volumes lógicos LVM e a configuração de diretórios como pontos de montagem. Execute o procedimento abaixo em ambos os nós de cluster.

Para preparar um sistema de arquivos de nós de cluster:

1. Crie um volume lógico LVM para os dados e o banco de dados do Servidor de Administração:

```
lvcreate -L <volume size> -n klfocdata <volume group name>
```

Crie um volume lógico LVM separado para armazenar o arquivo de resposta:

```
lvcreate -L <volume size> -n klfocstate <volume group name>
```

onde:

- `volume group name` é o nome do grupo de volumes usado pelo LVM.
- `klfocdata` e `klfocstate` são nomes de volumes lógicos. Esses volumes lógicos são criados dentro desse grupo de volumes.

  Recomendamos usar esses nomes de volume para fins de consistência, embora você possa especificar nomes personalizados, se necessário.
- `volume size` é o tamanho do volume. Recomendamos alocar pelo menos 500 GB para os dados e o banco de dados do Servidor de Administração. O volume para armazenar o arquivo de resposta requer uma pequena quantidade de espaço.

2. Crie diretórios a serem usados como pontos de montagem para os volumes lógicos.

   - Para os dados e o banco de dados do Servidor de Administração:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Para o arquivo de resposta:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

   Recomendamos usar os diretórios `/mnt/KlFocDataShare_klfoc` e `/mnt/KlFocStateShare_klfoc` para manter a consistência, embora você possa informar nomes personalizados, se necessário.

O sistema de arquivos dos nós de cluster é preparado. Depois disso, você deve configurar um sistema de arquivos de cluster replicado.

Configurar um sistema de arquivos de cluster replicado

Instalar e configurar o DRBD

O *DRBD* é um software de terceiros usado para replicação de dados (especificamente para os volumes de dados e pontos de montagem preparados na etapa anterior).

Depois de preparar o sistema de arquivos dos nós de cluster, você deve instalar os utilitários DRBD e configurar os recursos DRBD para a replicação de dados entre os nós de cluster. Execute o procedimento abaixo em ambos os nós de cluster.

Para instalar e configurar o DRBD em nós de cluster:

1. Instale os utilitários DRBD da seguinte forma:

   a. Ative os repositórios EPEL e ELRepo em ambos os nós:

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

b. Liste todas as versões disponíveis do pacote kmod-drbd9x e filtre a lista de pacotes criada para a plataforma el9_6 (por exemplo, a Platform V SberLinux OS Server (SLO) 9.6 é usada):

```
dnf search --showduplicates kmod-drbd9x | grep el9_6
```

c. Instale a versão mais recente disponível da lista em ambos os nós. Exemplo para Platform V SberLinux OS Server (SLO) 9.6:

```
dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
modprobe drbd
```

Caso uma versão mais recente apareça no futuro, substitua a string para a respectiva versão.

Recomendamos usar o DRBD versão 9.2.6 ou posterior, pois ele fornece criptografia de tráfego integrada.

O tráfego DRBD também pode ser criptografado usando sua própria solução VPN.

2. Crie arquivos de configuração de recurso DRBD para cada volume lógico criado durante a preparação de um sistema de arquivos (`klfocdata` e `klfocstate`).

   Todos os arquivos de configuração devem ser colocados em `/etc/drbd.d/`.

   - Recurso `klfocdata` (Dados e banco de dados do Servidor de Administração)

     Use a replicação assíncrona (protocolo A) para o recurso klfocdata. Configure todos os outros parâmetros de acordo com seu ambiente.

     Exemplo de arquivo de configuração:

```
resource klfocdata {
    protocol A;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

   - Recurso `klfocstate` (o arquivo de resposta)

     Use a replicação síncrona (protocolo C) para criar o recurso klfocstate. Configure todos os outros parâmetros de acordo com seu ambiente.

     Exemplo de arquivo de configuração:

```
resource klfocstate {
    protocol C;
    net {
```

```
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Inicialize os metadados do DRBD para ambos os recursos:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Inicie o DRBD em todos os recursos configurados:

```
drbdadm up all
```

O DRBD é instalado e configurado em ambos os nós de cluster.

Criar um sistema de arquivos replicado no nó de cluster ativo

Depois de instalar e configurar o DRBD em ambos os nós de cluster, crie um sistema de arquivos replicado no nó de cluster ativo. Execute o procedimento abaixo no nó de cluster ativo.

Para criar um sistema de arquivos replicado no nó de cluster ativo:

1. Promova ambos os recursos DRBD para a função Principal:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Formate os dispositivos DRBD para preparar os volumes replicados para uso nos nós de cluster:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Configure os parâmetros do sistema de arquivos:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Monte os dispositivos DRBD nos diretórios criados anteriormente:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

   Se o serviço multipathd estiver instalado, ele deve ser configurado para ignorar dispositivos `/dev/drbd*` em ambos os nós de cluster.

5. Verifique o status da replicação:

```
drbdadm status
```

   A saída da configuração correta do sistema de arquivos:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Um sistema de arquivos replicado no nó de cluster ativo é configurado. Depois disso, você deve instalar e configurar o Corosync e o Pacemaker nos nós de cluster.

Instalação e configuração do Corosync e o Pacemaker nos nós de cluster

O Corosync e o Pacemaker fornecem comunicação de cluster e gerenciamento de recursos para alta disponibilidade. Eles garantem que os serviços sejam movidos automaticamente para um nó íntegro em caso de falha, minimizando o tempo de inatividade.

Para instalar e configurar o Corosync e o Pacemaker nos nós de cluster:

1. Instale os pacotes necessários em ambos os nós de cluster:

```
dnf install pcs
dnf install drbd-pacemaker
```

2. Configure o Corosync e o Pacemaker em ambos os nós de cluster de acordo com a documentação oficial. Isso inclui a ativação do início automático, a geração e distribuição da chave de autenticação e a configuração de permissões de acesso para o arquivo authkey.

   Para garantir que as configurações estejam corretas, execute o seguinte comando em um dos nós de cluster:

```
pcs status
```

   A saída esperada deve mostrar o status do cluster e listar todos os nós ativos para confirmar que o Corosync está executando corretamente e que os nós estão se comunicando.

3. Em ambos os nós de cluster, defina as configurações básicas do cluster do Pacemaker:

```
pcs property set stonith-enabled=false
pcs property set symmetric-cluster=false
pcs resource defaults resource-stickiness=110
pcs resource defaults migration-threshold=3
pcs property set no-quorum-policy=ignore
```

4. Em ambos os nós de cluster, desative a inicialização de scripts que serão gerenciados pelo Corosync:

```
systemctl disable drbd.service
```

5. Em um dos nós de cluster, crie os recursos baseados em DRBD no Pacemaker.

- Recurso DRBD para klfocdata

  a. Crie um recurso de cluster para o volume DRBD `klfocdata`, permitindo que o cluster gerencie seu estado e monitore sua integridade automaticamente:

  ```
  pcs resource create drbd_klfocdata ocf:linbit:drbd \
  drbd_resource="klfocdata" \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Master interval=10s \
  op monitor role=Slave interval=30s \
  ```

  b. Crie um recurso gerenciado por cluster `ms_drbd_klfocdata` com base no recurso criado `drbd_klfocdata`:

  ```
  pcs resource clone drbd_klfocdata promotable=true
  master-max=1
  clone-max=2
  clone-node-max=1 notify=true
  ```

  c. Crie um ponto de montagem para o volume DRBD `fs_klfocdata`, especificando o dispositivo, o diretório de destino, o tipo de sistema de arquivos e as opções de montagem:

  ```
  pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
  device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" \
  fstype="ext4" \
  options="data=journal"
  ```

- Recurso DRBD para klfocstate

  a. Crie um recurso de cluster para o volume DRBD `klfocstate`, permitindo que o cluster gerencie seu estado e monitore sua integridade automaticamente:

  ```
  pcs resource create drbd_klfocstate ocf:linbit:drbd \
  drbd_resource=klfocstate \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Promoted interval=10s \
  op monitor role=Unpromoted interval=30s \
  ```

b. Crie um recurso ms_drbd_klfocstate gerenciado por cluster com base no recurso `drbd_klfocstate` criado:

```
pcs resource clone drbd_klfocstate promotable=true \
master-max=1 \
clone-max=2 \
clone-node-max=1 \
notify=true
```

c. Crie um ponto de montagem para o volume DRBD `fs_klfocstate`, especificando o dispositivo, o diretório de destino, o tipo de sistema de arquivos e as opções de montagem:

```
pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" \
fstype="ext4" \
options="noatime"
```

6. Em ambos os nós de cluster, desative a inicialização automática do serviço DRBD:

```
systemctl disable drbd.service
```

O Corosync e o Pacemaker são instalados e configurados nos nós de cluster. Depois disso, você deve instalar o DBMS e criar o banco de dados do Servidor de Administração e do IAM.

Instalação e configuração do DBMS do Platform V Pangolin

Depois de instalar e configurar o Corosync e o Pacemaker nos nós de cluster, você deve instalar o DBMS em ambos os nós.

Para instalar e configurar o DBMS:

1. Em ambos os nós de cluster, instale o Platform V Pangolin 6.5.1 x64 ou posterior.

   Para obter informações sobre como instalar o Platform V Pangolin, consulte a sua documentação.

2. Os nós de cluster com o DBMS instalado não podem ter contas de usuário DBMS com os seguintes nomes:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. No nó de cluster ativo, copie o diretório DBMS para o diretório `/mnt/KlFocDataShare_klfoc/dbms`:

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. Em ambos os nós de cluster, abra o arquivo de configuração `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf` e, em seguida, defina o diretório `/mnt/KlFocDataShare_klfoc/dbms` como o diretório de dados do banco de dados.

   Especifique também os caminhos para os arquivos de configuração (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` e `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) e remova o parâmetro `include_dir`:

   ```
   data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
   hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
   ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
   listen_addresses = '*'
   ```

5. No arquivo de configuração `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf`, ajuste a configuração do DBMS para atender aos requisitos do Kaspersky Security Center Linux.

6. Crie e configure contas para trabalhar com o PostgreSQL.

7. Crie o recurso de serviço DBMS:

   ```
   pcs resource create klfocsvc_dbms pgsql \
   pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
   config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
   op start timeout=60s interval=0s \
   op stop timeout=60s interval=0s \
   op monitor interval=30s timeout=60s \
   op promote timeout=120s interval=0s \
   op demote timeout=120s interval=0s \
   meta target-role=Started
   ```

8. Em ambos os nós de cluster, desative a inicialização automática do serviço DBMS:

   ```
   sudo systemctl disable pangolin.service
   ```

9. Adicione o recurso DBMS `klfocsvc_dbms` ao grupo de cluster `group_klfoc`:

   ```
   pcs resource group add group_klfoc klfocsvc_dbms
   ```

10. Anexe o nome do recurso DBMS `klfocsvc_dbms` no final da lista, por exemplo:

    ```
    group group_klfoc {
    ...
    klfocsvc_dbms
    }
    ```

11. No nó de cluster ativo, no servidor DBMS, crie um banco de dados para o IAM. O nome do banco de dados deve ser diferente daquele instalado para uso com o Kaspersky Security Center Linux. O Servidor de Administração não faz a remoção automática do banco de dados do IAM ao desinstalar ou mover o servidor para outro dispositivo. É necessário remover o banco de dados manualmente:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```

O DBMS é instalado e configurado. O banco de dados do Servidor de Administração e do IAM são criados. Depois disso, você deve instalar a Kaspersky Security Center Linux nos nós de cluster.

Instalação da Kaspersky Security Center Linux nos nós de cluster de failover distribuídos geograficamente

O Kaspersky Security Center Linux é instalado nos nós de cluster de failover distribuídos geograficamente por meio de um arquivo de resposta no modo silencioso, ou seja, sem a participação do usuário. O arquivo de resposta contém um conjunto personalizado de parâmetros de instalação: variáveis e seus respectivos valores.

Pré-requisitos:

- Execute todas as etapas preparatórias:
  - Preparação de um sistema de arquivos de nós de cluster
  - Configurar um sistema de arquivos de cluster replicado
  - Instalação e configuração do Corosync e o Pacemaker nos nós de cluster
  - Instalação e configuração do DBMS do Platform V Pangolin
- Os nós de cluster devem executar o Platform V SberLinux OS Server (SLO) 9.5.1 x64.
- Baixe o arquivo de instalação `ksc64_[version_number]_amd64.deb` do site da Kaspersky.

Instalação no nó ativo

Para instalar a Kaspersky Security Center Linux no nó ativo no modo silencioso:

1. Leia o Contrato de Licença do Usuário Final. Siga as etapas abaixo somente se entender e aceitar os termos do Contrato de Licença do Usuário Final.
2. Crie o grupo `kladmins` e as contas sem privilégios `ksc` e `ksciam` que devem ser membros do grupo `kladmins`. Para fazer isso, execute sequencialmente os seguintes comandos em uma conta com privilégios de raiz:

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

3. No diretório `/mnt/KlFocDataShare_klfoc/`, crie um diretório para os arquivos do Kaspersky Security Center Linux:

   ```
   mkdir /mnt/KlFocDataShare_klfoc/ksc/
   ```

4. Crie o arquivo de resposta (no formato TXT) e adicione a ele uma lista de variáveis no formato VARIABLE_NAME=variable_value. Adicione cada variável em uma linha separada.

Na lista de parâmetros usados para a instalação da Kaspersky Security Center Linux no modo silencioso, especifique os seguintes parâmetros necessários para a implementação do cluster distribuído geograficamente:

- `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

  Defina o valor `2` para implantar o cluster distribuído geograficamente.

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` e `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  O balanceador de DNS com verificação de integridade já deve estar implementado. Os valores desses parâmetros devem ser idênticos e definidos para o FQDN do balanceador de DNS.

5. Defina o valor da variável de ambiente `KLAUTOANSWERS` no ambiente raiz, ou no ambiente do usuário, que contém o nome completo do arquivo de resposta, incluindo o caminho, por exemplo, com o seguinte comando:

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. Inicie a instalação do Kaspersky Security Center Linux no modo silencioso executando os seguintes comandos:

   - No ambiente raiz:

   ```
   apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
   ```

   - No ambiente do usuário:

   ```
   sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
   ```

7. Desative a inicialização automática do serviço klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

8. Após a instalação da Kaspersky Security Center Linux, pare o nó de cluster ativo.

9. Mova todos os recursos de cluster para o nó passivo.

   Você pode usar o comando [[pcs node standby]] (e ativá-lo de volta com [[pcs node online]]).

Instalação no nó passivo

Para instalar a Kaspersky Security Center Linux no nó passivo:

1. Execute a instalação do Kaspersky Security Center Linux:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

2. Execute a configuração do Kaspersky Security Center Linux:

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

3. Leia o Contrato de Licença do Usuário Final (EULA) e a Política de Privacidade. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite os seguintes valores:

   - Digite `y` (sim), se você entende e aceita integralmente os termos do EULA. Digite `n` (não) se você não aceita os termos do EULA. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos do EULA.

   - Digite `y` se você entende e aceita os termos da Política de Privacidade e se concorda que seus dados serão tratados e transmitidos (inclusive para países terceiros), conforme descrito na Política de Privacidade. Digite n se você não aceita os termos da Política de Privacidade. Para usar o Kaspersky Security Center Linux, é necessário aceitar os termos da Política de Privacidade.

4. Selecione o nó de cluster passivo como um modo de instalação do Servidor de Administração.

5. Quando for solicitado, insira o caminho local para o ponto de montagem do compartilhamento de estado: `/mnt/KlFocStateShare_klfoc`.

6. Desative a inicialização automática do serviço klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Crie o recurso de serviço `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Adicione o recurso `klfocsvc_klfoc` para o grupo `group_klfoc`:

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. Anexe `klfocsvc_klfoc` no final da linha de grupo, por exemplo:

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Verifique se todos os recursos estão no estado iniciado no nó ativo.

```
pcs status
```

Configuração da criptografia entre nós de cluster

Para configurar a criptografia entre nós de cluster,

Se você instalou o DRBD versão 9.2.6 ou posterior durante a configuração de um sistema de arquivos de cluster replicado, configure a criptografia entre nós de cluster de acordo com a documentação oficial do DRBD.

Como alternativa, você pode criptografar o tráfego entre os nós de cluster usando sua própria solução de VPN.

O cluster de failover da Kaspersky Security Center Linux distribuído geograficamente é instalado. Depois disso, você deve instalar o Kaspersky Security Center Web Console em ambos os nós de cluster.

Instalação do Kaspersky Security Center Web Console em nós de cluster de failover distribuídos geograficamente

Para uma implementação de um cluster de failover da Kaspersky Security Center Linux distribuído geograficamente, a alta disponibilidade do Kaspersky Security Center Web Console deve ser compatível. Para isso, o Kaspersky Security Center Web Console deve ser instalado em ambos os nós de cluster.

Para instalar o Kaspersky Security Center Web Console:

1. Crie um usuário em ambos os nós para trabalhar com o Kaspersky Security Center Web Console. Para fazer isso, execute o seguinte comando em uma conta com privilégios de raiz:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
   ```

   em que a senha deve conter pelo menos 8 caracteres.

2. Leia o Contrato de Licença de Usuário Final (EULA) em ambos os nós. Caso o kit de distribuição do Kaspersky Security Center Linux não inclua um arquivo TXT com o texto do EULA, é possível baixá-lo pelo site da Kaspersky. Se você não aceitar os termos do Contrato de Licença, não instale o aplicativo.

3. Em ambos os nós, crie um arquivo de resposta que contenha os parâmetros para conexão do Kaspersky Security Center Web Console com o Servidor de Administração: `/etc/ksc-web-console-setup.json`.

   Exemplo de um arquivo de resposta que contém o conjunto mínimo de parâmetros

   O conjunto de parâmetros do arquivo de resposta depende da versão do Servidor de Administração ao qual o Kaspersky Security Center Web Console se conecta:

   - Servidor de Administração versão 16 ou posterior

     Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 16 ou posterior:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

- Servidor de Administração versão 15.4 ou posterior

  Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 15.4 ou anterior:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

É possível instalar o Kaspersky Security Center Web Console no mesmo dispositivo que o Servidor de Administração ou em um dispositivo diferente. Se o Kaspersky Security Center Web Console for instalado em um dispositivo diferente, o endereço do Kaspersky Security Center Web Console (especificado por `address`) e o endereço do Servidor de Administração (especificado por `iamHost` ou `kscHost`) serão diferentes. Se o Kaspersky Security Center Web Console for instalado no mesmo dispositivo que o Servidor de Administração, esses parâmetros terão os mesmos valores.

O valor `iamHost` deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Para obter informações detalhadas, consulte o artigo: Parâmetros de instalação do Kaspersky Security Center Web Console.

Você pode adicionar vários Servidores de Administração de versões diferentes à lista de servidores confiáveis. Nesse caso, os Servidores podem usar métodos de autenticação diferentes.

Recomendamos que os números de porta acima de 1024 sejam especificados. Se você quiser que o Kaspersky Security Center Web Console funcione em portas abaixo de 1024, após a instalação, certifique-se de ter o utilitário setcap e execute o seguinte comando:

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

Se você não tiver o utilitário setcap, é possível instalá-lo. **Clique neste link para visualizar os comandos.**

Para os sistemas operacionais Debian e Ubuntu, execute um dos seguintes comandos:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Para o SUSE Linux Enterprise Server e o Red Hat Enterprise Linux, execute o comando:

- `sudo zypper install libcap-progs`

4. Execute o arquivo de instalação em uma conta com privilégios de root em ambos os nós.

```
sudo apt-get install ksc-web-console-<build number>.x86_64.deb
```

Essa ação inicia a descompactação do arquivo de configuração. Espere até que a instalação seja concluída. Kaspersky Security Center Web Console está instalado no seguinte diretório: `/var/opt/kaspersky/ksc-web-console`.

5. Em um dos nós de cluster, crie um recurso Pacemaker para o serviço KSCWebConsole para que ele se torne um serviço gerenciado pelo Pacemaker:

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. Em ambos os nós, pare o serviço KSCWebConsole e desative sua inicialização automática:

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. Em um dos nós de cluster, adicione o recurso `ksc_webconsole` ao grupo `group_klfoc`:

```
crm configure edit group_klfoc
```

8. Anexe `ksc_webconsole` no final da linha de grupo, após `klfocsvc_dbms`, por exemplo:

```
group group_klfoc {
...
klfocsvc_dbms
ksc_webconsole
}
```

Quando a instalação estiver concluída, você poderá usar o navegador para abrir e fazer login no Kaspersky Security Center Web Console.

Contas para uso com o DBMS

Para instalar e gerenciar o Servidor de Administração e o IAM, você precisa de contas internas do banco de dados. Essas contas permitem acessar o banco de dados e exigem determinados direitos.

Um conjunto de direitos necessários depende dos seguintes critérios:

- Tipo de DBMS:
  - MySQL ou MariaDB
  - Baseado em PostgreSQL

- Método de criação do banco de dados do Servidor de Administração:
  - **Automático**. Durante a instalação do Servidor de Administração, você pode criar automaticamente um banco de dados do Servidor de Administração (adiante também denominado banco de dados do Servidor) usando o instalador do Servidor de Administração (o instalador).
  - **Manual**. Você pode usar um aplicativo de terceiros ou um script para criar um banco de dados vazio. Depois disso, você pode especificar este banco de dados como o banco de dados do Servidor durante a instalação do Servidor de Administração.

O banco de dados do IAM deve ser criado manualmente, independentemente do método escolhido para criar o banco de dados do Servidor de Administração.

Siga o princípio do menor privilégio ao conceder direitos e permissões às contas. Isso significa que os direitos concedidos devem ser suficientes apenas para executar as ações necessárias. Não use contas padrão de superusuário do DBMS, como 'root' ou 'postgres', como usuário de conexão ao DBMS para o Kaspersky Security Center Linux.

Não faça alterações manuais no banco de dados do Servidor de Administração e no banco de dados do IAM, incluindo a modificação de valores, exclusão ou adição de esquemas, tabelas e índices. Quaisquer alterações nos bancos de dados não executadas pelo próprio Servidor de Administração interrompem o seu funcionamento apropriado imediatamente ou logo após a atualização para a versão mais recente ou durante a restauração por meio de uma cópia de backup e assim por diante. A edição de bancos de dados só é permitida quando você tiver recebido instruções explícitas da equipe de Suporte Técnico da Kaspersky.
Ao desinstalar ou migrar o Servidor para outro dispositivo, você precisa excluir manualmente os bancos de dados do Servidor de Administração e do IAM.

As informações a seguir descrevem os direitos do DBMS que você precisa conceder às contas antes de instalar e iniciar o Servidor de Administração.

MySQL e MariaDB

Caso escolha o MySQL ou MariaDB como um DBMS, crie uma conta interna do DBMS para acessá-lo e conceda a essa conta os direitos necessários. Observe que o método de criação do banco de dados não afeta o conjunto de direitos. Os direitos necessários estão listados abaixo:

- Privilégios do esquema:
  - Banco de dados do Servidor de Administração: ALL (excluindo GRANT OPTION)
  - Esquemas do sistema (mysql e sys): SELECT, SHOW VIEW
  - O procedimento armazenado sys.table_exists: EXECUTE (caso use o MariaDB 10.5 ou anterior como um DBMS, não será necessário conceder o privilégio EXECUTE)
- Privilégios globais para todos os esquemas: PROCESS, SUPER.

Para obter mais informações sobre como configurar os direitos da conta, consulte o artigo Criar bancos de dados MySQL e MariaDB e contas de usuário.

Para obter detalhes sobre como mover dados de um espaço de tabelas compartilhado para um espaço de tabelas por arquivo, consulte Mover dados de um espaço de tabelas compartilhado para um espaço de tabelas por arquivo nos DBMSs MySQL e MariaDB.

Configurar privilégios para recuperação de dados do Servidor de Administração

Os direitos que você concedeu à conta interna do DBMS são suficientes para restaurar dados do Servidor de Administração do backup.

DBMS baseado em PostgreSQL

Dependendo do método de criação do banco de dados do servidor, conceda os direitos necessários à função, conforme descrito na tabela abaixo. Para obter mais informações sobre como configurar os direitos da função, consulte o artigo Criar bancos de dados MySQL e MariaDB e contas de usuário.

Direitos da função do Postgres

Criação automática de banco de dados		Criação manual de banco de dados
O usuário do *Postgres* não requer direitos adicionais.	Privilégios para uma nova função: CREATEDB.	Para uma nova função: • Privilégios no banco de dados do Servidor de Administração: ALL. • Privilégios em todas as tabelas no esquema público: ALL. • Privilégios em todas as sequências no esquema público: ALL.

Configurar privilégios para recuperação de dados do Servidor de Administração

Para restaurar dados do Servidor de Administração a partir do backup, a função Postgres usada para acessar o DBMS deve ter direitos de proprietário no banco de dados do Servidor de Administração.

Ao restaurar dados de uma cópia backup, conceda temporariamente direitos de superusuário do Postgres às contas padrão klserver e kliam que o Servidor de Administração e o IAM usam para se conectar ao DBMS (no exemplo, `klserver` e `kliam`, respectivamente):

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
```

Após a recuperação bem-sucedida dos dados, restaure os direitos originais das contas de usuário do Postgres.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

Criação de bancos de dados MySQL e MariaDB e contas de usuário

Pré-requisitos

Antes de criar bancos de dados e atribuir direitos às contas de usuário do SGBD, instale e configure um dos servidores de acordo com os requisitos de otimização (caso ainda não tenha feito isso):

- MariaDB x64 para trabalhar com o Kaspersky Security Center Linux
- MySQL x64 para trabalhar com o Kaspersky Security Center Linux

Não faça alterações manuais no banco de dados do Servidor de Administração e no banco de dados do IAM, incluindo a modificação de valores, exclusão ou adição de esquemas, tabelas e índices. Quaisquer alterações nos bancos de dados não executadas pelo próprio Servidor de Administração interrompem o seu funcionamento apropriado imediatamente ou logo após a atualização para a versão mais recente ou durante a restauração por meio de uma cópia de backup e assim por diante. A edição de bancos de dados só é permitida quando você tiver recebido instruções explícitas da equipe de Suporte Técnico da Kaspersky.
Ao desinstalar ou migrar o Servidor para outro dispositivo, você precisa excluir manualmente o banco de dados.

Para configurar a conta DBMS para instalar o Servidor de Administração:

1. Execute um ambiente para uso com MySQL ou MariaDB na conta raiz criada ao instalar o DBMS:

   ```
   sudo mysql -u root -p
   ```

2. Crie contas de usuário internas do DBMS com senhas. Os instaladores do Servidor de Administração e dos serviços do Servidor de Administração usam essa conta de usuário interna do DBMS para acessar o banco de dados.

   Crie uma conta de usuário do Servidor de Administração chamada `kscdbadmin` e especifique a senha em `<password>`:

   ```
   CREATE USER 'kscdbadmin' IDENTIFIED BY '< senha >';
   ```

3. Conceda os seguintes privilégios para criar a conta DBMS:

   - Privilégios do esquema:
     - Banco de dados do Servidor de Administração: ALL (excluindo GRANT OPTION)
     - Esquemas do sistema (mysql e sys): SELECT, SHOW VIEW
     - O procedimento armazenado sys.table_exists: EXECUTE
   - Privilégios globais para todos os esquemas: PROCESS, SUPER.

   Para conceder os privilégios necessários à conta DBMS criada, execute o seguinte script:

   ```
   GRANT USAGE ON *.* TO 'kscdbadmin';
   GRANT ALL ON kav.* TO 'kscdbadmin';
   ```

```
GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';
GRANT PROCESS ON *.* TO 'kscdbadmin';
GRANT SUPER ON *.* TO 'kscdbadmin';
```

Caso use o MariaDB 10.5 ou anterior como um DBMS, não será preciso conceder o privilégio EXECUTE. Nesse caso, exclua o seguinte comando do script:

`GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin'`.

4. Para visualizar a lista de privilégios concedidos à conta do DBMS, execute o seguinte comando:

   ```
   SHOW grants for 'kscdbadmin';
   ```

5. Crie uma conta do servidor IAM chamada `iamdbadmin` e especifique a senha em <`password`>:

   ```
   CREATE USER 'iamdbadmin' IDENTIFIED BY '<password>';
   ```

   Caso use o MySQL 8.0 ou anterior como um DBMS, observe que, para essas versões, a autenticação "Caching SHA2 password" não é compatível. Altere a autenticação padrão de "Cache de senha SHA2" para "Senha nativa do MySQL":

   - Para criar uma conta DBMS que use a autenticação "Senha nativa do MySQL", execute o seguinte comando:

     ```
     CREATE USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '< senha >';
     ```

   - Para alterar a autenticação de uma conta DBMS existente, execute o seguinte comando:

     ```
     ALTER USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '< senha >';
     ```

6. Conceda os seguintes privilégios para criar a conta DBMS:

   - Privilégios do esquema:
     - Banco de dados do Servidor de Administração: ALL (excluindo GRANT OPTION)
     - Esquemas do sistema (mysql e sys): SELECT, SHOW VIEW
     - O procedimento armazenado sys.table_exists: EXECUTE
   - Privilégios globais para todos os esquemas: PROCESS, SUPER.

   Para conceder os privilégios necessários à conta DBMS criada, execute o seguinte script:

   ```
   GRANT USAGE ON *.* TO 'iamdbadmin';
   GRANT ALL ON iam.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
   GRANT PROCESS ON *.* TO 'iamdbadmin';
   GRANT SUPER ON *.* TO 'iamdbadmin';
   ```

   Caso use o MariaDB 10.5 ou anterior como um DBMS, não será preciso conceder o privilégio EXECUTE. Nesse caso, exclua o seguinte comando do script: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin'`.

7. Para visualizar a lista de privilégios concedidos à conta do DBMS, execute o seguinte comando:

   ```
   SHOW grants for 'iamdbadmin';
   ```

8. Crie um banco de dados do Servidor de Administração (neste exemplo, o nome é *kav*) executando o seguinte comando:

   ```
   CREATE DATABASE kav
   ```

   Use o mesmo nome de banco de dados especificado na etapa de criação da conta de usuário do DBMS.

9. Crie um banco de dados do IAM (neste exemplo, o nome do banco de dados do IAM é *iam*):

   ```
   CREATE DATABASE iam
   ```

Exemplo dos comandos básicos das instruções

```
administrator@ksclinux:~$ sudo mysql -u root -p

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 8

Server version: 8.4.11-0ubuntu0.26.04.1 (Ubuntu)

Copyright (c) 2000, 2026, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its

affiliates. Other names may be trademarks of their respective

owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE USER 'kscdbadmin' IDENTIFIED BY 'Your_P@$$w0rd';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT USAGE ON *.* TO 'kscdbadmin';

ON mysql.* TO 'kscdbadmin';

GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';

GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';

GRANT PROCESS ON *.* TO 'kscdbadmin';

GRANT SUPER ON *.* TO 'kscdbadmQuery OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL ON kav.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)
```

```
mysql> GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';

in';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT PROCESS ON *.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SUPER ON *.* TO 'kscdbadmin';

Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> SHOW grants for 'kscdbadmin';

+-----------------------------------------------------------------------+

| Grants for kscdbadmin@% |

+-----------------------------------------------------------------------+

| GRANT PROCESS, SUPER ON *.* TO `kscdbadmin`@`%` |

| GRANT ALL PRIVILEGES ON `kav`.* TO `kscdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `mysql`.* TO `kscdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `sys`.* TO `kscdbadmin`@`%` |

| GRANT EXECUTE ON PROCEDURE `sys`.`table_exists` TO `kscdbadmin`@`%` |

+-----------------------------------------------------------------------+

5 rows in set (0.00 sec)

mysql> CREATE USER 'iamdbadmin' IDENTIFIED BY 'Your_P@$$w0rd';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT USAGE ON *.* TO 'iamdbadmin';

'iamdbadmin';

GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
```

```
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';

GRANT PROCESS ON *.* TO 'iamdbadmin';

GRANT SUPER ON *.* TO 'iamdbaQuery OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL ON iam.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';

dmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT PROCESS ON *.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SUPER ON *.* TO 'iamdbadmin';

Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> SHOW grants for 'iamdbadmin';

+-------------------------------------------------------------------+

| Grants for iamdbadmin@% |

+-------------------------------------------------------------------+

| GRANT PROCESS, SUPER ON *.* TO `iamdbadmin`@`%` |

| GRANT ALL PRIVILEGES ON `iam`.* TO `iamdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `mysql`.* TO `iamdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `sys`.* TO `iamdbadmin`@`%` |

| GRANT EXECUTE ON PROCEDURE `sys`.`table_exists` TO `iamdbadmin`@`%` |

+-------------------------------------------------------------------+

5 rows in set (0.00 sec)
```

```
mysql> CREATE DATABASE kav;

Query OK, 1 row affected (0.01 sec)

mysql> CREATE DATABASE iam;

Query OK, 1 row affected (0.01 sec)

mysql> exit

Bye

administrator@ksclinux:~$
```

Criar bancos de dados baseados em PostgreSQL e contas de usuário

Antes de conceder direitos à conta do SGBD, verifique se o servidor do SGBD PostgreSQL está configurado para funcionar com o Kaspersky Security Center Linux.

Não faça alterações manuais no banco de dados do Servidor de Administração e no banco de dados do IAM, incluindo a modificação de valores, exclusão ou adição de esquemas, tabelas e índices. Quaisquer alterações nos bancos de dados não executadas pelo próprio Servidor de Administração interrompem o seu funcionamento apropriado imediatamente ou logo após a atualização para a versão mais recente ou durante a restauração por meio de uma cópia de backup e assim por diante. A edição de bancos de dados só é permitida quando você tiver recebido instruções explícitas da equipe de Suporte Técnico da Kaspersky.
Ao desinstalar ou migrar o Servidor para outro dispositivo, você precisa excluir manualmente os bancos de dados do Servidor de Administração e do IAM.

Para criar bancos de dados e configurar contas de usuário do SGBD para instalar o Kaspersky Security Center Linux:

1. Execute o ambiente de gerenciamento do SGBD:

   `sudo -i -u postgres psql`

2. Faça login com o usuário do *Postgres* no banco de dados *Postgres*.

3. Crie a função do Postgres para gerenciar o banco de dados do Servidor de Administração (neste exemplo, a função `kscdbadmin`):

   `CREATE USER "kscdbadmin" WITH PASSWORD '<password>';`

4. Crie um banco de dados do Servidor de Administração (neste exemplo, o nome do banco de dados do Servidor de Administração é `kav`):

   `CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

   Recomendamos especificar a função do Postgres criada na etapa 3 destas instruções como proprietária do banco de dados do Servidor de Administração (neste exemplo, a função é `kscdbadmin` e a senha é `<password>`).

   Especificar outro usuário como proprietário do banco de dados

   Se for necessário especificar outra função do Postgres, conecte-se ao banco de dados do Servidor de Administração com essa função proprietária (ou com a função de superusuário) e execute os seguintes comandos:

```
GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
GRANT USAGE ON SCHEMA public TO "kscdbadmin";
GRANT CREATE ON SCHEMA public TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
```

Certifique-se de que a função de proprietário do banco de dados do Servidor de Administração tenha os privilégios CONNECT e TEMPORARY.

Caso ocorra o erro "A nova codificação (UTF8) é incompatível com a codificação do banco de dados de modelo", crie um banco de dados usando o comando:
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin" TEMPLATE template0;`
em vez de:
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

5. Crie uma função do Postgres para gerenciar o banco de dados do IAM (neste exemplo, a função do Postgres é `iamdbadmin`):

```
CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
```

6. Crie um banco de dados do IAM (neste exemplo, o nome do banco de dados do IAM é `iam`):

```
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

O nome do banco de dados do IAM deve ser diferente do nome do banco de dados instalado para gerenciar o banco de dados do Servidor de Administração.

Recomendamos especificar a função do Postgres criada na etapa 5 destas instruções como proprietária do banco de dados do IAM (neste exemplo, a função é `iamdbadmin` e a senha é `<senha>`).

Especificar outro usuário como proprietário do banco de dados do IAM

Se for necessário especificar outra função do Postgres, conecte-se ao banco de dados do IAM com essa função (ou com a função de superusuário) e execute os seguintes comandos:

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

Certifique-se de que a função de proprietário do banco de dados do IAM tenha os privilégios CONNECT e TEMPORARY.

Caso ocorra o erro "A nova codificação (UTF8) é incompatível com a codificação do banco de dados de modelo", crie um banco de dados usando o comando:
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin" TEMPLATE template0;`
em vez de:
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";`

Exemplo dos comandos básicos das instruções

```
administrator@ksclinux:~$ sudo -i -u postgres psql
psql (18.4 (Ubuntu 18.4-0ubuntu.0.26.04.1))
Type "help" to help.
postgres=# CREATE USER kscdbadmin WITH PASSWORD 'password';
CREATE ROLE
postgres=# CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
CREATE DATABASE
postgres=# CREATE USER iamdbadmin WITH PASSWORD 'password';
CREATE ROLE
postgres=# CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
CREATE DATABASE
postgres=# exit
administrator@ksclinux:~$
```

Mover dados de um espaço de tabela compartilhado para um espaço de tabela individual nos DBMSs MySQL e MariaDB

Em um DBMS MySQL e MariaDB, é possível armazenar dados das seguintes formas:

- Como um espaço de tabela compartilhado, quando os dados de todos os bancos de dados do usuário forem armazenados em um único arquivo (geralmente no arquivo `ibdata1`).
- Como um espaço de tabela individual, quando um espaço para dados separado é criado como um arquivo separado.

Usar um espaço de tabela compartilhado aumenta o risco de fragmentação. Como não é possível executar uma operação `SHRINK`, um arquivo em um espaço de tabela compartilhado pode ocupar cerca de 90% do espaço em disco. Isso prejudica o desempenho do subsistema de disco. Portanto, é útil optar por um espaço de tabela individual.

Este artigo descreve como mover dados de um espaço de tabela compartilhado para um espaço de tabela individual. Se os DBMSs MySQL ou MariaDB também forem utilizados por outros aplicativos, será necessário mover os bancos de dados desses aplicativos para o espaço de tabela individual.

> Qua recomendamos realizar este procedimento somente se você estiver usando os DBMSs MySQL ou MariaDB para o Servidor de Administração.
> Mover dados de um espaço de tabela compartilhado para um espaço de tabela individual mai aumentar a carga no subsistema de disco.

Pré-requisitos

Antes de começar, certifique-se de que:

- Uma cópia de backup dos dados do Servidor de Administração foi criada por meio da execução de uma tarefa de backup de dados ou do utilitário klbackup.
- Uma cópia de backup de outros aplicativos foi criada, cujos bancos de dados são gerenciados por um DBMS MySQL ou MariaDB (se houver).
- No dispositivo com o DBMS instalado, há um espaço livre em disco na partição com o banco de dados.

O espaço em disco necessário corresponde a 150% do tamanho total atual dos bancos de dados (tamanho atual do arquivo `ibdata1`).

Processar

Para mover dados de um espaço de tabela compartilhado para um espaço de tabela individual:

1. Pare o serviço do Servidor de Administração do Kaspersky Security Center e outros aplicativos por meio da instância do DBMS para a qual você deseja executar este procedimento.

2. Dependendo da versão do DBMS, faça login no seu DBMS como superusuário e então, em qualquer aplicativo conveniente, execute o script `fix_tablespace.sql`.

   É possível visualizar os scripts `fix_tablespace.sql` clicando nestes links:

   Visualizar o script para MySQL 5.7 e MariaDB 10.1+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

   Visualizar o script para MySQL 8.0+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
```

```
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

A execução do script não deve ser interrompida.
Se nenhum erro de DBMS ocorreu, mas você interrompeu a execução do script, execute o script novamente ou pare de executar as etapas deste procedimento, reinicie o serviço DBMS e restaure os dados do Servidor de Administração a partir do backup.

3. Na seção `[mysqld]` do arquivo my.cnf, defina o parâmetro `innodb_file_per_table` como `1`.
4. Reinicie o serviço MySQL ou MariaDB.
5. Reinicie o serviço do Servidor de Administração do Kaspersky Security Center.

Os dados serão movidos de um espaço de tabela compartilhado para um espaço de tabela individual.

Certificados para trabalhar com o Kaspersky Security Center Linux

A seção contém informações sobre certificados do Kaspersky Security Center Linux, sobre como emitir e substituir certificados para o Kaspersky Security Center Web Console e como renovar um certificado para o Servidor de Administração caso o Servidor interaja com o Kaspersky Security Center Web Console.

Sobre os certificados do Kaspersky Security Center

O Kaspersky Security Center usa os seguintes tipos de certificados para permitir uma interação segura entre os componentes do aplicativo:

- Certificado do Servidor de Administração
- Certificado móvel
- Certificado do Servidor Web
- Certificado do Kaspersky Security Center Web Console
- Certificado do Identity and Access Manager

Por padrão, o Kaspersky Security Center usa certificados autoassinados (ou seja, certificados emitidos pelo próprio Kaspersky Security Center). Se necessário, você pode substituir os certificados autoassinados por certificados do usuário de acordo com os padrões de segurança da sua organização. Ao usar um certificado personalizado, o arquivo de certificado deve incluir a cadeia completa de chaves públicas, incluindo todos os certificados intermediários até a Autoridade Certificadora (CA) raiz. Depois que o Servidor de Administração verifica se um certificado personalizado atende a todos os requisitos aplicáveis, este certificado assume o mesmo escopo funcional de um certificado autoassinado. A única diferença é que o certificado autoassinado é reemitido automaticamente pelo Servidor de Administração, enquanto o certificado do usuário precisa ser reemitido manualmente após sua expiração. Você pode substituir os certificados por certificados do usuário por meio do utilitário klsetsrvcert ou da seção de propriedades do Servidor de Administração no Kaspersky Security Center Web Console, dependendo do tipo de certificado. Ao usar o utilitário klsetsrvcert, é preciso especificar um tipo de certificado usando um dos seguintes valores:

- C (certificado comum para as portas 13000 e 13291).
- CR (certificado de reserva comum para as portas 13000 e 13291).
- M (certificado móvel para porta 13292).
- MR (certificado de reserva móvel para a porta 13292).
- MCA (autoridade de certificação móvel para certificados de usuário gerados automaticamente).

O período de validade máximo para qualquer um dos certificados do Servidor de Administração deve ser de 397 dias ou menos.

Certificados do Servidor de Administração

Um certificado do Servidor de Administração é necessário para os seguintes propósitos:

- Autenticação do Servidor de Administração quando o Kaspersky Security Center Web Console se conecta a ele.
- Interação segura entre o Servidor de Administração e o Agente de Rede nos dispositivos gerenciados.
- Autenticação quando os Servidores de Administração principais estão conectados aos Servidores de Administração secundários.

O certificado do Servidor de Administração é criado automaticamente durante a instalação do componente do Servidor de Administração e é armazenado no diretório /var/opt/kaspersky/klnagent_srv/1093/cert/. Você especifica o certificado do Servidor de Administração ao criar um arquivo de resposta para instalar o Kaspersky Security Center Web Console. Este certificado é chamado comum ("C"). Após a instalação do Kaspersky Security Center Web Console, o certificado especificado é copiado para o diretório /var/opt/kaspersky/ksc-web-console/certificates/external.

O certificado do Servidor de Administração é válido por 397 dias. O Kaspersky Security Center gera automaticamente um certificado de reserva comum ("CR") 90 dias antes da expiração do certificado comum. O certificado de reserva comum é subsequentemente usado para a substituição perfeita do certificado do Servidor de Administração. Quando o certificado comum está prestes a expirar, o certificado de reserva comum é usado para manter a conexão com as instâncias do Agente de Rede instaladas nos dispositivos gerenciados. Com esta finalidade, o certificado de reserva comum torna-se automaticamente o novo certificado comum 24 horas antes de o antigo certificado comum expirar.

O período de validade máximo para qualquer um dos certificados do Servidor de Administração deve ser de 397 dias ou menos.

Se necessário, você pode atribuir um certificado personalizado ao Servidor de Administração. Por exemplo, isso pode ser necessário melhorar a integração com o PKI existente da sua empresa ou para a configuração personalizada dos campos do certificado. Caso o certificado tenha sido substituído, todos os Agentes de Rede anteriormente conectados ao Servidor de Administração via SSL perderão a conexão e retornarão o "Erro de autenticação do Servidor de Administração". Para eliminar o erro, será necessário restaurar a conexão após a substituição do certificado.

Caso o certificado do Servidor de Administração tenha se perdido, é preciso reinstalar o componente Servidor de Administração e restaurar os dados para poder recuperá-lo.

Você também pode fazer backup do certificado do Servidor de Administração separadamente de outras configurações do Servidor de Administração para mover o Servidor de Administração de um dispositivo para outro, sem reconectar os Agentes de Rede.

Se o Kaspersky Security Center Web Console for aberto em navegadores diferentes e for baixado o arquivo de certificado do Servidor de Administração na janela de propriedades do Servidor de Administração, os arquivos baixados terão nomes diferentes.

Certificados móveis

Um certificado móvel ("M") é necessário para autenticação do Servidor de Administração em dispositivos móveis. Especifique o certificado de dispositivos móveis nas propriedades do Servidor de Administração.

Além disso, existe um certificado de reserva móvel ("MR"), que é usado para a substituição perfeita do certificado móvel. O Kaspersky Security Center gera automaticamente este certificado 90 dias antes da expiração do certificado de dispositivos móveis. Quando o certificado móvel está prestes a expirar, o certificado de reserva móvel é usado para manter a conexão com instâncias do Agente de Rede instaladas em dispositivos móveis gerenciados. Com esta finalidade, o certificado de reserva móvel torna-se automaticamente o novo certificado móvel 24 horas antes de o antigo certificado comum expirar.

Caso o cenário de conexão exija o uso de um certificado de cliente em dispositivos móveis (conexão envolvendo autenticação SSL bidirecional), é possível gerar esses certificados através da autoridade de certificação para certificados de usuário gerados automaticamente ("MCA"). Além disso, nas propriedades do Servidor de Administração, é possível especificar certificados de cliente personalizados emitidos por uma autoridade de certificação, enquanto a integração com a infraestrutura de chave pública (PKI) do domínio de sua organização permite a emissão de certificados de cliente por meio da autoridade de certificação do seu domínio.

Além disso, para a autenticação do Servidor de Administração em dispositivos móveis que executam o sistema operacional iOS, é necessário um certificado do Servidor de MDM do iOS. Para obter mais informações, consulte Configuração de um certificado do Servidor de MDM do iOS.

Certificado do servidor da Web

O Servidor Web, um componente do Servidor de Administração do Kaspersky Security Center, usa um tipo especial de certificado. Esse certificado é necessário para publicar pacotes de instalação do Agente de Rede, que serão baixados posteriormente em dispositivos gerenciados, bem como em pacotes de instalação do Kaspersky Security for Mobile. Para isso, o Servidor Web pode usar vários certificados.

Se a compatibilidade para dispositivo móvel estiver desativada, o Servidor Web usa um dos seguintes certificados, em ordem de prioridade:

1. Certificado de Servidor Web personalizado que você especificou manualmente no Console de Administração
2. Certificado do Servidor de Administração Comum ("C")

Se a compatibilidade para dispositivo móvel estiver habilitada, o Servidor Web usa um dos seguintes certificados, em ordem de prioridade:

1. Certificado de Servidor Web personalizado que você especificou manualmente no Console de Administração
2. Certificado móvel personalizado
3. Certificado móvel autoassinado ("M")
4. Certificado do Servidor de Administração Comum ("C")

Certificado do Kaspersky Security Center Web Console

O Servidor do Kaspersky Security Center Web Console (aqui referido como Web Console) tem seu próprio certificado. Quando você visita um site, o navegador verifica se a conexão é confiável. O certificado do Web Console permite autenticar o Web Console e é usado para criptografar o tráfego entre um navegador e o Web Console.

Quando o Web Console é aberto, o navegador pode informar que a conexão com o Web Console não é privada e o certificado do Web Console é inválido. Essa advertência é exibida porque o certificado do Kaspersky Security Center Web Console é autoassinado e gerado automaticamente pelo Kaspersky Security Center. Para remover essa advertência, é possível fazer o seguinte:

- Substitua o certificado do Web Console por um personalizado (opção recomendada). Crie um certificado confiável na infraestrutura e que atenda aos requisitos para certificados personalizados.
- Adicione o certificado do Web Console na lista de certificados de navegador confiáveis. Recomendamos usar essa opção somente se não puder criar um certificado personalizado.

Por padrão, um certificado autoassinado é válido por 30 dias. Você pode alterar esse valor no arquivo de configuração do Web Console, /var/opt/kaspersky/ksc-web-console/server/config.json. Para aplicar o valor especificado, é necessário reiniciar o processo do Web Console.

O Web Console reemite automaticamente esse certificado e passa a usá-lo antes da data de expiração do certificado autoassinado.

Você pode substituir o certificado autoassinado do Web Console por um certificado do usuário.

Certificado do Identity and Access Manager

Um certificado do Identity and Access Manager (certificado IAM) é necessário para os seguintes propósitos:

- Autenticação do Servidor de Administração quando o navegador de um usuário se conecta a ele por meio do protocolo OAuth.
- Autenticação do Servidor de Administração quando o Kaspersky Security Center Web Console se conecta a ele.

O certificado IAM é criado automaticamente na primeira vez que você executa o Servidor de Administração. O certificado está armazenado no dispositivo do Servidor de Administração no diretório: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem (para o cluster de failover da Kaspersky Security Center: <pasta de dados compartilhada>/iam/main_certificate.pem). Você deve especificar o caminho para o certificado IAM utilizando o parâmetro `iamCertPath` ao criar um arquivo de resposta para instalar o Kaspersky Security Center Web Console.

O certificado IAM é válido por 365 dias. O Kaspersky Security Center gera automaticamente um certificado de reserva do IAM 48 horas antes da expiração do certificado atual. Após isso, o certificado de reserva é utilizado para a substituição descomplicada do certificado IAM expirado.

O período de validade máximo para qualquer um dos certificados IAM deve ser de 397 dias ou menos.

Se necessário, é possível atribuir um certificado IAM personalizado. Por exemplo, isso pode ser necessário melhorar a integração com o PKI existente da sua empresa ou para a configuração personalizada dos campos do certificado.

Ao fazer login no Kaspersky Security Center Web Console, o navegador é redirecionado para a página de login do Servidor de Administração (https://<`Endereço do Servidor de Administração`>:4444) para fazer a autenticação. O tráfego entre o navegador e o Servidor de Administração é criptografado utilizando o protocolo TLS e o certificado IAM.

O navegador pode informar que a conexão com o Servidor de Administração não é privada e que o certificado IAM é inválido. Essa advertência aparece porque o certificado IAM é autoassinado e gerado de forma automática pelo Kaspersky Security Center. Para remover essa advertência, é possível fazer o seguinte:

- Substitua o certificado IAM por um certificado personalizado (opção recomendada). Crie um certificado confiável na infraestrutura e que atenda aos requisitos para certificados personalizados.
- Adicione o certificado IAM à lista de certificados de navegador confiáveis. Recomendamos usar essa opção somente se não puder criar um certificado personalizado.

Requisitos para certificados personalizados usados no Kaspersky Security Center Linux

A tabela abaixo exibe os requisitos para certificados personalizados especificados para diferentes componentes do Kaspersky Security Center Linux.

Tipo de certificado	Requisitos	Comentário
Certificado comum, certificado de reserva comum ("C", "CR")	Comprimento mínimo da chave: 2048. Restrições básicas: • Restrição de comprimento do caminho: nenhuma Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Utilização estendida de chave (opcional): autenticação de servidor, autenticação de cliente. O certificado deve incluir um Nome alternativo da entidade (SAN) válido que contenha o endereço de loopback do Servidor de Administração: • Para IPv4: 127.0.0.1 • Para IPv6: 0:0:0:0:0:0:0:1	O parâmetro Utilização estendida de chave é opcional. O valor da restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhuma", mas não inferior a "1".
Certificado do Servidor Web	Utilização estendida de chave: autenticação do servidor. O contêiner PKCS # 12/PEM do qual o certificado é especificado inclui a cadeia completa de chaves públicas. O nome alternativo do assunto (SAN) do certificado está presente; ou seja, o valor do campo `subjectAltName` é válido. O certificado atende aos requisitos em vigor dos navegadores impostos aos certificados do servidor, bem como aos requisitos básicos atuais do Fórum do navegador/CA.	—
Certificado do Kaspersky Security Center Web Console	Uso estendido de chave (EKU): autenticação do servidor. O contêiner PEM do qual o certificado é especificado inclui a cadeia completa de chaves públicas. O nome alternativo do assunto (SAN) do certificado está presente; ou seja, o valor do campo `subjectAltName` é válido. O valor deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` O certificado atende aos requisitos em vigor de navegadores para certificados de servidor, bem como os requisitos básicos atuais do Fórum do navegador/CA.	Certificados criptografados não são compatíveis com o Kaspersky Security Center Web Console.
Certificado do Identity and Access Manager (certificado do IAM)	Utilização estendida de chave: autenticação do servidor. O contêiner PEM do qual o certificado é especificado inclui a cadeia completa de chaves públicas. O certificado atende aos requisitos em vigor de navegadores para certificados de servidor, bem como os requisitos básicos atuais do Fórum do navegador/CA.	Certificados criptografados não são compatíveis com o Kaspersky Security Center Web Console.

Reemissão dos certificados internos do Kaspersky Security Center Web Console

O Kaspersky Security Center Web Console usa os seguintes certificados:

- Um certificado público (certificado TLS do Web Console), que o Web Console apresenta ao navegador para estabelecer uma conexão HTTPS.
- Um certificado interno que o Web Console usa para conexões TLS.

Certificado público

A maioria dos navegadores impõe um limite no prazo de validade de um certificado. Para se enquadrar neste limite, o prazo de validade do certificado público do Kaspersky Security Center Web Console é limitado a 30 dias. Você pode substituir um certificado existente recebido de uma autoridade de certificação (CA) emitindo um novo certificado autoassinado manualmente.

Quando o Kaspersky Security Center Web Console for aberto, o navegador poderá informar que a conexão com ele não é privada e o certificado dele é inválido. Essa advertência aparece, porque o certificado do Kaspersky Security Center Web Console é autoassinado e gerado automaticamente pelo Kaspersky Security Center. Para remover ou evitar esse aviso, é possível fazer o seguinte:

- Substitua o certificado público autoassinado do Web Console por um certificado do usuário (opção recomendada). Crie um certificado confiável na infraestrutura e que atenda aos requisitos para certificados personalizados.
- Adicione o certificado do Kaspersky Security Center Web Console à lista de certificados confiáveis do navegador. Recomendamos usar essa opção somente se não puder criar um certificado personalizado.

Certificado interno

O certificado interno do Web Console é usado somente para a autenticação mútua interna dos componentes do Web Console e não é exibido ao usuário.

Por padrão, o período de validade do certificado interno do Kaspersky Security Center Web Console é de 3 anos (1095 dias).

14 dias antes do término do prazo especificado, o Web Console exibe uma notificação lembrando você de reemitir o certificado interno.

Para reemitir o certificado interno expirado do Kaspersky Security Center Web Console:

Reinstale o Kaspersky Security Center Web Console executando uma das seguintes ações:

- Caso queira usar o mesmo arquivo de instalação do Kaspersky Security Center Web Console, remova o Kaspersky Security Center Web Console e depois instale a mesma versão do Kaspersky Security Center Web Console.
- Se você deseja usar um arquivo de instalação de uma versão com upgrade, execute o comando de upgrade.

O certificado do Kaspersky Security Center Web Console é reemitido.

Substituir o certificado do Kaspersky Security Center Web Console

Por padrão, quando você instala o Kaspersky Security Center Web Console Server (também conhecido como Kaspersky Security Center Web Console), um certificado do navegador para o aplicativo é emitido automaticamente. Você pode substituir o certificado automaticamente gerado por um certificado personalizado.

Para atribuir um certificado do usuário do Kaspersky Security Center Web Console:

1. Salve o arquivo do certificado e o arquivo da chave privada no seguinte diretório:

   /var/opt/kaspersky/ksc-web-console/certificates/external/

   > Formato de arquivo compatível: PEM.
   > São necessários privilégios de root para ler e gravar no diretório. O usuário sob o qual o serviço interativo do Web Console é executado tem apenas permissão de leitura.

2. Nomeie os arquivos da seguinte forma:

   - web-console.crt: o arquivo do certificado.
   - web-console.key: o arquivo da chave privada sem senha.

Um certificado principal personalizado foi atribuído e está sendo usado pelo Web Console.

Se você quiser substituir o certificado do usuário:

- Se você quiser substituir o certificado do usuário por outro certificado do usuário, siga as mesmas instruções.
- Se você quiser substituir o certificado do usuário por um certificado autoassinado, exclua um ou ambos os arquivos do certificado do usuário.

Quando um certificado do usuário expira, o Web Console exibe uma notificação correspondente e continua a usar o certificado expirado.

Se o certificado principal do usuário que você especificou for inválido, o Web Console exibe uma notificação correspondente, emite um certificado principal autoassinado e passa a usá-lo.

A notificação é exibida pela primeira vez 14 dias antes da expiração do certificado.

Converter um certificado PFX para o formato PEM

Para usar um certificado PFX no Kaspersky Security Center Web Console, você deve primeiro convertê-lo para o formato PEM usando qualquer utilitário multiplataforma baseado em OpenSSL conveniente.

Para converter um certificado PFX para o formato PEM no sistema operacional Linux:

1. Em um utilitário multiplataforma baseado em OpenSSL, execute os seguintes comandos:

   ```
   openssl pkcs12 -in <nome do arquivo.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <nome do arquivo.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Certifique-se de que o arquivo de certificado e a chave privada sejam gerados no mesmo diretório onde o arquivo .pfx está armazenado.

3. O Kaspersky Security Center Web Console não oferece suporte a certificados protegidos por senha. Portanto, execute o seguinte comando em um utilitário multiplataforma baseado em OpenSSL para remover uma senha do arquivo .pem:

```
openssl rsa -in key.pem -out key-without-passphrase.pem
```

Não use o mesmo nome para os arquivos .pem de entrada e saída.

Como resultado, o novo arquivo .pem não é criptografado. Você não precisa inserir uma senha para usá-lo.

Os arquivos .crt e .pem estão prontos para uso, então você pode especificá-los no instalador do Kaspersky Security Center Web Console.

Cenário: especificação do certificado personalizado do Servidor de Administração

É possível atribuir o certificado personalizado do Servidor de Administração, por exemplo, para melhor integração com a infraestrutura de chave pública (PKI) existente de sua empresa ou para configuração personalizada dos campos de certificado. É útil substituir o certificado imediatamente após a instalação do Servidor de Administração e antes que o Assistente de início rápido for concluído.

O período de validade máximo para qualquer um dos certificados do Servidor de Administração deve ser de 397 dias ou menos.

Pré-requisitos

As seguintes condições devem ser atendidas:

- O novo certificado deve ser criado no formato PKCS#12 (por exemplo, por meio da PKI da organização).
- Para o novo certificado, os requisitos listados na tabela abaixo devem ser atendidos.

  Na tabela a seguir, observe o requisito "CA: true". Isso significa que o novo certificado deve ser emitido por uma autoridade de certificação (CA) confiável. O novo certificado com o requisito "CA: true" deve incluir toda a cadeia de confiança e uma chave privada que deve ser armazenada em um arquivo com a extensão pfx ou p12.

Requisitos para os certificados do Servidor de Administração

Tipo de certificado	Requisitos
Certificado comum, certificado de reserva comum ("C", "CR")	Comprimento mínimo da chave: 2048. Restrições básicas: • Restrição de comprimento do caminho: nenhuma O valor da restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhuma", mas não inferior a "1". Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Uso estendido de chave (EKU): autenticação de servidor e autenticação de cliente. O EKU é opcional, mas caso o seu certificado o contenha, os dados de autenticação do servidor e do cliente devem ser especificados no EKU. O certificado deve incluir um Nome Alternativo da Entidade (SAN) válido que contenha o endereço de loopback do Servidor de Administração: • Para IPv4: 127.0.0.1 • Para IPv6: 0:0:0:0:0:0:0:1

Tipo de certificado	Requisitos
Certificado de dispositivo móvel, certificado reserva de dispositivo móvel ("M", "MR")	Comprimento mínimo da chave: 2048. Restrições básicas: • CA: true • Restrição de comprimento do caminho: nenhuma O valor da Restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhum" se o certificado comum tiver um valor de Restrição do comprimento do caminho não inferior a "1". Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Utilização estendida de chave: autenticação do servidor. O EKU é opcional, mas caso o seu certificado o contenha, os dados de autenticação do servidor devem ser especificados no EKU.
Certificado CA para certificados de usuário gerados automaticamente ("MCA")	Comprimento mínimo da chave: 2048. Restrições básicas: • CA: true • Restrição de comprimento do caminho: nenhuma O valor da Restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhum" se o certificado comum tiver um valor de Restrição do comprimento do caminho não inferior a "1". Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Uso estendido de chave (EKU): autenticação do cliente. O EKU é opcional, mas caso o seu certificado o contenha, os dados de autenticação do cliente devem ser especificados no EKU.

Os certificados emitidos por uma CA pública não têm a permissão de assinatura de certificado. Para usar esses certificados, certifique-se de ter instalado o Agente de Rede versão 13 ou posterior em pontos de distribuição ou gateways de conexão na rede. Caso contrário, não será possível usar os certificados sem a permissão de assinatura.

Fases

A especificação do certificado do Servidor de Administração prossegue em etapas:

1. **Substituição do certificado do Servidor de Administração**

   Use a linha de comando do utilitário klsetsrvcert para este fim.

2. **Especificação de um novo certificado e restauração da conexão de Agentes de Rede com o Servidor de Administração**

   Caso o certificado tenha sido substituído, todos os Agentes de Rede anteriormente conectados ao Servidor de Administração via SSL perderão a conexão e retornarão o "Erro de autenticação do Servidor de Administração". Para especificar o novo certificado e restaurar a conexão, use a linha de comando com o utilitário klmover.

3. **Especificação de um novo certificado no diretório de certificados do Kaspersky Security Center Web Console**

   Salve o arquivo com o certificado do Servidor de Administração no diretório: /var/opt/kaspersky/ksc-web-console/certificates/external/

   Nomeie o arquivo como <address>-admin-server.crt, em que <address> é o endereço do Servidor de Administração especificado na configuração `iamHost` do arquivo de respostas do instalador do Web Console.

Formato de arquivo compatível: PEM.
A leitura e a gravação no diretório exigem privilégios de root. O usuário sob o qual o serviço interativo do Web Console é executado tem apenas permissão de leitura.

Resultados

Ao concluir o cenário, o certificado do Servidor de Administração é substituído e o servidor é autenticado pelos Agentes de Rede nos dispositivos gerenciados.

Substituição do certificado do Servidor de Administração usando o utilitário klsetsrvcert

Para evitar perder o controle dos dispositivos, consulte Cenário: Especificar o certificado personalizado do Servidor de Administração antes de continuar.

Para substituir o certificado do Servidor de Administração:

Na linha de comando, execute o seguinte utilitário:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o
<validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

A descrição dos parâmetros do utilitário klsetsrvcert é apresentada na tabela abaixo.

Valores dos parâmetros do utilitário klsetsrvcert

Configuração	Valor
`-t < tipo de certificado >`	Tipo de certificado a ser substituído. Valores possíveis do parâmetro `< tipo de certificado >`: • `C` – substitui o certificado para as portas 13000 e 13291. • `CR` – substitui o certificado reserva comum para as portas 13000 e 13291.
`-f < horário da substituição >`	Cronograma de alteração do certificado, usando o formato "DD-MM-AAA hh:mm" (para portas 13000 e 13291). Utilize esse parâmetro se quiser substituir o certificado comum pelo certificado de reserva comum antes que o certificado comum expire. Especifique a hora em que os dispositivos gerenciados devem ser sincronizados com o Servidor de Administração em um novo certificado.
`-i < caminho para o novo certificado >`	Contêiner com o certificado e chave privada no formato PKCS#12 (arquivo com a extensão .p12 ou .pfx).
`-p < senha >`	Senha usada para a proteção o contêiner p12. O certificado e uma chave privada são armazenados no contêiner, portanto, a senha é necessária para descriptografar o arquivo com o contêiner.
`-o < parâmetros de validação >`	Parâmetros de validação de certificado (separados por ponto e vírgula). Para usar um certificado personalizado sem a permissão de assinatura, especifique `-o NoCA` no utilitário klsetsrvcert. Isso é útil para certificados emitidos por uma CA pública. Para alterar o comprimento da chave de criptografia para os tipos de certificado C ou CR, especifique `-o RsaKeyLen:< comprimento da chave >` no utilitário klsetsrvcert, em que o parâmetro `< comprimento da chave >` é o valor do comprimento da chave necessário. Caso contrário, o comprimento da chave do certificado atual será usado.
`-g < nome dns >`	Um novo certificado será criado para o nome DNS especificado (Nome comum e Nome alternativo da entidade).

Configuração	Valor
`-r < certificados raiz >`	Lista de autoridades de certificado raiz confiáveis, formato PEM.
`-l < caminho do arquivo de registro >`	Arquivo de saída dos resultados. Por padrão, a saída é redirecionada no fluxo de saída padrão.

Por exemplo, para especificar o certificado personalizado do Servidor de Administração, use o seguinte comando:

```
klsetsrvcert -t C -i <caminho para o novo certificado> -p <senha> -o NoCA
```

Após a substituição do certificado, todos os Agentes de Rede conectados com Servidor de Administração por meio de SSL perdem a conexão. Para restaurá-la, use a linha de comando do utilitário klmover.

Para evitar a perda das conexões dos Agentes de Rede, use os seguintes comandos:

1. Para instalar o novo certificado,

   ```
   klsetsrvcert -t CR -i <caminho para o novo certificado> -p <senha> -o NoCA
   ```

2. Para especificar a data em que o novo certificado será aplicado,

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

em que "`DD-MM-YYYY hh:mm`" é a data 3 a 4 semanas antes da data atual. A mudança de horário para alterar o certificado para um novo permitirá que um novo certificado seja distribuído a todos os Agentes de Rede.

Perguntas e Respostas

Quais etapas adicionais são necessárias após a substituição do certificado comum do Servidor de Administração?

1. Garanta que os **requisitos para certificados personalizados sejam atendidos**.

   Se você estiver usando um certificado personalizado em vez do autoassinado, antes de atualizar a Kaspersky Security Center Linux para a versão mais recente, certifique-se de que o certificado inclua o Nome alternativo da entidade (SAN). Caso contrário, é importante substituir o certificado antes de atualizar o Kaspersky Security Center Linux. Caso contrário, você não poderá fazer login no Web Console após a atualização.

   Para certificar-se de que o certificado inclui o SAN:

   1. No dispositivo com o Servidor de Administração instalado, execute o comando:

      - Para um dispositivo baseado em Linux:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - Para um dispositivo baseado em Windows:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

2. Assegure-se de que o Nome alternativo da entidade (SAN) esteja presente na saída do comando e contenha o endereço do dispositivo do Servidor de Administração.

3. Se o Nome alternativo da entidade estiver ausente, use o utilitário klsetsrvcert para substituir o certificado do usuário por um certificado que atenda aos requisitos.

2. O arquivo de configuração do Servidor IAM deve conter o endereço atual do Servidor de Administração. Caso contrário, adicione o endereço ao arquivo de configuração.

3. Reinstale o Web Console para evitar o seguinte erro:

   O Servidor de Administração usa um certificado não confiável. Reconfigure o aplicativo especificando um certificado válido ou entre em contato com o administrador principal.

Conexão dos Agentes de Rede ao Servidor de Administração usando o utilitário klmover

Você pode usar o utilitário klmover para restabelecer a conexão de dispositivos não gerenciados com o Servidor de Administração, por exemplo, após uma falha do Servidor de Administração, caso a restauração pelo backup não seja possível.

Para restaurar a conexão, execute o utilitário klmover na linha de comando:

- Para Linux:
  - Para sistemas de 32 bits: `/opt/kaspersky/klnagent/bin/klmover [-address <endereço do servidor>] [-pn <número da porta>] [-ps <número da porta SSL>] [-nossl] [-cert <caminho para o arquivo do certificado>`
  - Para sistemas de 64 bits: `/opt/kaspersky/klnagent64/bin/klmover [-address <endereço do servidor>] [-pn <número da porta>] [-ps <número da porta SSL>] [-nossl] [-cert <caminho para o certificado do arquivo>]`
- Para Windows:
  - Para sistemas de 32 bits: `<caminho>\klmover.exe [-address <endereço do servidor>] [-pn <número da porta>] [-ps <número da porta SSL>] [-nossl] [-cert <caminho para o certificado do arquivo>`
  - Para sistemas de 64 bits: `<caminho>\klmover.exe [-address <endereço do servidor>] [-pn <número da porta>] [-ps <número da porta SSL>] [-nossl] [-cert <caminho para o certificado do arquivo>`
- Para macOS:

  `/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <endereço do servidor>] [-pn <número da porta>] [-ps <número da porta SSL>] [-nossl] [-cert <caminho para o arquivo do certificado>]`

onde `<caminho>` é o caminho de instalação padrão do Agente de Rede ou o caminho de instalação especificado por você nas configurações do pacote de instalação do Agente de Rede.

Para impedir que intrusos movam dispositivos para fora do controle do Servidor de Administração, é altamente recomendável ativar a proteção por senha para executar o utilitário klmover. Para ativar a proteção por senha, selecione a opção **Usar senha de desinstalação** nas configurações da política do Agente de Rede.

Se você perder ou esquecer a senha do Agente de Rede protegido por senha instalado no dispositivo que não está mais sob a gestão do Kaspersky Security Center Linux, não será possível remover o Agente de Rede por meio do utilitário klmover ou da linha de comando. Nesse caso, será necessário reinstalar o sistema operacional no dispositivo com o Agente de Rede instalado e protegido por senha.

O utilitário klmover requer direitos de administrador local.

A ativação da opção **Usar senha de desinstalação** em dispositivos Windows também ativará a proteção por senha para a ferramenta Cleaner (cleaner.exe).

Você não pode usar o utilitário klmover para dispositivos clientes conectados ao Servidor de Administração por meio de gateways de conexão. Para esses dispositivos, você precisa reconfigurar o Agente de Rede ou reinstalar o Agente de Rede e especificar o gateway de conexão.

A descrição dos parâmetros do utilitário klmover é apresentada na tabela abaixo.

Valores dos parâmetros do utilitário klmover

Configuração	Valor
`-address < endereço do servidor >`	Endereço do Servidor de Administração para conexão. É possível especificar um endereço IP ou o nome DNS.
`-pn < número da porta >`	Número da porta pela qual a conexão não criptografada será estabelecida com Servidor de Administração. O número da porta padrão é 14000.
`-ps < número da porta SSL >`	Número da porta SSL pela qual a conexão criptografada será estabelecida com o Servidor de Administração usando o protocolo SSL. O número da porta padrão é 13000.
`-nossl`	Usa a conexão não criptografada com Servidor de Administração. Caso a chave não esteja sendo usada, o agente de rede é conectado ao Servidor de Administração usando o protocolo SSL codificado.
`-cert < caminho para o arquivo do certificado >`	Usa o arquivo de certificado especificado para autenticação de acesso com o Servidor de Administração.
`-nauninstpwd < senha >`	Use este parâmetro para especificar a senha de desinstalação do Agente de Rede. Configuração opcional.

Reemissão do certificado do servidor da Web

O certificado do Servidor Web usado no Kaspersky Security Center Linux é necessário para publicar pacotes de instalação do Agente de Rede que você posteriormente distribui aos dispositivos gerenciados, bem como para publicar perfis de iOS MDM, aplicativos iOS e pacotes de instalação do Kaspersky Endpoint Security for Mobile. Dependendo da configuração atual do aplicativo, vários certificados podem funcionar como o certificado do servidor Web (para obter mais detalhes, consulte Sobre os certificados do Kaspersky Security Center Linux).

Pode ser necessário emitir novamente o certificado do Servidor Web para atender aos requisitos de segurança específicos da sua organização ou para manter a conexão contínua dos dispositivos gerenciados antes de iniciar a atualização do aplicativo. O Kaspersky Security Center oferece duas maneiras de reemitir o certificado do Servidor Web. A escolha entre os dois métodos depende de haver dispositivos móveis conectados e gerenciados por meio do protocolo móvel (ou seja, usando o certificado de dispositivos móveis).

Se você nunca especificou seu próprio certificado personalizado como o certificado do Servidor da Web na seção **Servidor Web** da janela de propriedades do Servidor de Administração, o certificado móvel atua como o certificado do Servidor Web. Nesse caso, a reemissão do certificado do Web Server é realizada por meio da reemissão do próprio protocolo móvel.

Para reemitir o certificado do Servidor Web se você algum dispositivo móvel gerenciado por meio do protocolo móvel:

1. Gere seu certificado personalizado e prepare-o para uso no Kaspersky Security Center Linux. Verifique se o certificado personalizado atende aos requisitos do Kaspersky Security Center Linux. Se necessário, modifique o certificado.

2. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

3. Na guia **Geral**, selecione a seção **Servidor Web**.

4. Na subseção **Via HTTP**, selecione a opção **Carregar certificado do arquivo** e clique no botão **Alterar certificado**.

5. Na janela que é aberta, no campo **Formato do certificado** selecione o tipo do seu certificado:

   - Se você selecionou **Contêiner PKCS#12**, clique no botão **Procurar** ao lado do campo **Certificado** e especifique o arquivo de certificado em seu disco rígido. Se o arquivo do certificado for protegido por senha, digite a senha no campo **Senha**.

   - Se você selecionou **Certificado X.509**, clique no botão **Procurar** ao lado do campo **Chave privada** e especifique a chave privada no seu disco rígido. Se a chave privada for protegida por senha, digite a senha no campo **Senha**.

6. Clique no botão **Salvar** e, em seguida, clique em **OK**.

   A janela é fechada.

7. Se necessário, no campo **Porta HTTPS do Servidor Web**, altere o número da porta HTTPS para o Servidor Web e clique no botão **Salvar**.

O certificado do Servidor Web é emitido novamente.

Para reemitir o certificado do Servidor Web quando você não tiver nenhum dispositivo móvel gerenciado por meio do protocolo móvel:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Certificados**.

3. Se você planeja continuar usando o certificado emitido pelo Kaspersky Security Center, faça o seguinte:

   a. Selecione a opção **Certificado emitido através do Servidor de Administração** e clique no botão **Procurar**.

   b. Na janela que é aberta, em **Endereço de conexão** e grupos de configurações **Termo de ativação**, selecione as opções relevantes e clique em **OK**.

Como alternativa, se você planeja usar seu próprio certificado personalizado, faça o seguinte:

a. Verifique se o certificado personalizado atende aos requisitos do Kaspersky Security Center Linux. Se necessário, modifique o certificado.

b. Selecione a opção **Outro certificado**, clique no botão **Gerenciar certificado** e, na janela que é aberta, clique no botão **Procurar**.

c. Na janela que é aberta, no campo **Formato do certificado** selecione o tipo do seu certificado:

   - Se você selecionou **Contêiner PKCS#12**, clique no botão **Procurar** ao lado do campo **Certificado** e especifique o arquivo de certificado em seu disco rígido. Se o arquivo do certificado for protegido por senha, digite a senha no campo **Senha**.

   - Se você selecionou **Certificado X.509**, clique no botão **Procurar** ao lado do campo **Chave privada** e especifique a chave privada no seu disco rígido. Se a chave privada for protegida por senha, digite a senha no campo **Senha**.

d. Clique no botão **Salvar** e, em seguida, clique em **OK**.

O certificado móvel é reemitido para ser usado como o certificado do Servidor Web.

Alterar o certificado IAM padrão para um certificado personalizado

Para atribuir um certificado do usuário do IAM:

1. Gere seu certificado personalizado e prepare-o para uso no Kaspersky Security Center Linux. Verifique se o certificado personalizado atende aos requisitos do Kaspersky Security Center Linux.

2. Certifique-se de que o grupo kladmins tenha acesso aos arquivos do certificado IAM.

3. Localize o arquivo de configuração do IAM: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   Neste arquivo, adicione os caminhos para os arquivos de certificado IAM à seção `server_iam`:

   - `certificates.main.cert`: Caminho para o arquivo do certificado principal.

   - `certificates.main.key`: Caminho para a chave privada do certificado principal. A chave privada não deve ser protegida por senha.

4. Reinicie o serviço kliam executando o seguinte comando:

   ```
   sudo service kliam_srv restart
   ```

5. Salve o arquivo do certificado IAM no seguinte diretório:

   /var/opt/kaspersky/ksc-web-console/certificates/external/

Formato de arquivo compatível: PEM.
O usuário sob o qual o serviço Kaspersky Security Center Web Console é executado deve ter privilégios suficientes para ler os arquivos salvos no diretório.

6. Dê ao arquivo o nome: <address>-iam-server.crt

   em que <address> é o endereço do IAM especificado na configuração `iamHost` do arquivo de respostas do instalador do Web Console.

Um certificado do usuário do IAM foi atribuído e está sendo usado pelo Web Console.

Se precisar substituir o certificado do usuário do IAM, siga as mesmas instruções.

Se o seu certificado IAM não for válido e um novo certificado válido não tiver sido recebido, um erro será exibido no Web Console.

Por padrão, uma notificação de aviso é exibida 14 dias antes do vencimento do certificado atual. Uma notificação crítica é exibida 2 dias antes do vencimento do certificado atual.

Se o IAM tiver mudado para um certificado de reserva depois que você especificou manualmente um certificado IAM (autoassinado ou de usuário) para o Web Console, o Web Console obterá automaticamente o certificado IAM de reserva e continuará a se conectar ao Servidor de Administração. O certificado do usuário que você especificou permanece no diretório /var/opt/kaspersky/ksc-web-console/certificates/external, mas não é usado.

Para alterar o certificado IAM de reserva:

1. Localize o arquivo de configuração do IAM: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   Nesse arquivo, especifique os caminhos para os arquivos do certificado IAM:

   - `server_iam.certificates.reserve.cert`: Caminho para o arquivo do certificado principal.
   - `server_iam.certificates.reserve.key`: Caminho para a chave privada do certificado principal. A chave privada não deve ser protegida por senha.

2. Reinicie o serviço kliam executando o seguinte comando:

   ```
   sudo systemctl restart kliam_srv.service
   ```

   Quando o arquivo do certificado atual expirar, o certificado IAM de reserva será usado em seu lugar.

Adicionar o endereço do Servidor de Administração à configuração do Servidor IAM

Depois de alterar o certificado do Servidor de Administração comum ("C") durante uma atualização, realocação ou migração, você precisa especificar o endereço do Servidor de Administração no arquivo de configuração do Servidor IAM para garantir a validação adequada do certificado entre o Servidor IAM e o Servidor de Administração.

Para adicionar o endereço do Servidor de Administração à configuração do Servidor IAM:

1. Obtenha o valor Nome alternativo da entidade (SAN) do certificado do Servidor de Administração comum ("C") executando o seguinte comando:

```
sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
```

2. Dependendo da saída do comando, execute uma das seguintes ações:

- Se a saída indicar que o valor está ausente ou contém apenas o endereço IP da rede, verifique os **requisitos do certificado do usuário**.

  Se você estiver usando um certificado personalizado em vez do autoassinado, antes de atualizar a Kaspersky Security Center Linux para a versão mais recente, certifique-se de que o certificado inclua o Nome alternativo da entidade (SAN). Caso contrário, é importante substituir o certificado antes de atualizar o Kaspersky Security Center Linux. Caso contrário, você não poderá fazer login no Web Console após a atualização.

  Para certificar-se de que o certificado inclui o SAN:

  1. No dispositivo com o Servidor de Administração instalado, execute o comando:

     - Para um dispositivo baseado em Linux:

       ```
       sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
       ```

     - Para um dispositivo baseado em Windows:

       ```
       certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
       ```

  2. Assegure-se de que o Nome alternativo da entidade (SAN) esteja presente na saída do comando e contenha o endereço do dispositivo do Servidor de Administração.

  3. Se o Nome alternativo da entidade estiver ausente, use o utilitário klsetsrvcert para substituir o certificado do usuário por um certificado que atenda aos requisitos.

  Se ele não atender aos requisitos, substitua o certificado comum do Servidor de Administração no Servidor de Administração anterior usando o utilitário klsetsrvcert. Depois disso, repita o procedimento de atualização, realocação ou migração.

- Se o valor corresponder ao valor especificado durante a instalação do Kaspersky Security Center Linux (na etapa **Insira o nome DNS do servidor IAM** do assistente de instalação ou, para instalação silenciosa, no parâmetro `KLSRV_UNATT_IAM_ADDRESS`), nenhuma ação adicional é necessária. O Servidor IAM e o Servidor de Administração vão interagir corretamente.

- Se o valor contiver nomes DNS ou endereços de loopback (127.0.0.1 e/ou 0:0:0:0:0:0:0:1), use um deles no arquivo de configuração. Recomenda-se o uso do endereço 127.0.0.1.

3. Em `server_iam` no arquivo de configuração do Servidor IAM, certifique-se de que o valor `ksc_address: "<SAN_address>"` esteja definido como um dos endereços SAN no certificado geral do Servidor de Administração.

   Você pode usar um editor de texto para modificar o arquivo de configuração do Servidor IAM, por exemplo, vi. O seguinte comando abre o arquivo no editor de texto vi:

```
vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Exemplo do bloco server_iam no arquivo de configuração do Servidor IAM:

```
server_iam:
    iam_address: "ksc.example.com"
    server_display_name: "ksc.example.com"
    ksc_address: "oldksc.example.internal"
    ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
```

Use o mesmo espaçamento do exemplo.

4. Certifique-se de que o nome da rede na configuração `ksc_address` seja resolvido para o endereço de loopback (127.0.0.1 ou 0:0:0:0:0:0:0:1) do Servidor de Administração. Para fazer isso, você pode usar o utilitário Ping no Servidor de Administração.

   Se o endereço permitido for diferente ou não puder ser resolvido, adicione uma linha ao arquivo de hosts no Servidor de Administração.

5. Reinicie o serviço do Servidor IAM para aplicar as alterações de configuração executando o seguinte comando:

   ```
   sudo systemctl restart kliam_srv.service
   ```

O endereço do Servidor de Administração é adicionado ao arquivo de configuração do Servidor IAM pelo certificado comum do Servidor de Administração.

Solução de problemas

Vários Servidores de Administração com o mesmo nome de rede na rede e problemas de configuração do Servidor IAM podem causar erros ao fazer login no Web Console. A tabela abaixo descreve possíveis erros e resoluções.

Erro	Descrição	Solução
Sua solicitação não pode ser processada no momento. Aguarde e tente novamente.	Além do processo de inicialização dos dados após atualizar ou restaurar o Kaspersky Security Center Linux, este erro pode ocorrer se a conexão com o Servidor de Administração usando o endereço de rede especificado falhar.	Verifique se o endereço especificado resolve para o endereço IP do Servidor de Administração atual.
O Servidor de Administração usa um certificado não confiável. Reconfigure o aplicativo especificando um certificado válido ou entre em contato com o administrador principal.	O erro pode ocorrer se o valor do endereço no arquivo de configuração do Servidor IAM não corresponder ao valor no atributo Nome alternativo da entidade (SAN) do certificado comum do Servidor de Administração.	Siga as instruções acima.
O nome de usuário ou a senha estão incorretos.	Além das credenciais incorretas, este erro pode ocorrer se outro Servidor de Administração com o mesmo nome já existir na rede.	Verifique se o endereço especificado resolve para o endereço IP do Servidor de Administração atual.

Definir uma pasta compartilhada

Após a instalação do Servidor de Administração, é possível especificar o local da pasta compartilhada nas propriedades do Servidor de Administração. Por padrão, a pasta compartilhada é criada no dispositivo com o Servidor de Administração. No entanto, em alguns casos (como alta carga ou a necessidade para o acesso a partir de uma rede isolada), é útil localizar a pasta compartilhada em um recurso de arquivo dedicado.

A pasta compartilhada é usada ocasionalmente na implementação de Agente de Rede.

A diferenciação entre maiúsculas e minúsculas para a pasta compartilhada deve estar desativada.

Login no Kaspersky Security Center Web Console e logout

É possível fazer login no Kaspersky Security Center Web Console após instalar o Servidor de Administração e o Web Console Server. Você deve saber o endereço da Web do Servidor de Administração e o número de porta especificado durante a instalação (por padrão, a porta é 8080). No navegador, o JavaScript deve ser ativado.

É possível fazer login no Kaspersky Security Center Web Console usando os seguintes métodos:

- Ao usar a autenticação do domínio (conexão única)

  Este método é utilizado para a autenticação segura no Kaspersky Security Center Web Console conectado ao Servidor de Administração versão 16 e posteriores. Se você deseja usar a autenticação do domínio, deve especificar parâmetros adicionais para a interação com o Identity and Access Manager (IAM) durante a instalação do Kaspersky Security Center Web Console.

- Ao especificar o nome e a senha de usuário do domínio

  Antes de entrar com uma conta de usuário do domínio, faça a sondagem do controlador de domínio para obter a lista de usuários do domínio. Em seguida, você deve especificar o nome do usuário do domínio e a senha para fazer login no Servidor de Administração. Este método oferece autenticação somente via Microsoft Active Directory.

- Ao especificar o nome e a senha de usuário interno

A conta de usuário com a qual você deseja fazer login no Kaspersky Security Center Web Console deve ter uma função atribuída. Antes de entrar, certifique-se de que o domínio ou a conta de usuário interno tenham uma função atribuída. Caso contrário, ocorrerá um erro de login.

Fazer login utilizando a autenticação do domínio (conexão única)

Para fazer login no Kaspersky Security Center Web Console usando a autenticação do domínio:

1. No navegador, acesse o endereço https://<Kaspersky Security Center Web Console>:<Número da porta>.

   A página de seleção do Servidor de Administração será exibida.

2. Se tiver adicionado vários servidores confiáveis, selecione, na lista Servidores de Administração, o Servidor de Administração ao qual deseja se conectar.

   Caso apenas um Servidor de Administração tenha sido adicionado, a lista de Servidores de Administração não será exibida.

   O navegador será redirecionado para o endereço https://<Servidor de Administração>:4444.

3. Configure a autenticação do domínio Kerberos.

4. Execute uma das seguintes ações:

   - Clique no botão **Usar autenticação do domínio**.
   - Caso um ou mais Servidores de Administração virtuais sejam criados no Servidor e o usuário desejar fazer login no Servidor virtual usando a autenticação do domínio:

     a. Clique em **Mostrar as opções do Servidor virtual**.

     b. Digite o nome do Servidor de Administração virtual que você especificou enquanto criava o servidor virtual.

     c. Clique no botão **Usar autenticação do domínio**.

5. Especifique o código de segurança de uso único gerado pelo app autenticador no dispositivo móvel.

   No primeiro login, configure a autenticação em duas etapas para a sua conta. Se a configuração da autenticação de dois fatores não estiver disponível, entre em contato com um usuário que tenha o direito Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário** e tenha configurado a autenticação de dois fatores, a fim de adicionar sua conta à lista de permissão da autenticação de dois fatores.

Após o login, a página inicial do Kaspersky Security Center Web Console será exibida, contendo o idioma e o tema usados pela última vez. Você pode navegar pelo Kaspersky Security Center Web Console e usá-lo para uso com o Kaspersky Security Center Linux.

Fazer login especificando o nome e a senha do domínio ou usuário interno

Para fazer login no Kaspersky Security Center Web Console especificando o nome de usuário e a senha:

1. No navegador, acesse o endereço https://<Kaspersky Security Center Web Console>:<Número da porta>.

   A página de seleção do Servidor de Administração será exibida.

2. Se tiver adicionado vários servidores confiáveis, selecione, na lista Servidores de Administração, o Servidor de Administração ao qual deseja se conectar.

   Caso apenas um Servidor de Administração tenha sido adicionado, a lista de Servidores de Administração não será exibida.

   O navegador será redirecionado para o endereço https://<Servidor de Administração>:4444.

3. Execute uma das seguintes ações:

   - Para fazer login no Servidor de Administração com uma conta de usuário do domínio, insira o nome de usuário e a senha do usuário.

     É possível inserir o nome de usuário do usuário do domínio em um dos seguintes formatos:

     - `Nome_de_usuário@dns.domain`
     - `NTDOMAIN\Nome_de_usuário`

     Antes de entrar com uma conta de usuário do domínio, faça a sondagem do controlador de domínio para obter a lista de usuários do domínio.

- Para fazer login no Servidor de Administração com o nome de usuário e a senha do administrador, insira o nome de usuário e a senha do usuário interno.
- Se um ou mais Servidores virtuais forem criados no Servidor e você quiser fazer login em um Servidor virtual:

  a. Clique em **Mostrar as opções do Servidor virtual**.

  b. Digite o nome do Servidor de Administração virtual que você especificou enquanto criava o servidor virtual.

  c. Digite o nome de usuário e a senha do administrador que tem direitos no Servidor de Administração virtual.

4. Clique no botão **Login**.
5. Especifique o código de segurança de uso único gerado pelo app autenticador no dispositivo móvel.

   No primeiro login, configure a autenticação em duas etapas para a sua conta. Se a configuração da autenticação de dois fatores não estiver disponível, entre em contato com um usuário que tenha o direito Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário** e tenha configurado a autenticação de dois fatores, a fim de adicionar sua conta à lista de permissão da autenticação de dois fatores.
6. Caso a alteração forçada de senha esteja ativada para sua conta ou sua senha tenha expirado, a janela de alteração de senha será exibida. Defina uma nova senha para fazer login no Kaspersky Security Center Web Console.

Após o login, a página inicial do Kaspersky Security Center Web Console será exibida, contendo o idioma e o tema usados pela última vez. Você pode navegar pelo Kaspersky Security Center Web Console e usá-lo para uso com o Kaspersky Security Center Linux.

Fazer logout

Para fazer o logout do Kaspersky Security Center Web Console,

No painel superior, vá para o menu da conta clicando no nome dela e selecione **Sair**.

O Kaspersky Security Center Web Console é fechado, e a página de login é exibida.

Interface do Kaspersky Security Center Web Console

O Kaspersky Security Center Linux é gerenciado por meio da interface do Kaspersky Security Center Web Console.

A janela do Kaspersky Security Center Web Console contém os seguintes itens:

- Menu principal na parte esquerda da janela
- Painel superior na parte superior da janela
- Área de trabalho na parte direita da janela

Menu principal

O menu principal contém as seguintes seções:

- **Servidor de Administração**. Exibe o nome do Servidor de Administração ao qual você está atualmente conectado. É possível abrir as propriedades do Servidor de Administração clicando no nome dele.
- **Navegação do console**. Exibe o mapa do menu principal. A maioria das seções exibidas pode ser adicionada aos marcadores ou definida como página inicial. Por padrão, os **Navegação do console** são definidos como a página inicial. É possível alterar essa configuração.
- **Monitoramento**. Fornecem uma visão geral da infraestrutura, dos status de proteção e das estatísticas.
- **Gerenciamento de ativos**. Contém ferramentas para gerenciamento de dispositivos e hardware e políticas de aplicativos da Kaspersky.
- **Tarefas**. Contém ferramentas para criar e executar tarefas.
- **Usuários e funções**. Permite gerenciar usuários e funções, configurar direitos de usuário atribuindo funções aos usuários e associar perfis de política com as funções.
- **Repositórios**. Fornece acesso aos repositórios de aplicativos.
- **Gerenciamento de software**. Permite gerenciar aplicativos da Kaspersky e de terceiros, bem como pacotes de instalação e patches.
- **Operações**. Contém uma variedade de operações, incluindo licenciamento de aplicativos, exibição e gerenciamento de dispositivos criptografados e eventos de criptografia.
- **Descoberta e implementação**. Permite fazer a sondagem da rede para descobrir dispositivos cliente e distribuir os dispositivos para grupos de administração manual ou automaticamente. Esta seção também contém o assistente de início rápido e o assistente de implementação da proteção.
- **Marketplace**. Contém informações sobre toda a variedade de soluções empresariais da Kaspersky e permite selecionar as que você precisa e, em seguida, prosseguir com a compra dessas soluções no site da Kaspersky.
- **Configurações**. Permite fazer backup do estado atual de um plug-in da web para poder restaurar o estado salvo posteriormente. Contém suas configurações pessoais relacionadas à aparência da interface, como idioma da interface ou tema.

Se necessário, você pode minimizar o menu principal para ícones clicando no símbolo de chevron (<<) na parte inferior da tela.

Painel superior

O painel superior sempre é exibido em todas as seções do console e não pode ser ocultado.

O lado esquerdo do painel contém o nome e o logotipo do aplicativo. Se você clicar no nome ou no logotipo do aplicativo, a página inicial do Kaspersky Security Center Web Console será aberta.

No lado direito do painel, as seguintes configurações são exibidas:

- Ícone de notificação (🔔). Se você clicar no ícone, um painel com notificações será aberto.
- O menu da sua conta. Contém um link para a Ajuda do Kaspersky Security Center Linux. Ele também permite que você saia do Kaspersky Security Center Linux, altere a senha da sua conta e visualize a versão do Kaspersky Security Center Web Console e a lista de plug-ins da Web de gerenciamento instalados.

Área de trabalho

A área de trabalho exibe as informações que você escolhe visualizar nas seções da janela da interface do Kaspersky Security Center Web Console. Ela também contém elementos de controle que podem ser usados para configurar como as informações são exibidas.

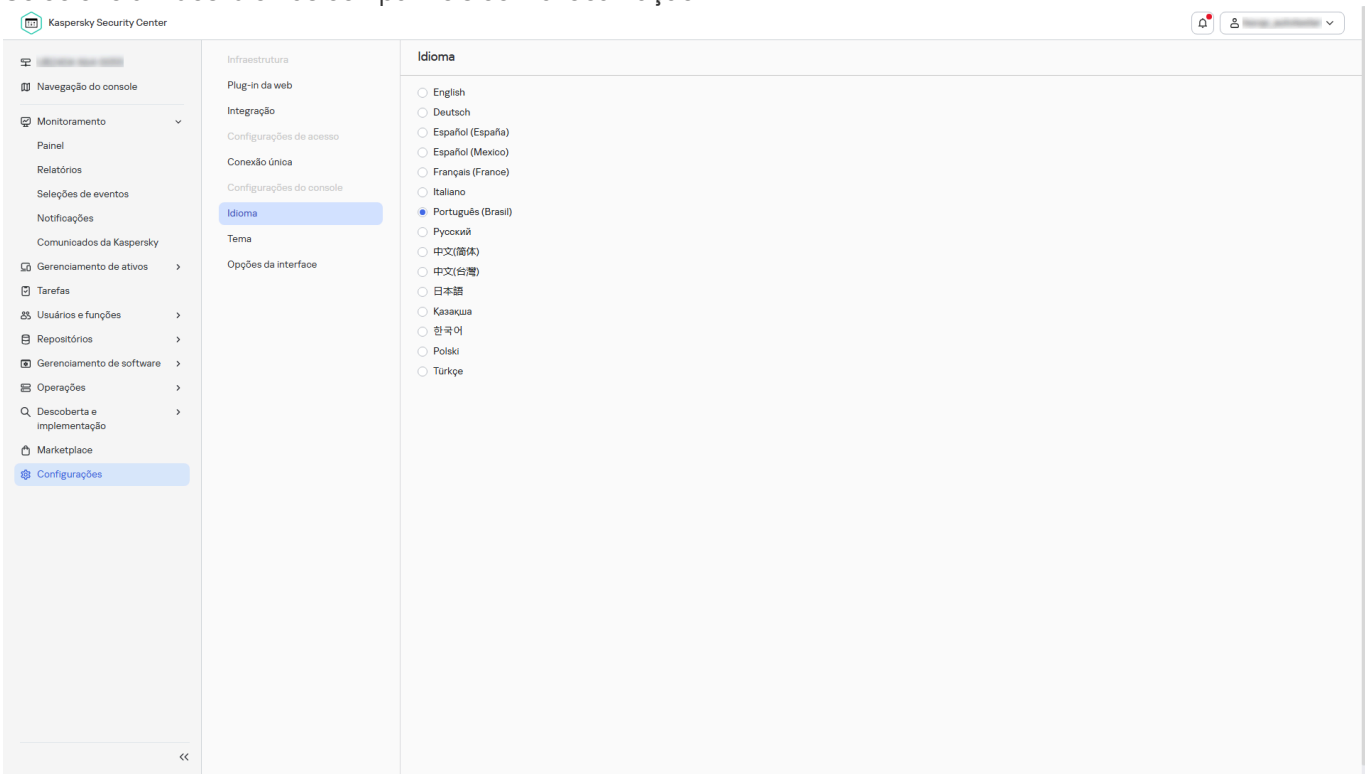
> Recomendamos usar uma única guia do navegador para uso com o Kaspersky Security Center Web Console.

Alteração do idioma da interface do Kaspersky Security Center Web Console

É possível selecionar o idioma da interface do Kaspersky Security Center Web Console.

Para alterar o idioma da interface:

1. No menu principal, vá para **Configurações** → **Idioma**.
2. Selecione um dos idiomas compatíveis com a localização.



Alteração do idioma da interface do Kaspersky Security Center Web Console

Alteração da página inicial do Kaspersky Security Center Web Console

A página inicial é exibida depois de realizar login no Kaspersky Security Center Web Console.

Por padrão, a **seção** **Navegação do console** é definida como a página inicial. Se necessário, você pode alterá-la.

Para alterar a página inicial:

1. Na seção **Navegação do console**, passe o cursor do mouse sobre o item que você deseja definir como página inicial.
2. Depois de o ícone de página inicial (⌂) aparecer, clique nele.

   A página inicial é alterada. Uma mensagem correspondente é exibida na tela. O item selecionado como página inicial é marcado com o ícone de casa (⌂).

> As seções **Marketplace** e **Configurações** não podem ser definidas como página inicial.

Adicionar e remover favoritos

Você pode adicionar seções frequentemente usadas do Kaspersky Security Center Web Console aos favoritos para acessá-las rapidamente na seção **Favoritos** no menu principal.

> A seção **Favoritos** não aparecerá no menu principal se você não adicionar nenhuma seção a ela.

Será possível adicionar aos favoritos apenas seções que exibam páginas. Por exemplo, ao acessar **Gerenciamento de ativos** → **Dispositivos gerenciados**, uma página com a tabela de dispositivos é aberta, o que significa que é possível adicionar esta seção aos favoritos. Se nenhuma janela ou elemento for exibido após selecionar a seção no menu principal, não será possível adicionar essa seção aos favoritos.

Para adicionar uma seção aos favoritos:

1. No menu principal, passe o cursor do mouse sobre a seção que deseja fixar.
2. Depois de o ícone de favorito (🔖) aparecer, clique nele.

   A seção é exibida em **Favoritos**.

Para remover uma seção dos favoritos:

1. No menu principal, acesse a seção **Favoritos**.
2. Passe o cursor do mouse sobre a seção que deseja remover e clique no ícone de favorito (🔖).

   A seção será removida dos favoritos.

Também é possível adicionar e remover elementos dos favoritos na seção **Navegação do console**, passando o cursor do mouse sobre eles e clicando no ícone (🔖) de Favoritos. O item selecionado será marcado com o ícone (🔖) de favorito e exibido na seção **Favoritos** no menu principal. Se quiser remover o item dos favoritos, clique no ícone (🔖) de favorito.

A seção **Favoritos** só aparece no menu principal. Ela nunca aparece na página **Navegação do console**.

Remoção do Kaspersky Security Center Web Console.

Pode ser necessário remover o Kaspersky Security Center Web Console Server (também conhecido como Kaspersky Security Center Web Console) nos seguintes casos:

- Restaurar dados de um backup com outro certificado comum.
- Reemitir o certificado comum do Servidor de Administração.
- Substituir o certificado do Web Console pelo certificado personalizado.
- O Kaspersky Security Center Web Console não é mais usado em um dispositivo.

Para instalar o Kaspersky Security Center Web Console:

1. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:
   - `sudo dnf remove ksc-web-console`
   - `sudo apt remove ksc-web-console`
2. Verifique o resultado executando o seguinte comando:

   `sudo systemctl status KSC*`

   O Kaspersky Security Center Web Console deve estar ausente na saída do comando.

Se você quiser restaurar o Kaspersky Security Center Web Console, instale-o no dispositivo conforme descrito no artigo: Instalar o Kaspersky Security Center Web Console.

Assistente de início rápido

O Kaspersky Security Center Linux lhe permite ajustar uma seleção mínima de configurações necessárias para criar um sistema de gerenciamento centralizado para proteger a rede contra ameaças à segurança. Esta configuração é executada por meio do Assistente de início rápido. Quando o assistente estiver em execução, você pode fazer as seguintes modificações ao aplicativo:

- Adicione arquivos de chaves ou insira códigos de ativação que podem ser distribuídas automaticamente para os dispositivos dentro de grupos de administração.
- Configure a entrega por e-mail de notificações de eventos ocorridos durante a operação do Servidor de Administração e dos aplicativos gerenciados.

- Crie uma política de proteção para estações de trabalho e servidores, assim como tarefas de verificação de malwares, tarefas de download de atualização e tarefas de backup dos dados, para o nível superior da hierarquia de dispositivos gerenciados.

  O Assistente de início rápido cria políticas somente para aplicativos para os quais a pasta **Dispositivos gerenciados** não contém nenhuma política. O Assistente de início rápido não cria tarefas se algumas já tiverem sido criadas com os mesmos nomes para o nível superior da hierarquia dos dispositivos gerenciados.

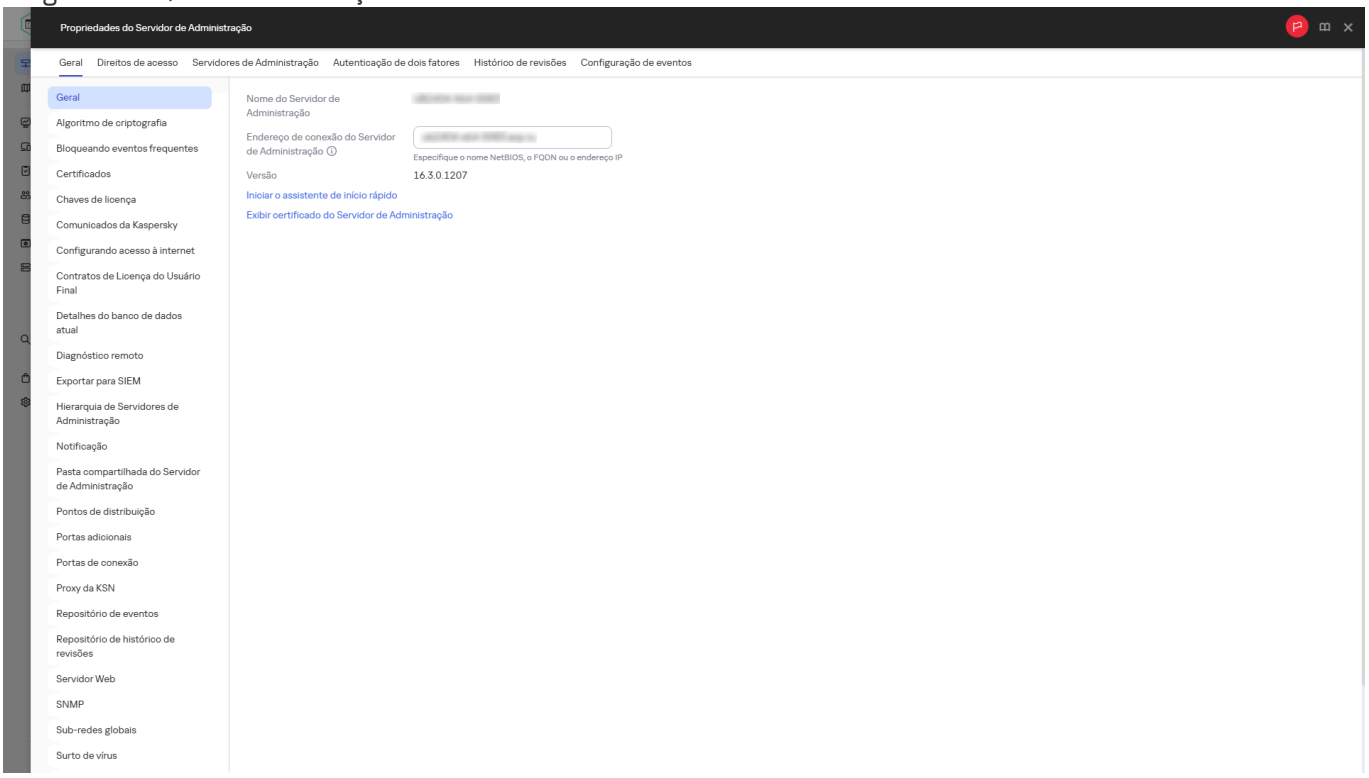
O aplicativo solicita automaticamente que você execute o Assistente de início rápido após a instalação do Servidor de Administração, na primeira conexão a ele. Você também pode iniciar o Assistente de início rápido manualmente a qualquer momento.

Para iniciar o Assistente de Início Rápido manualmente:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Geral**.



Janela de propriedades do Servidor de Administração

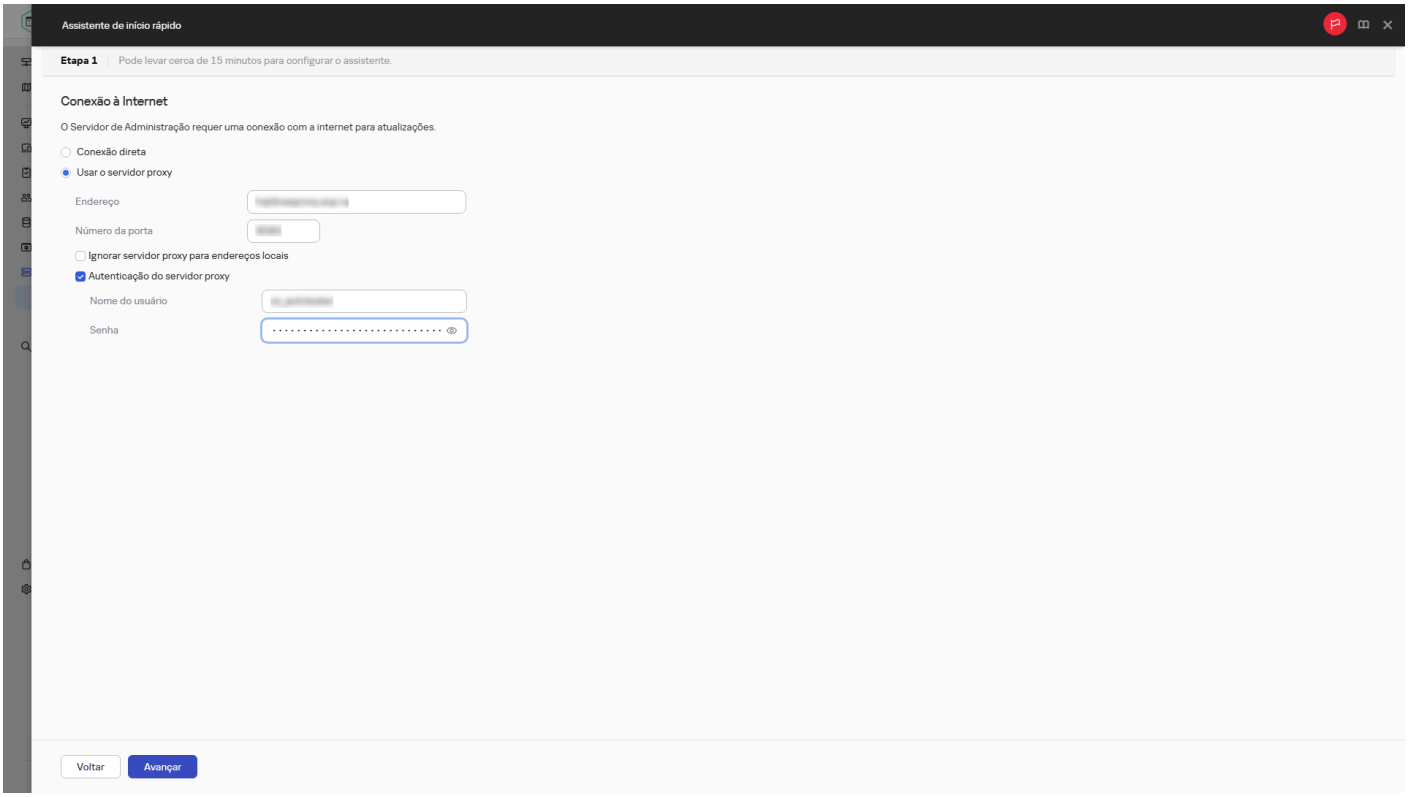
3. Clique em **Iniciar o assistente de início rápido**.

   O assistente solicita que você execute a configuração inicial do Servidor de Administração. Siga as etapas do Assistente. Prossiga pelo assistente usando o botão **Avançar**.

Etapa 1. Especificando as configurações de conexão da Internet

Especifique as configurações de acesso à Internet para o Servidor de Administração. É preciso configurar o acesso à Internet para usar a Kaspersky Security Network e baixar atualizações de bancos de dados de antivírus para o Kaspersky Security Center Linux e aplicativos Kaspersky gerenciados.

Ative a opção **Usar o servidor proxy** caso queira usar um servidor proxy para se conectar com a Internet. Caso essa opção esteja ativada, os campos estarão disponíveis para inserir as configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:



Internet connection settings

- **Endereço**

  Endereço do servidor proxy usado para conexão do Kaspersky Security Center Linux à Internet.

- **Número da porta**

  Número da porta pela qual a conexão proxy do Kaspersky Security Center Linux será estabelecida.

- **Ignorar servidor proxy para endereços locais**

  Nenhum servidor proxy será usado para conectar-se aos dispositivos na rede local.

- **Autenticação do servidor proxy**

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

  Este campo de entrada está disponível se a caixa de seleção **Usar o servidor proxy** estiver marcada.

- **Nome do usuário**

  Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

- **Senha**

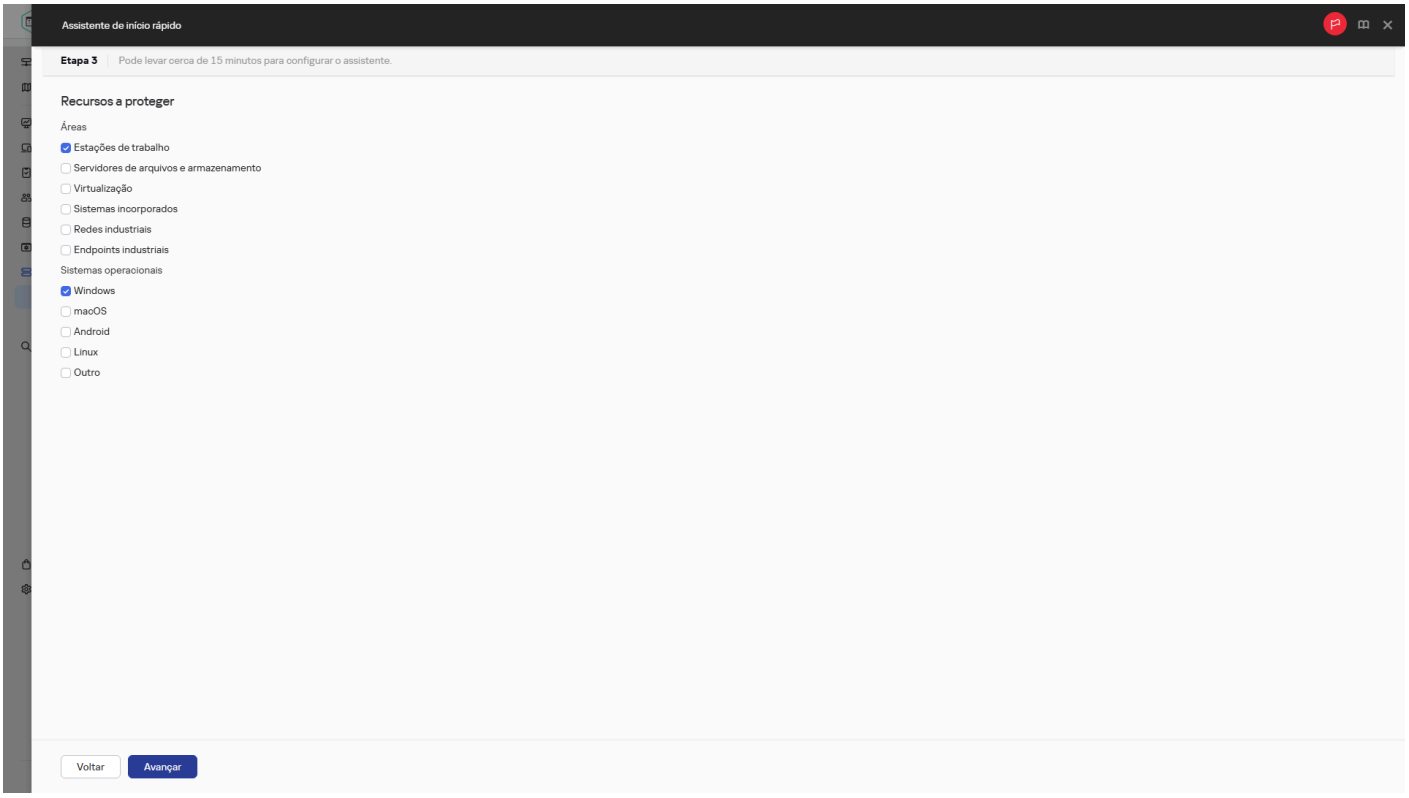
  A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

  Para ver a senha inserida, mantenha pressionado o botão **Mostrar** pelo tempo que você desejar.

É possível configurar o acesso à Internet posteriormente, de modo separado, a partir do assistente de início rápido.

Etapa 2. Download das atualizações necessárias

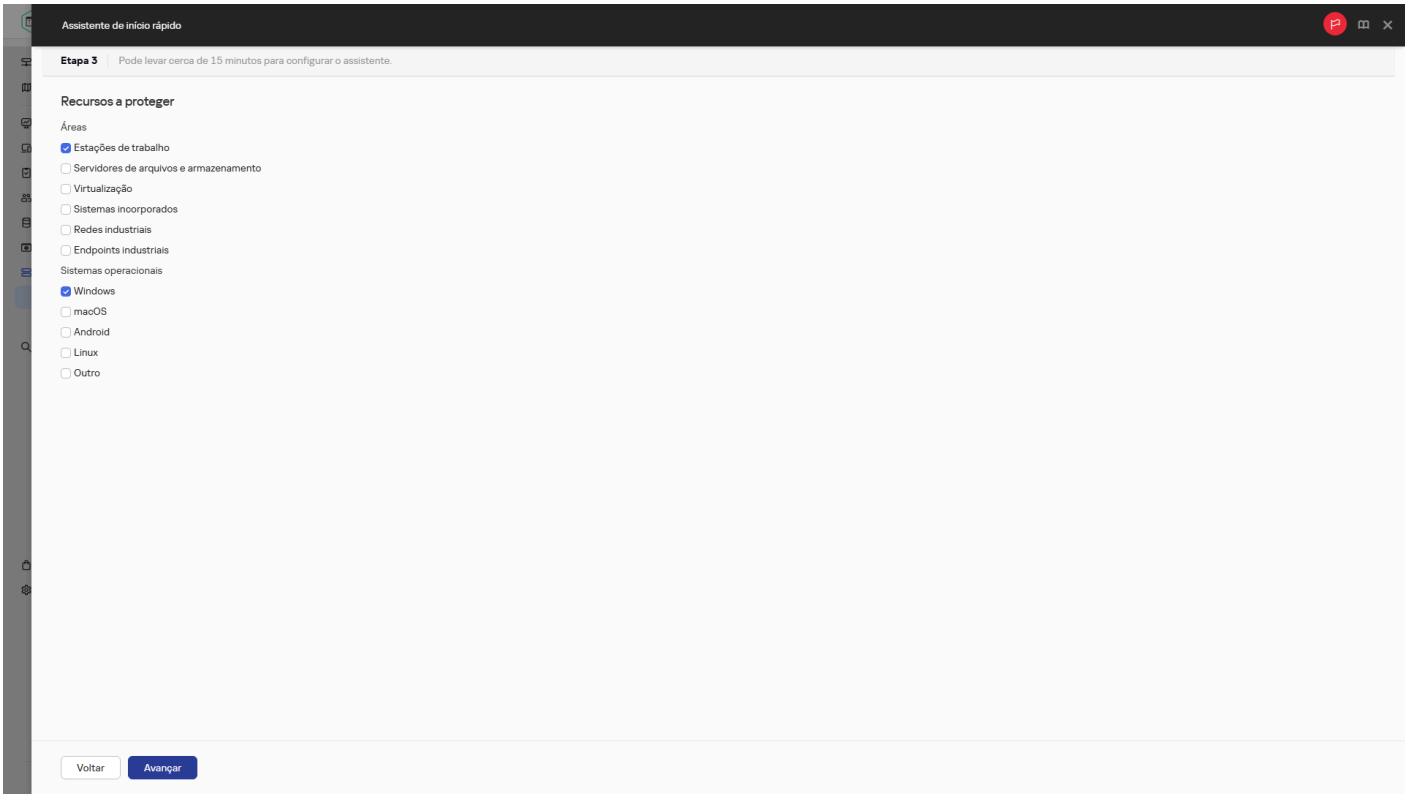
As atualizações necessárias são baixadas dos servidores da Kaspersky automaticamente.



Download das atualizações necessárias

Etapa 3. Seleção dos ativos a serem protegidos

Selecione as áreas de proteção e os sistemas operacionais que estão em uso na sua rede. Ao selecionar essas opções, você especifica os filtros para plugins de gerenciamento de aplicativos e pacotes de distribuição nos servidores da Kaspersky que podem ser baixados para instalação nos dispositivos clientes em sua rede.



Seleção dos ativos a serem protegidos

Selecione as opções:

- **Áreas**

  Você pode selecionar os seguintes escopos de proteção:

  - **Estações de trabalho**
  - **Servidores de arquivos e armazenamento**
  - **Virtualização**
  - **Sistemas incorporados**
  - **Redes industriais**
  - **Endpoints industriais**

- **Sistemas operacionais**

  Você pode selecionar as seguintes plataformas:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Outro

  Para obter informações sobre os sistemas operacionais compatíveis, consulte os requisitos de hardware e software para o Kaspersky Security Center Web Console.

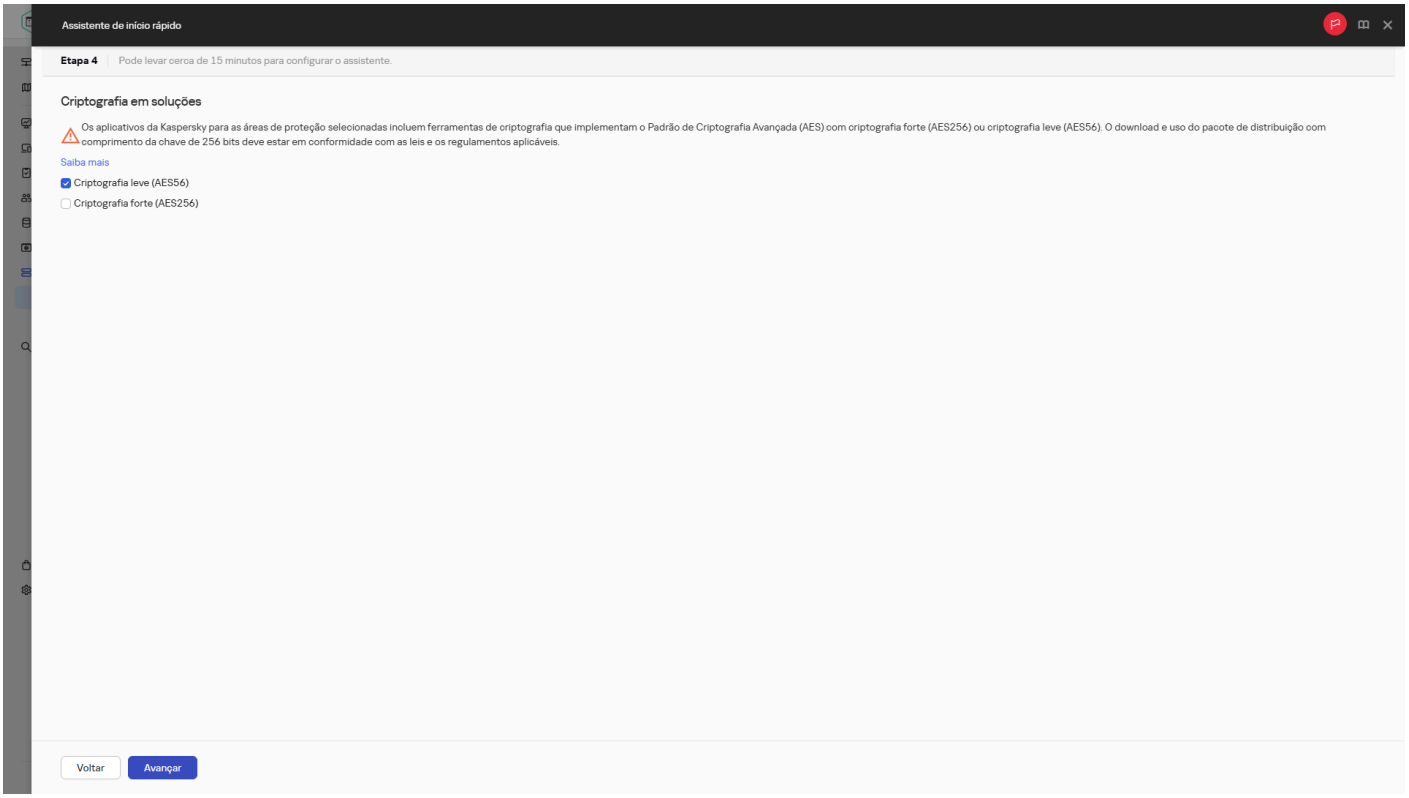
Você pode selecionar os pacotes de aplicativos Kaspersky na lista de pacotes disponíveis posteriormente, separadamente do Assistente de início rápido. Para simplificar a busca pelos pacotes necessários, é possível filtrar a lista de pacotes disponíveis por diversos critérios.

Etapa 4. Selecionar a criptografia em soluções

A janela **Criptografia em soluções** é exibida apenas se você tiver selecionado **Estações de trabalho** como escopo de proteção.

O Kaspersky Endpoint Security for Windows inclui ferramentas de criptografia para as informações armazenadas nos dispositivos cliente baseados em Windows. Essas ferramentas de criptografia têm Advanced Encryption Standard (AES) implementado com comprimento de chave de 256 ou 56 bits.

O download e o uso do pacote de distribuição com um comprimento de chave de 256 bits devem ser executados em conformidade com as leis e regulamentos aplicáveis. Para baixar um pacote de distribuição do Kaspersky Endpoint Security for Windows que seja válido para as necessidades da sua organização, consulte a legislação do país em que os dispositivos clientes da sua organização estejam localizados.



Selecionar a criptografia em soluções

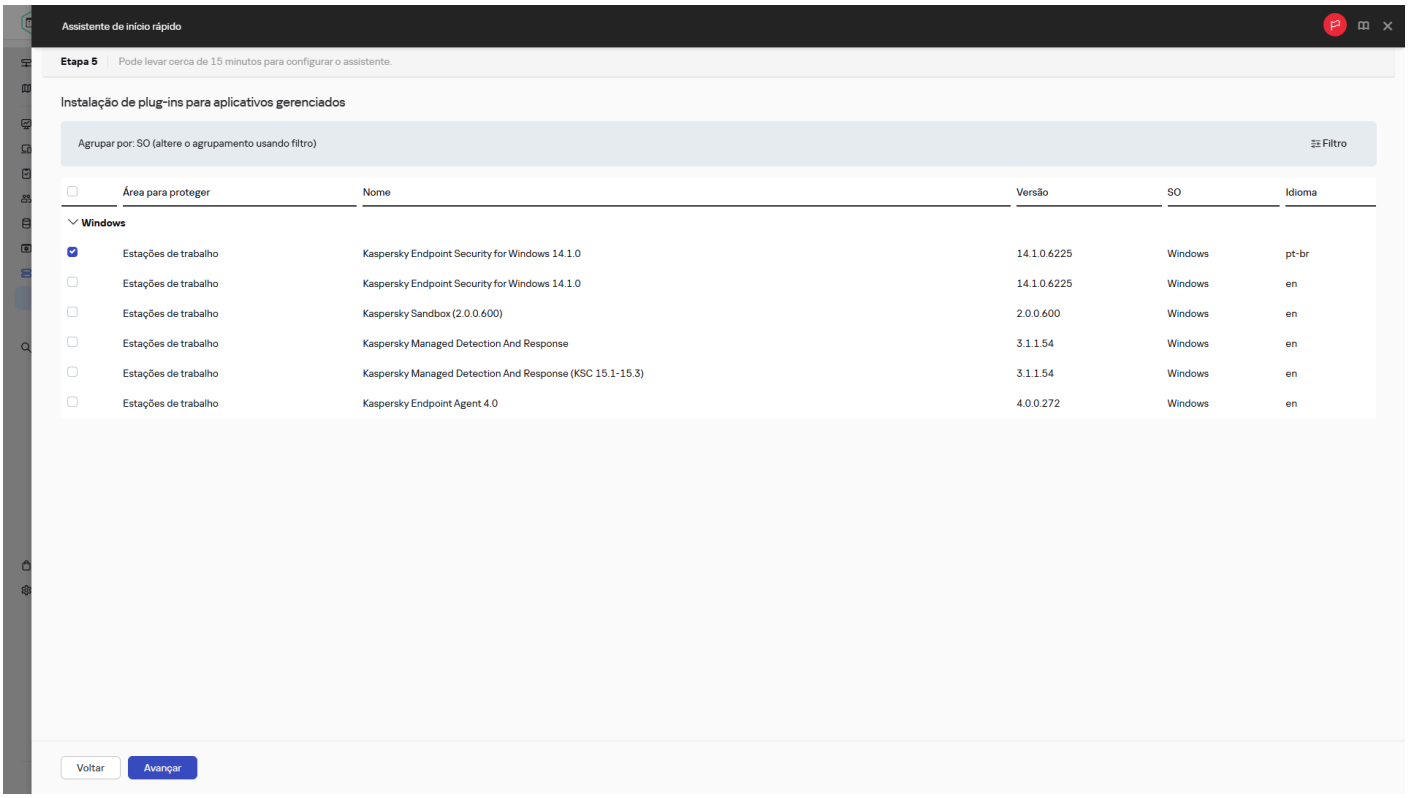
Na janela **Criptografia em soluções**, selecione um dos seguintes tipos de criptografia:

- Criptografia leve. Esse tipo de criptografia usa um comprimento de chave de 56 bits.
- Criptografia forte. Esse tipo de criptografia usa um comprimento de chave de 256 bits.

É possível selecionar posteriormente o pacote de distribuição para o Kaspersky Endpoint Security for Windows com o tipo de criptografia necessário, de modo separado, a partir do assistente de início rápido.

Etapa 5. Configurar a instalação dos plugins para os aplicativos gerenciados

Selecione os plugins para os aplicativos gerenciados a ser instalados. Uma lista de plugins localizados nos servidores da Kaspersky é exibida. A lista é filtrada de acordo com as opções selecionadas na etapa anterior do assistente. Por padrão, uma lista completa inclui plugins de todos os idiomas. Para exibir apenas o plugin de um idioma específico, use o filtro.



Instalação dos plugins para os aplicativos gerenciados

A lista de plugins inclui as seguintes colunas:

- **Área para proteger**

  As áreas selecionadas para receber proteção são exibidas nesta coluna.

- **Tipo**

  Os tipos de plug-in são exibidos nesta coluna.

- **Nome**

  Os plugins, dependendo das áreas de proteção e das plataformas que você selecionou na etapa anterior, são selecionados.

- **Versão**

  A lista inclui plugins de todas as versões colocadas nos servidores da Kaspersky. Por padrão, os plugins das versões mais recentes são selecionados.

- **Versão mais recente**

  Esta coluna indica se uma versão do plug-in é a mais recente. Caso o valor **true** seja exibido, o plug-in corresponde à versão mais recente. Se o valor **false** for exibido, o plug-in corresponde a uma versão posterior.

- **SO**

  Essa coluna exibe os sistemas operacionais dos plug-ins.

- **Idioma**

  Por padrão, o idioma de localização de um plug-in é definido pelo idioma do Kaspersky Security Center Linux selecionado na instalação. Você pode especificar outros idiomas na lista suspensa **Mostrar o idioma localizado do Console de Administração ou**.

Após os plugins serem selecionados, clique em **Avançar** para iniciar a instalação.

É possível instalar os plug-ins de gerenciamento para aplicativos da Kaspersky manualmente, de modo separado do assistente de início rápido.

O assistente de início rápido instala automaticamente os plug-ins selecionados. Para instalar alguns plugins, você deve aceitar os termos do EULA. Leia o texto do EULA exibido, selecione, a caixa de seleção **Concordo em participar da Kaspersky Security Network** e clique no botão **Instalar**. Se você não aceitar os termos do EULA, o plugin não será instalado.

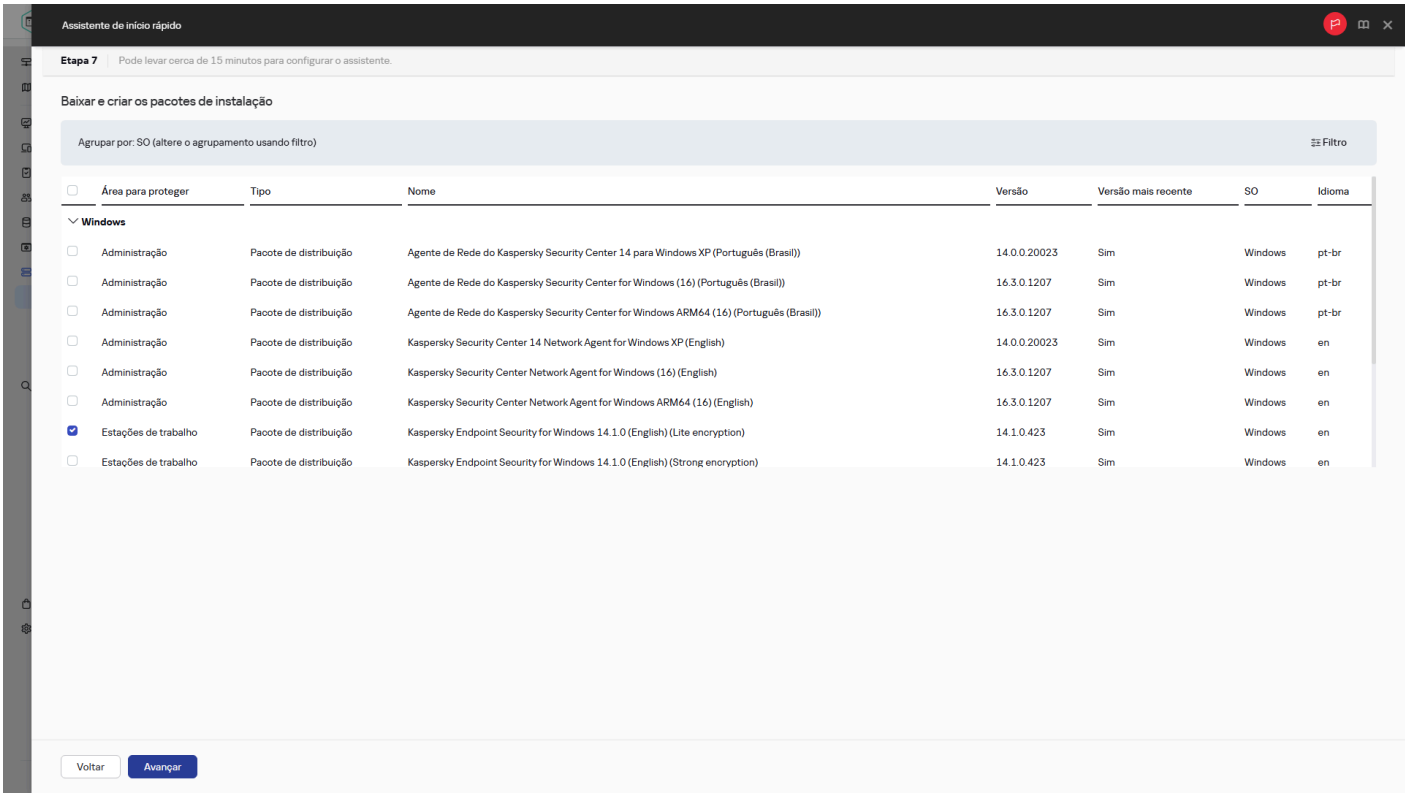
Quando todos os plugins selecionados estiverem instalados, o Assistente de início rápido direcionará você automaticamente para a próxima etapa.

Etapa 6. Baixando os pacote de distribuição e criando pacotes de instalação

Selecione os pacotes de distribuição para baixar.

As distribuições de aplicativos gerenciados podem exigir a instalação de uma versão mínima específica do Kaspersky Security Center Linux.

Após selecionar um tipo de criptografia para o Kaspersky Endpoint Security for Windows, a lista dos pacotes de distribuição dos dois tipos de criptografia é exibida. Um pacote de distribuição com o tipo de criptografia selecionado está selecionado na lista. Você pode selecionar pacotes de distribuição de qualquer tipo de criptografia. O idioma do pacote de distribuição corresponde ao idioma do Kaspersky Security Center Linux. Caso não exista um pacote de distribuição de aplicativos no idioma do Kaspersky Security Center Linux, o pacote de distribuição em inglês será selecionado.



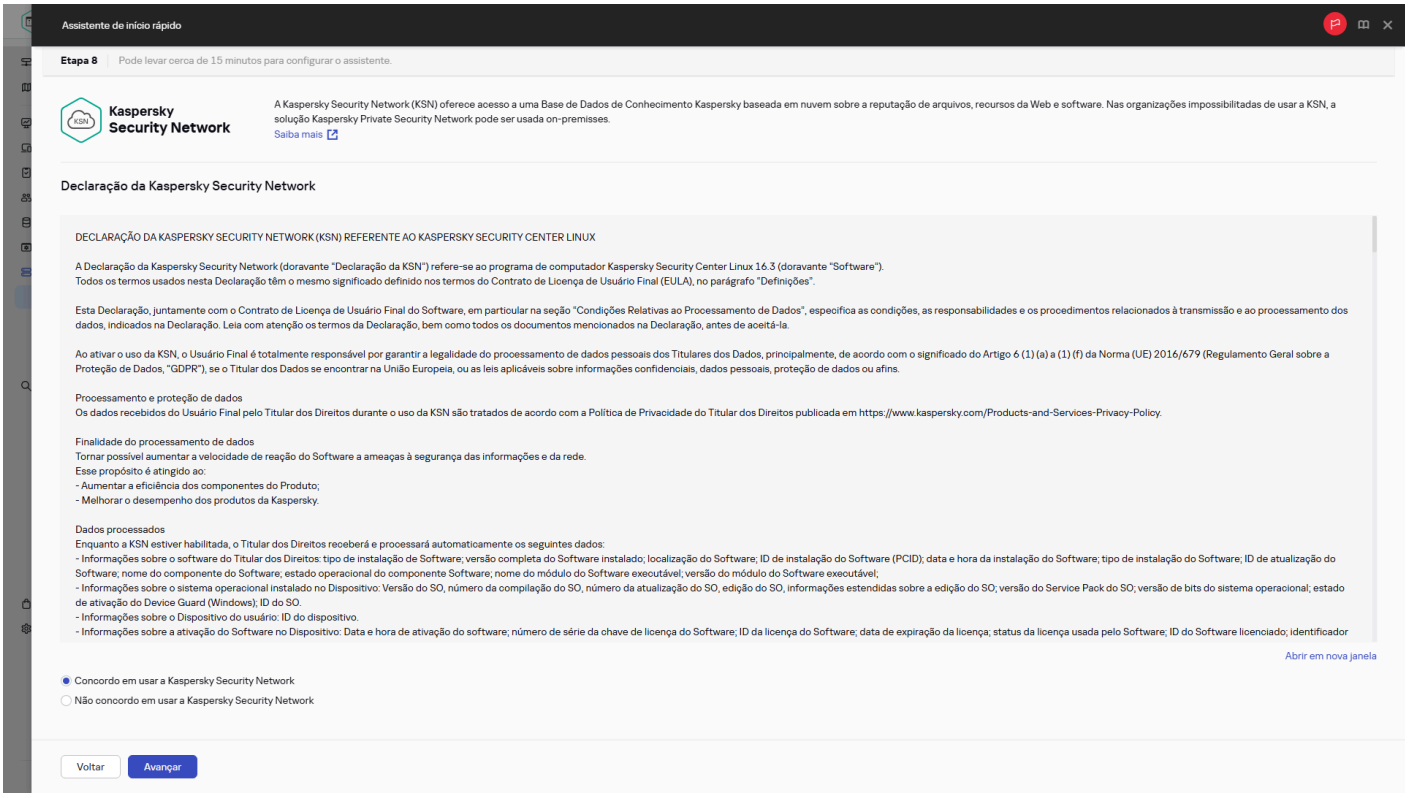
Baixando os pacote de distribuição e criando pacotes de instalação

Para concluir o download de alguns pacotes de distribuição, você deve aceitar o EULA. Quando você clica no botão **Aceitar**, o texto do EULA é exibido. Para prosseguir para a próxima etapa do assistente, você deve aceitar os termos e condições do EULA e os termos e condições da Política de Privacidade da Kaspersky. Se você não aceitar os termos e condições, o download do pacote será cancelado.

Após aceitar os termos e condições do EULA e os termos e condições da Política de Privacidade da Kaspersky, o download dos pacotes de distribuição continua. Posteriormente, você pode suar os pacotes de instalação para implementar aplicativos Kaspersky em dispositivos cliente.

Etapa 7. Configurar a Kaspersky Security Network

Especifique as configurações para encaminhar informações sobre as operações do Kaspersky Security Center Linux à Base de Dados de Conhecimento da Kaspersky Security Network.



Configurar a Kaspersky Security Network

Escolha uma das seguintes opções:

- **Concordo em participar da Kaspersky Security Network**

  O Kaspersky Security Center Linux e os aplicativos gerenciados instalados nos dispositivos clientes transferem automaticamente os detalhes de operação para a Kaspersky Security Network. A participação na Kaspersky Security Network assegura atualizações mais rápidas dos bancos de dados que contêm informações sobre vírus e outras ameaças, que assegura uma resposta mais rápida a ameaças de segurança emergentes.

- **Não concordo em participar da Kaspersky Security Network**

  O Kaspersky Security Center Linux e os aplicativos gerenciados não fornecerão informações à Kaspersky Security Network.

  Se você selecionar esta opção, o uso da Kaspersky Security Network será desativado.

É possível configurar o acesso a Kaspersky Security Network (KSN) posteriormente, de modo separado, a partir do assistente de início rápido.

Etapa 8. Selecionando o método de ativação do aplicativo

Selecione uma das seguintes opções de ativação do Kaspersky Security Center Linux:

- **Inserindo o seu código de ativação**

  Um *código de ativação* é uma sequência única de vinte letras latinas e números. Você insere um código de ativação para adicionar uma chave que ativa o Kaspersky Security Center Linux. Você recebe o código de ativação através do endereço de e-mail especificado após a compra do Kaspersky Security Center.

  Para ativar o aplicativo com um código de ativação, é necessário acesso à Internet para se conectar aos servidores de ativação da Kaspersky.

  Se você selecionou essa opção de ativação, pode ativar a opção **Automaticamente implementar chave de licença nos dispositivos gerenciados**.

  Se esta opção estiver ativada, a chave de licença será implementada automaticamente para os dispositivos gerenciados.

  Se esta opção estiver desativada, você poderá implantar a chave de licença em dispositivos gerenciados posteriormente na seção **Operações → Licenciamento → Licenças** do menu principal.

- **Especificando um arquivo de chave**

  O *Arquivo de chave* é um arquivo com a extensão .key fornecido a você pela Kaspersky. O objetivo do arquivo de chave é adicionar uma chave que ativa o aplicativo.

  Você recebe o arquivo de chave via endereço de e-mail especificado após a compra do Kaspersky Security Center.

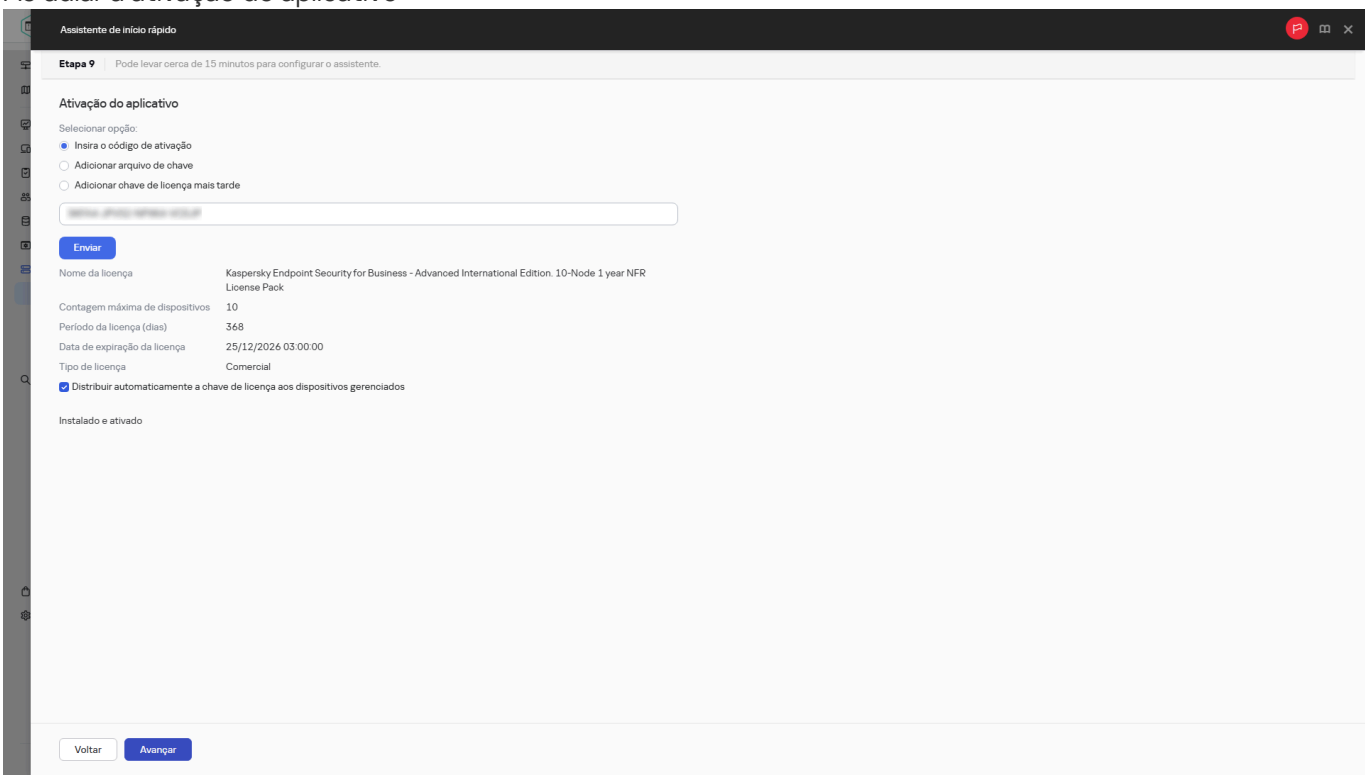
  Você não precisa se conectar aos servidores de ativação da Kaspersky para ativar o aplicativo com um arquivo de chave.

  Se você selecionou essa opção de ativação, pode ativar a opção **Automaticamente implementar chave de licença nos dispositivos gerenciados**.

  Se esta opção estiver ativada, a chave de licença será implementada automaticamente para os dispositivos gerenciados.

  Se esta opção estiver desativada, você poderá implantar a chave de licença em dispositivos gerenciados posteriormente na seção **Operações → Licenciamento → Licenças** do menu principal.

- Ao adiar a ativação do aplicativo



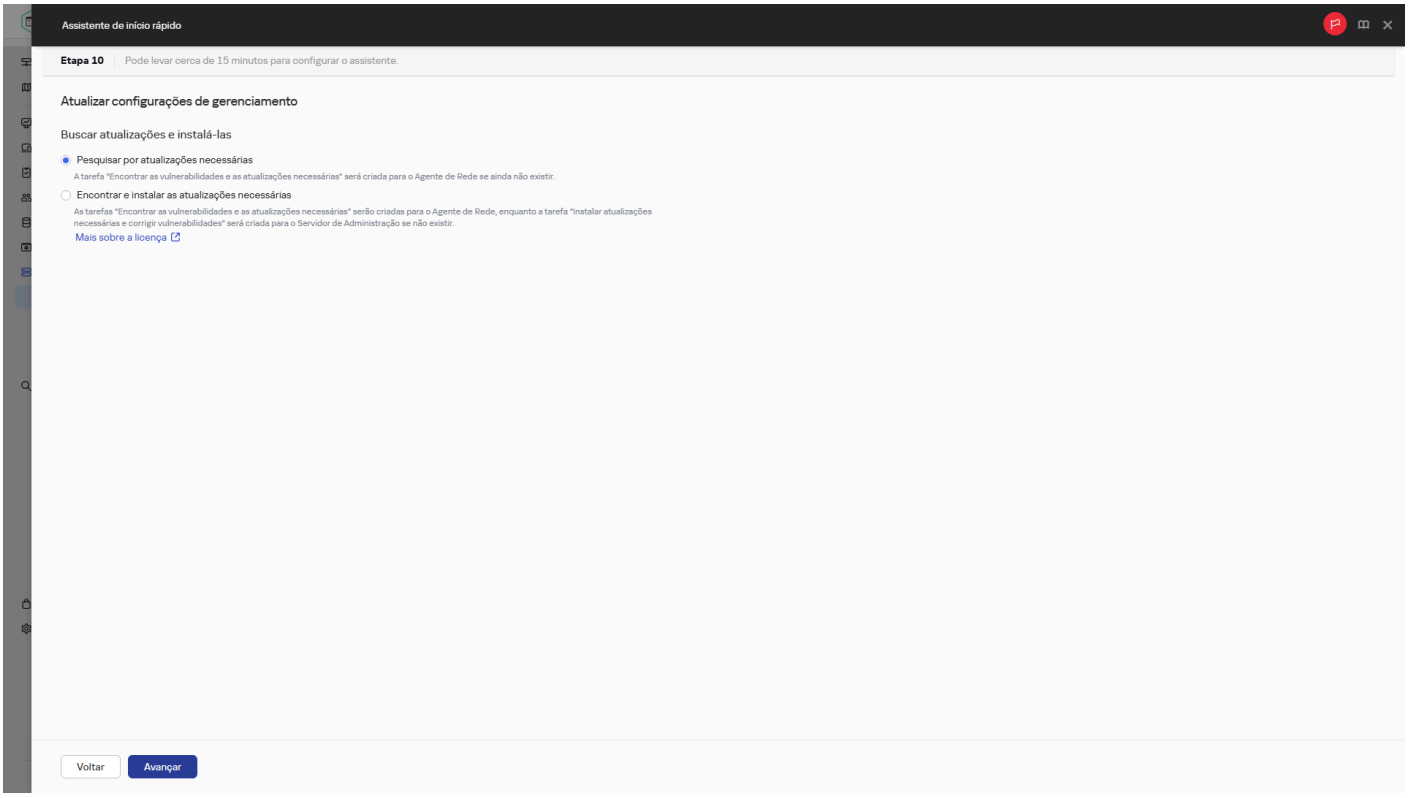
Selecionando o método de ativação do aplicativo

Se você decidiu adiar a ativação do aplicativo, poderá adicionar uma chave de licença depois a qualquer momento selecionando **Operações** → **Licenciamento**.

Ao trabalhar com o Kaspersky Security Center implementado a partir de uma AMI paga ou uma SKU com base no uso e faturamento mensal, você não pode especificar um arquivo de chave ou inserir um código.

Etapa 9. Especificar as configurações de gerenciamento de atualização de terceiros

A etapa **Atualizar configurações de gerenciamento** do assistente de início rápido não será exibida se você não tiver a licença de Gerenciamento de patches e vulnerabilidades e se a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* já existir.



Configurações de gerenciamento de atualização de terceiros

Para atualizações de software de terceiros, selecione uma das seguintes opções:

- **Pesquisar por atualizações necessárias**

  A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente, caso você não tenha uma.

  Esta opção está marcada por padrão.

- **Encontrar e instalar as atualizações necessárias**

  As tarefas *Encontrar as vulnerabilidades e as atualizações necessárias* e *Instalar as atualizações necessárias e corrigir vulnerabilidades* são criadas automaticamente, se ainda não existirem.

  Esta opção está disponível apenas sob a licença de Gerenciamento de patches e vulnerabilidades.

Para atualizações do Windows Update, selecione **Usar as origens de atualização definidas na política do domínio.**

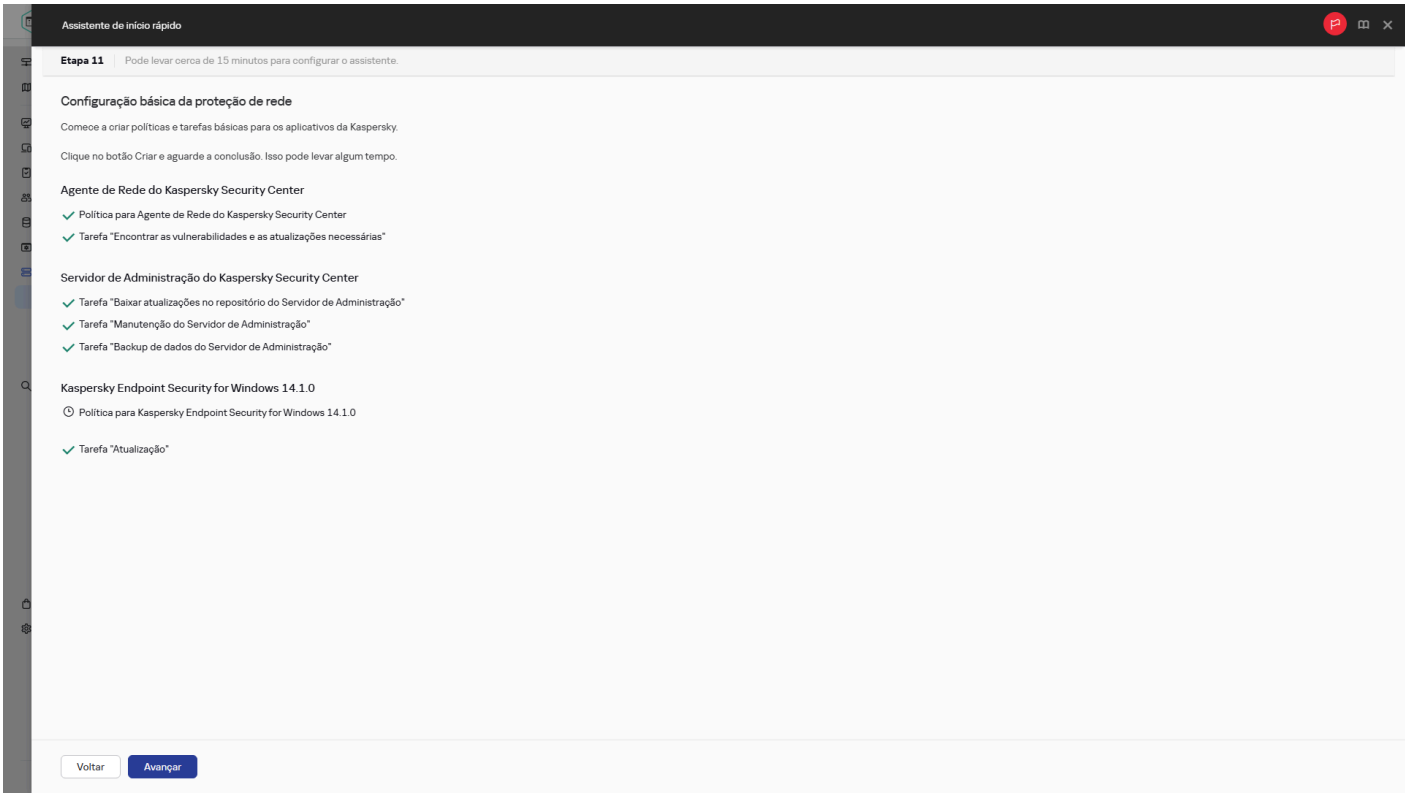
Os dispositivos clientes baixarão as atualizações do Windows Update, de acordo com as configurações de diretiva de domínio. A política do Agente de Rede é criada automaticamente, se você não tiver uma.

É possível criar as tarefas *Encontrar as vulnerabilidades e as atualizações necessárias* e *Instalar as atualizações necessárias e corrigir vulnerabilidades* separadamente do assistente de início rápido.

Etapa 10. Criar uma configuração básica de proteção de rede

Você poderá verificar a lista de políticas e tarefas que foram criadas.

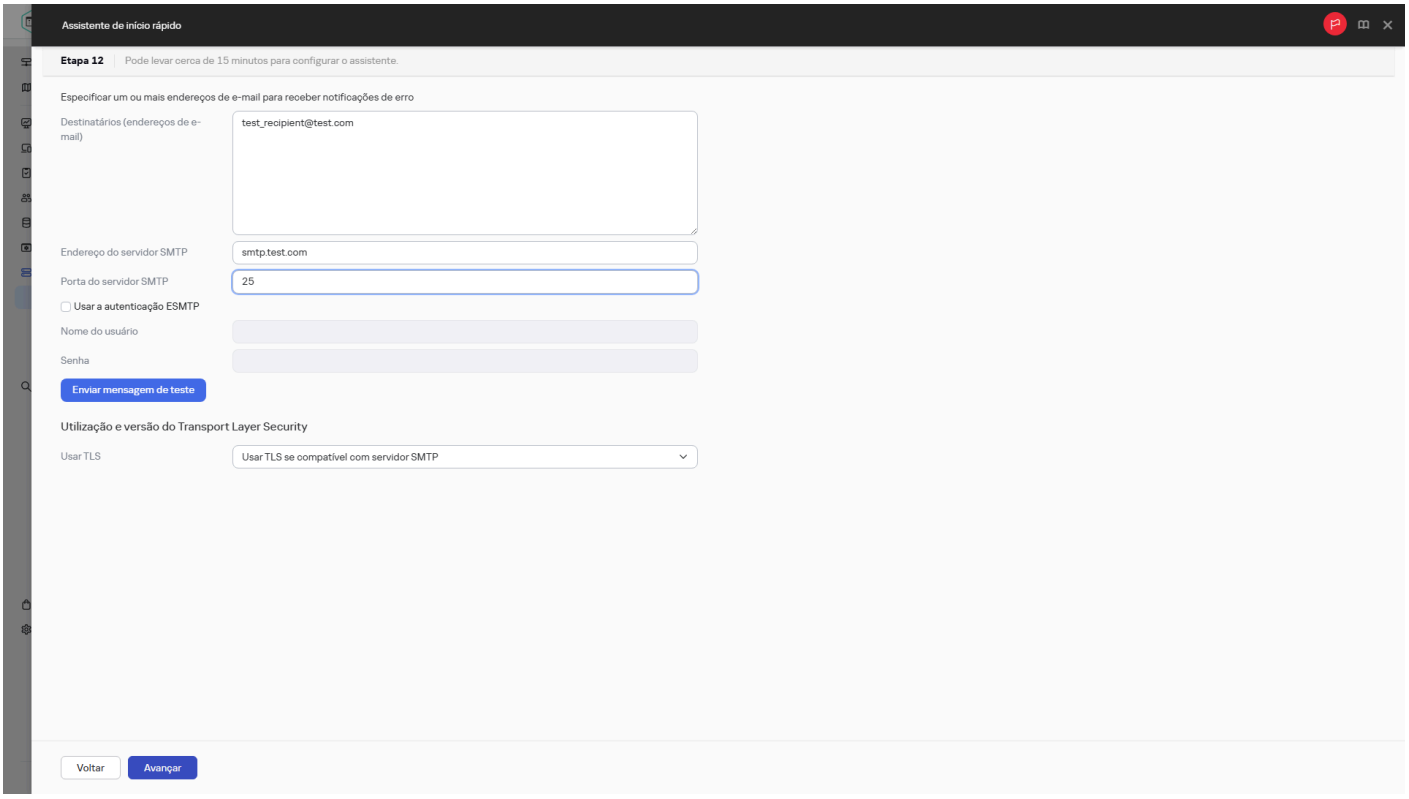
Espere pela conclusão da criação de políticas e tarefas antes de prosseguir à etapa seguinte do assistente.



Criar uma configuração básica de proteção de rede

Etapa 11. Configurar notificações por e-mail

Configure a entrega de notificações sobre os eventos registrados durante a operação dos aplicativos Kaspersky em dispositivos clientes. Essas configurações serão usadas como as configurações padrão para as políticas de aplicativo.



Configurar notificações por e-mail

Para configurar a entrega de notificações sobre os eventos que ocorrem nos aplicativos Kaspersky, use as seguintes configurações:

- **Destinatários (endereços de e-mail)**

  Os endereços de e-mail de usuários aos quais o aplicativo enviará notificações. Você pode especificar um ou mais endereços. Se você inserir mais de um endereço, separe-os com um ponto-e-vírgula.

- **Endereço do servidor SMTP**

  O endereço ou os endereços dos servidores de e-mail da sua organização.

  Se você inserir mais de um endereço, separe-os com um ponto-e-vírgula. Você pode usar os seguintes parâmetros:

  - Endereço IPv4 ou IPv6
  - Nome de DNS do servidor SMTP

- **Porta do servidor SMTP**

  Número da porta de comunicação do servidor SMTP. Se você usar vários servidores SMTP, a conexão com eles será estabelecida por meio da porta de comunicação especificada. O número da porta padrão é 25.

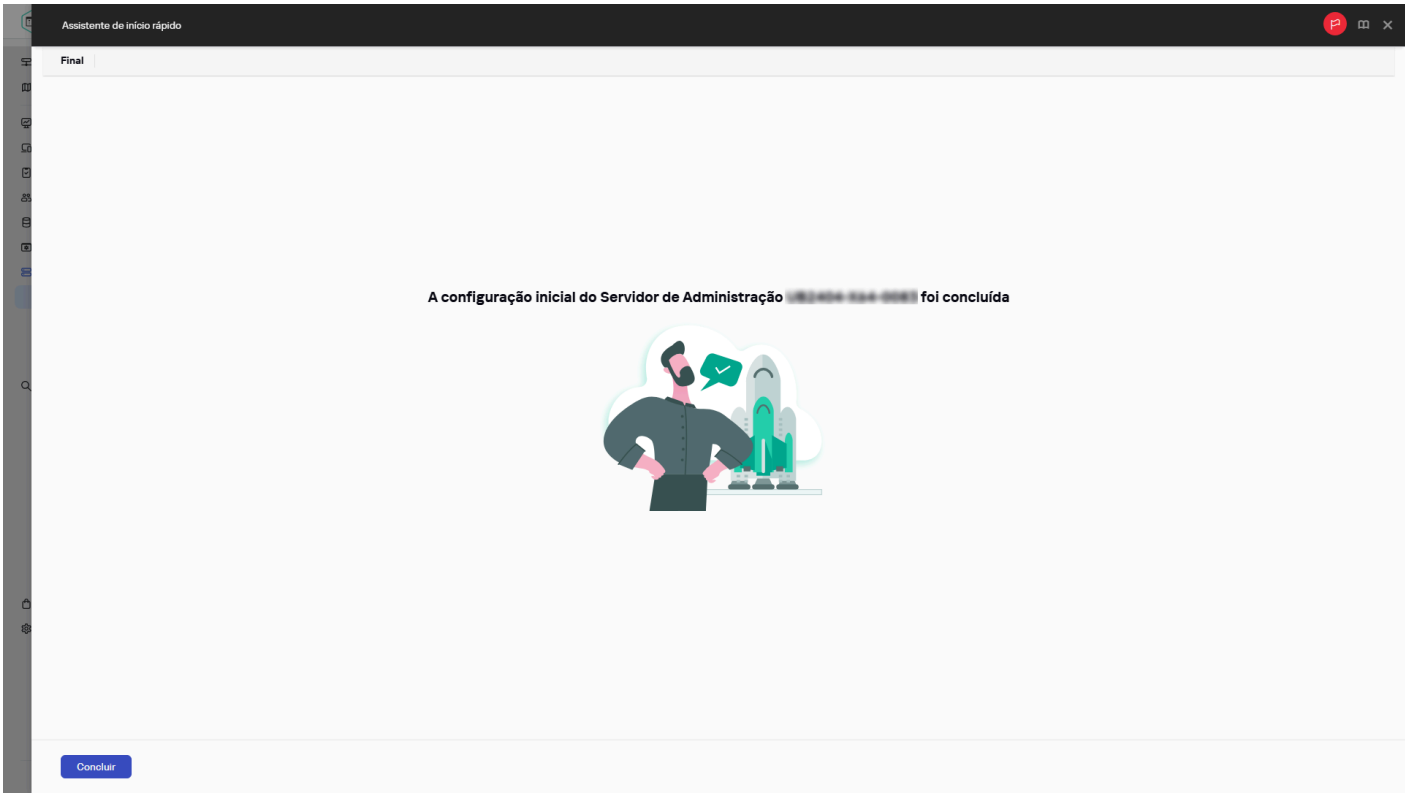
- **Usar a autenticação ESMTP**

  Ativa o suporte da autenticação ESMTP. Após selecionar a caixa de seleção, nos campos **Nome do usuário** e **Senha**, você poderá especificar as configurações de autenticação ESMTP. Por padrão, esta caixa de seleção está desmarcada.

Você pode testar as novas configurações de notificação por e-mail clicando no botão **Enviar mensagem de teste**.

Etapa 12. Fechar o Assistente de início rápido

Para fechar o assistente, pressione o botão **Concluir**.



Etapa final do Assistente de início rápido

Depois de concluir o assistente de início rápido, será possível executar o Assistente de implementação da proteção para instalar automaticamente aplicativos antivírus ou o Agente de Rede em dispositivos na sua rede.

Assistente de implementação da proteção

Para instalar os aplicativos da Kaspersky, você pode usar o assistente de Implementação da proteção. O assistente de Implementação da proteção permite a instalação remota de aplicativos por meio de pacotes de instalação especialmente criados ou diretamente de um pacote de distribuição.

O Assistente de implementação da proteção executa as seguintes ações:

- Baixa um pacote de instalação para implementação do aplicativo (se não foi criado anteriormente). O pacote de instalação está localizado em **Gerenciamento de software** → **Pacotes de instalação**. Você pode usar esse pacote de instalação para instalação do aplicativo no futuro.
- Cria e executa uma tarefa de instalação remota para dispositivos específicos ou para um grupo de administração. A tarefa de instalação remota recém-criada é armazenada na seção **Tarefas**. Você pode iniciar essa tarefa manualmente mais tarde. O tipo de tarefa é **Instalar o aplicativo remotamente**.

Caso queira instalar o agente de rede em dispositivos com o sistema operacional SUSE Linux Enterprise Server 15, instale o pacote insserv-compat primeiro para configurar o agente de rede.

Etapa 1. Iniciar o assistente de implementação da proteção

O Assistente de implementação da proteção pode ser iniciado a qualquer momento.

Para iniciar o assistente de implementação da proteção manualmente,

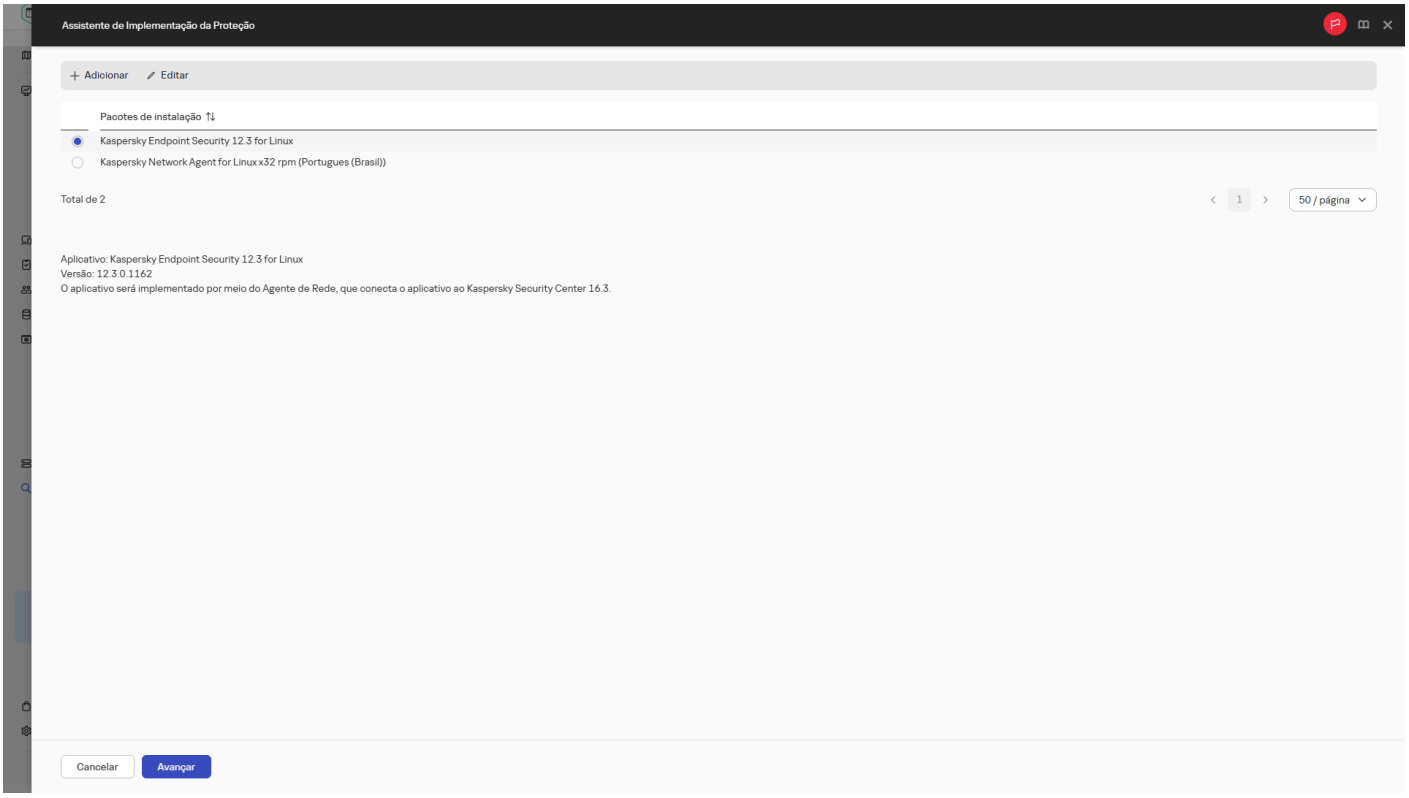
No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Assistente de implementação da proteção**.

O assistente de implementação da proteção é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

Etapa 2. Seleção do pacote de instalação

Selecione o pacote de instalação do aplicativo que deseja instalar.

Se o pacote de instalação do aplicativo necessário não estiver listado, clique no botão **Adicionar** e selecione o aplicativo na lista.



Seleção do pacote de instalação

Etapa 3. Seleção de um método de distribuição de arquivo de chave ou código de ativação

Selecione um método para a distribuição de arquivo de chave ou do código de ativação:

- **Não adicionar chave de licença ao pacote de instalação**

  A chave será automaticamente distribuída a todos os dispositivos com os quais ela for compatível:

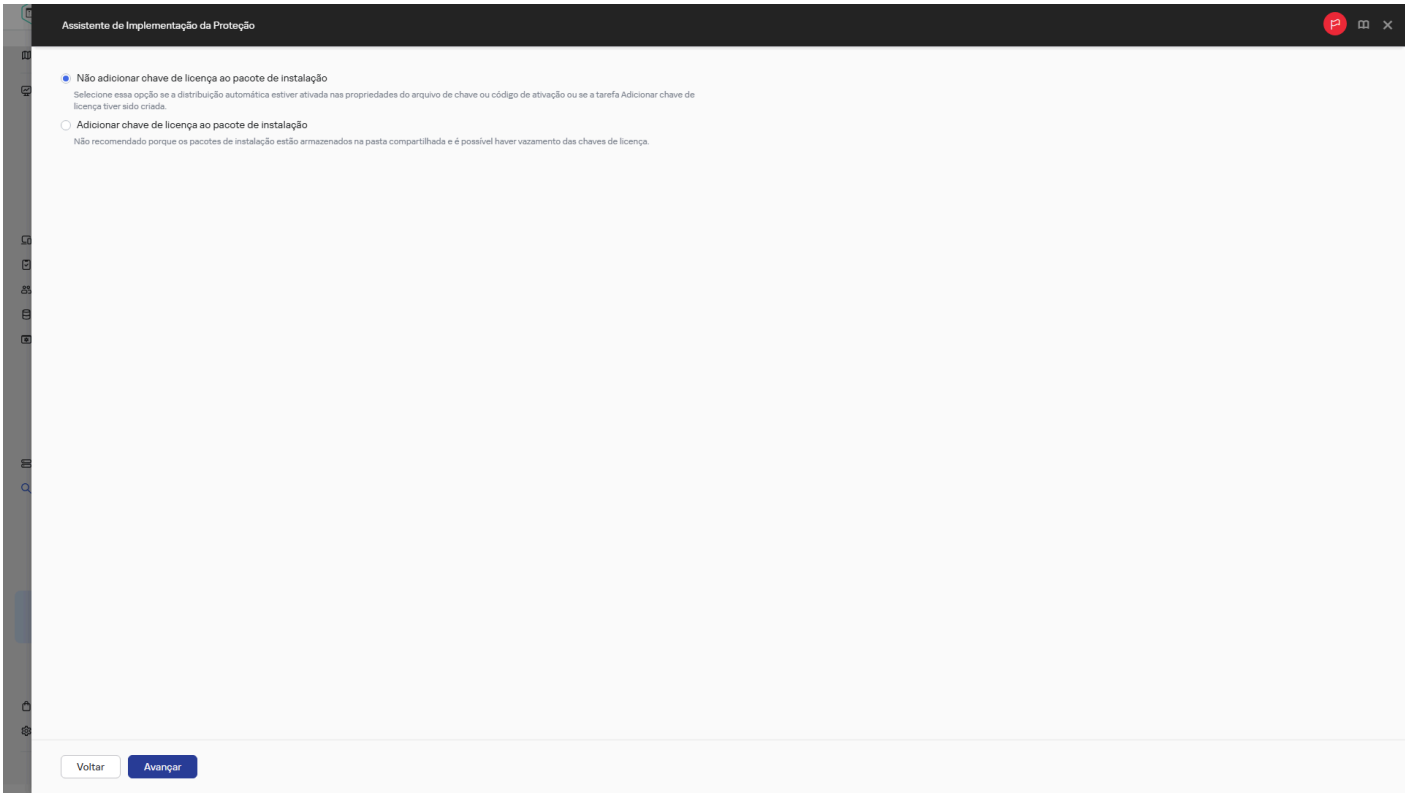
  - Se a distribuição automática foi ativada nas propriedades da chave.
  - Se a tarefa **Adicionar chave** foi criada.

- **Adicionar chave de licença ao pacote de instalação**

  A chave é distribuída aos dispositivos em conjunto com o pacote de instalação.

  Não recomendamos que distribua a chave usando este método, porque os direitos de acesso de Leitura são ativados para o repositório de pacotes de instalação.

Caso o pacote de instalação já inclua um arquivo de chave ou código de ativação, essa janela será exibida, mas conterá apenas as informações da chave de licença.

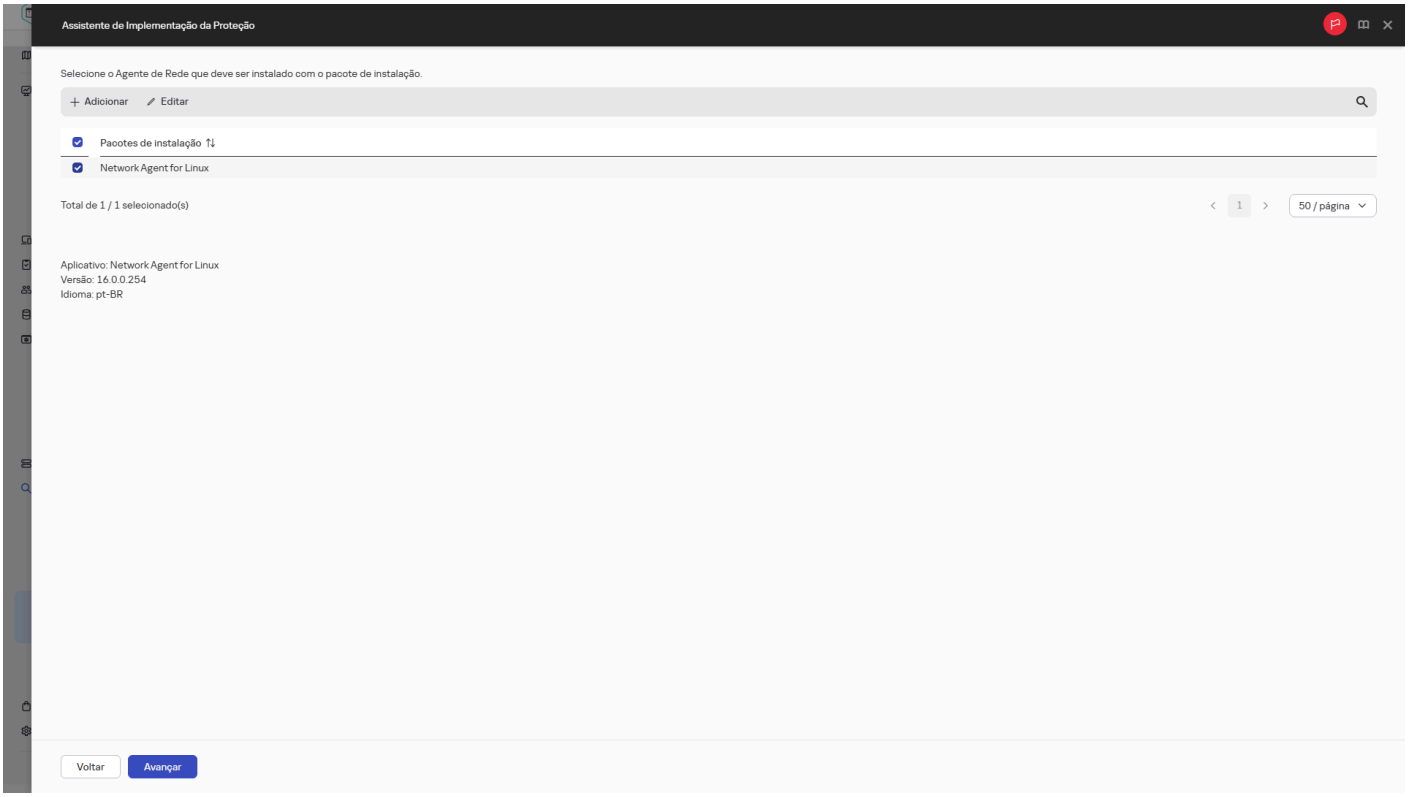


Seleção de um método de distribuição de arquivo de chave ou código de ativação

Etapa 4. Seleção de versão do Agente de Rede

Se tiver selecionado o pacote de instalação de um aplicativo que não o Agente de Rede, você também precisará instalar o Agente de Rede, que conecta o aplicativo ao Servidor de Administração.

Selecione a versão mais recente do Agente de Rede.



Seleção de versão do Agente de Rede

Etapa 5. Seleção de dispositivos

Especifique uma lista de dispositivos nos quais o aplicativo será instalado:

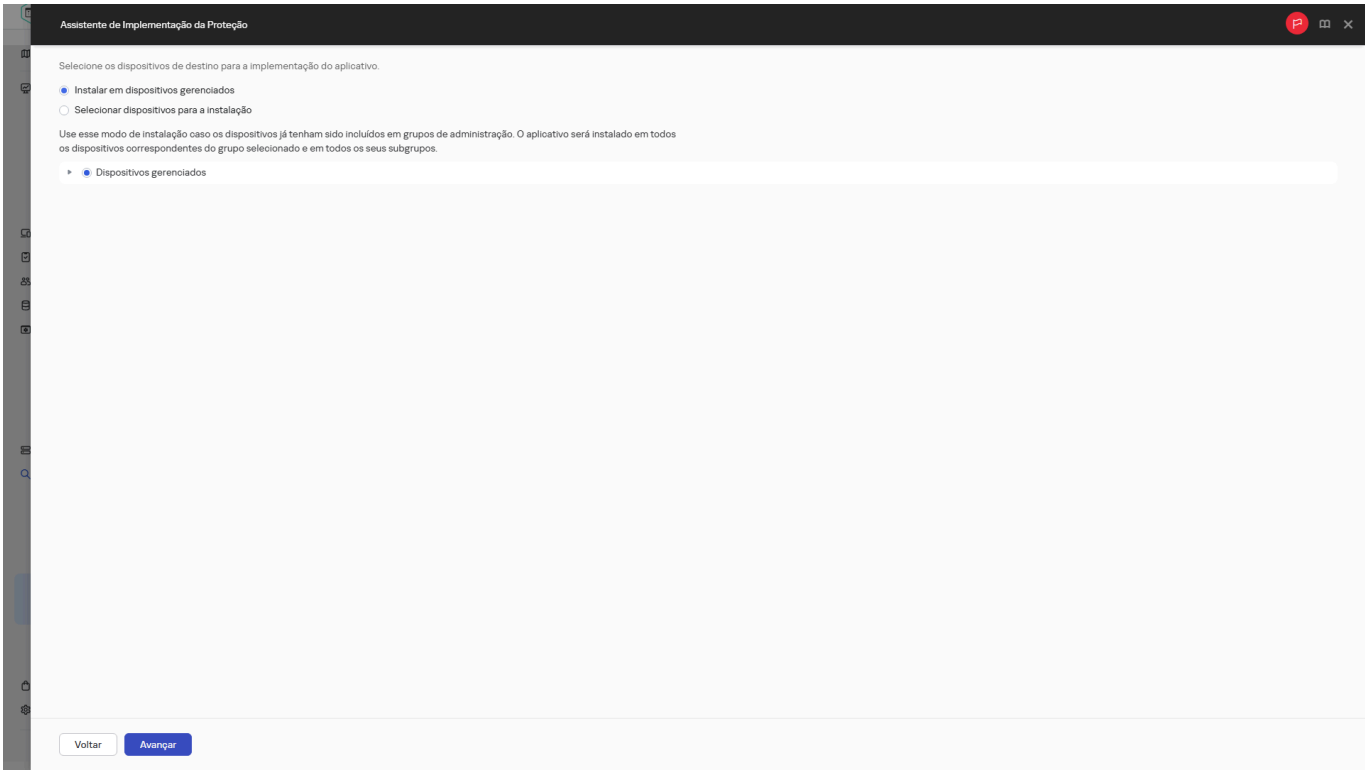
- **Instalar em dispositivos gerenciados**

  Se esta opção estiver selecionada, a tarefa de instalação remota para um grupo de dispositivos será criada.

- **Selecionar dispositivos para a instalação**

  A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.



Especificação da lista de dispositivos nos quais o aplicativo será instalado

Etapa 6. Especificação das configurações de tarefa de instalação remota

Na página **Configurações da tarefa de instalação remota**, especifique as configurações para a instalação remota do aplicativo.

No grupo de configurações **Forçar download do pacote de instalação**, especifique como os arquivos que são necessários para instalar um aplicativo são distribuídos nos dispositivos clientes:

- **Usando o Agente de Rede**

  Se esta opção de seleção estiver ativada, os pacotes de instalação são entregues aos dispositivos clientes pelo Agente de Rede instalado neles.

  Caso esta opção estiver desativada, os pacotes de instalação serão entregues usando as ferramentas do sistema operacional dos dispositivos clientes.

  Recomendamos que você ative esta opção se a tarefa tiver sido atribuída a dispositivos com o Agente de Rede instalado.

  Por padrão, esta opção está ativada.

- **Usando recursos do sistema operacional através de pontos de distribuição**

  Se a caixa de seleção estiver marcada, os pacotes de instalação serão entregues aos dispositivos clientes usando os mecanismos do sistema operacional por meio de um ponto de distribuição. Você pode selecionar esta opção se houver, no mínimo, um ponto de distribuição na rede.

  Se opção **Uso do Agente de Rede** estiver ativada, os arquivos serão entregues pelas ferramentas do sistema operacional, apenas se os recursos do Agente de Rede estiverem indisponíveis.

Por padrão, esta opção está ativada para as tarefas de instalação remotas que são criadas em um Servidor de Administração virtual.

A única maneira de instalar um aplicativo para Windows (inclusive o Agente de Rede para Windows) em um dispositivo que não tenha o Agente de Rede instalado é usando um ponto de distribuição baseado no Windows. Portanto, ao instalar um aplicativo do Windows:

- Selecione esta opção.
- Verifique e confirme se um ponto de distribuição foi atribuído aos dispositivos clientes de destino.
- Verifique se o ponto de distribuição é baseado em Windows.

- **Usando recursos do sistema operacional através do Servidor de Administração**

  Caso esta opção esteja ativada, os arquivos serão transmitidos para os dispositivos clientes usando as ferramentas do sistema operacional pelo Servidor de Administração. Você pode ativar esta opção se nenhum Agente de Rede estiver instalado no dispositivo cliente, mas esse está na mesma rede que o Servidor de Administração.

  Por padrão, esta opção está ativada.

Defina as configurações adicionais:

- **Não reinstalar o aplicativo se ele já estiver instalado**

  Se esta opção estiver ativada, o aplicativo selecionado não será reinstalado se já estiver instalado neste dispositivo cliente.

  Se esta opção não estiver ativada, o aplicativo será instalado de qualquer forma.

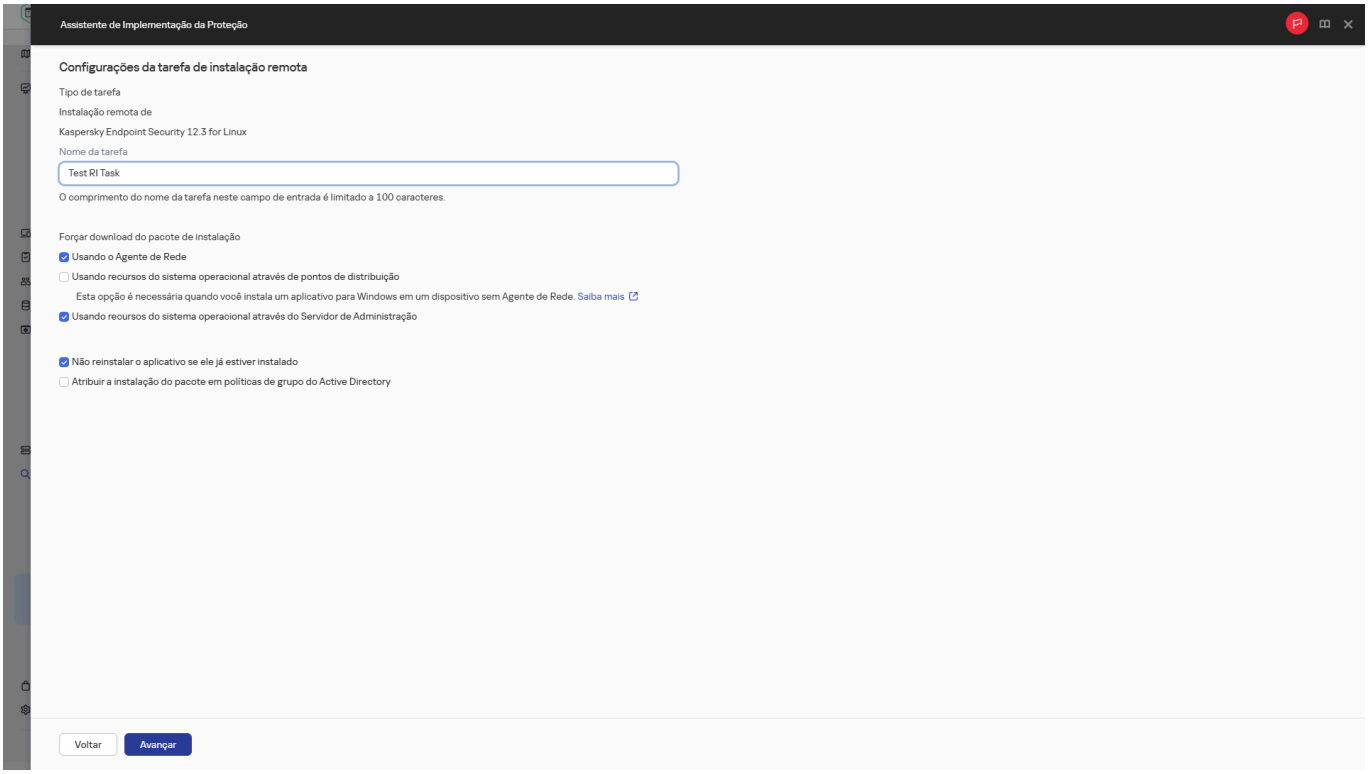
  Por padrão, esta opção está ativada.

- **Atribuir a instalação do pacote em políticas de grupo do Active Directory**

  Se esta opção estiver ativada, é instalado um pacote de instalação, usando as políticas de grupo do Active Directory.

  Essa opção fica disponível se o pacote de instalação do Agente de Rede estiver selecionado.

Por padrão, esta opção está desativada.



Especificação das configurações de tarefa de instalação remota

Etapa 7. Gerenciamento de reinício

Especifique a ação a ser executada se o sistema operacional precisar ser reiniciado quando você instalar o aplicativo:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

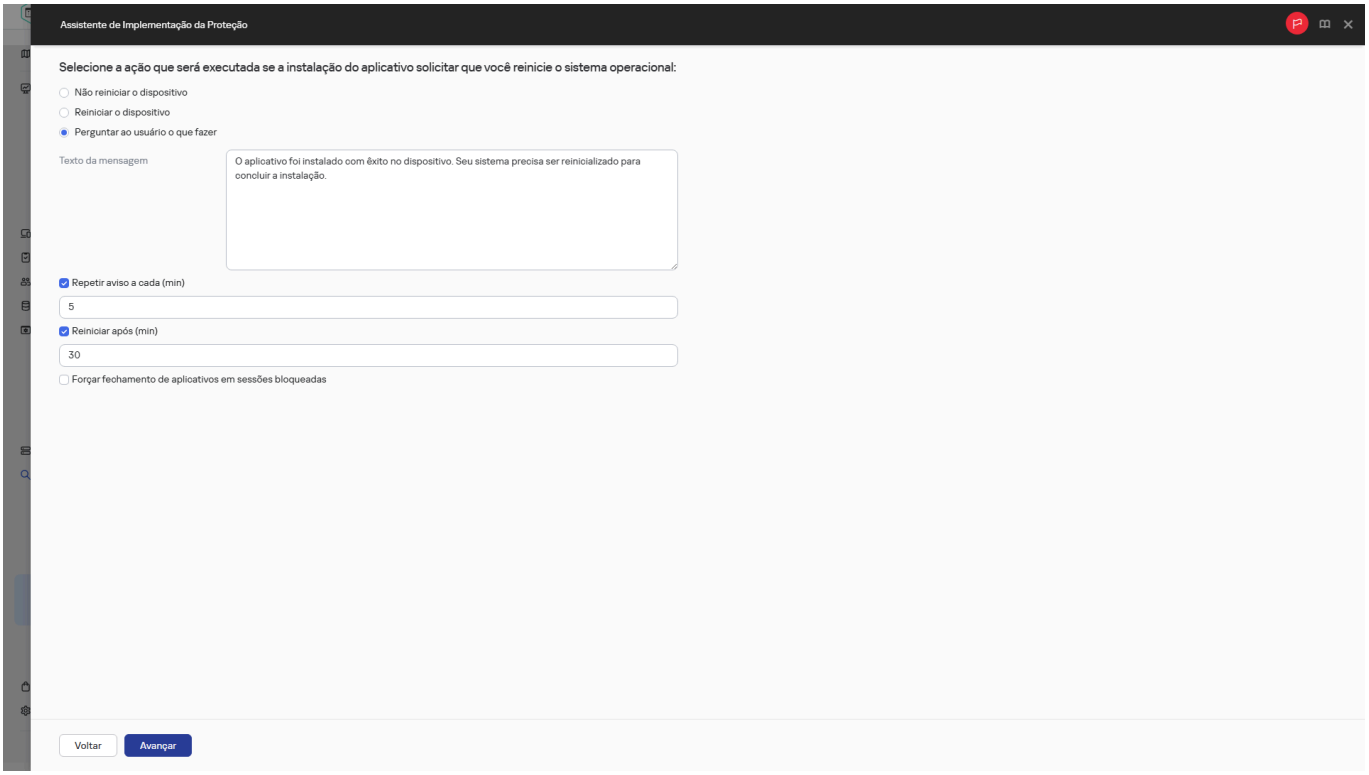
- **Forçar fechamento de aplicativos em sessões bloqueadas**

  A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

  Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

  Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

  Por padrão, esta opção está desativada.



Seleção da opção de reinício do sistema operacional

Etapa 8. Remoção de aplicativos incompatíveis antes de instalação

Esta etapa só estará presente se o aplicativo implementado for incompatível com outros aplicativos.

Selecione a opção se quiser que o Kaspersky Security Center Linux remova automaticamente aplicativos incompatíveis com o aplicativo implementado.

A lista de aplicativos incompatíveis também é exibida.

Se você não marcar esta opção, o aplicativo será instalado apenas em dispositivos que não têm aplicativos incompatíveis.

Etapa 9. Movimentação de dispositivos para dispositivos gerenciados

Especifique se os dispositivos devem ser movidos para um grupo de administração depois da instalação do Agente de Rede.

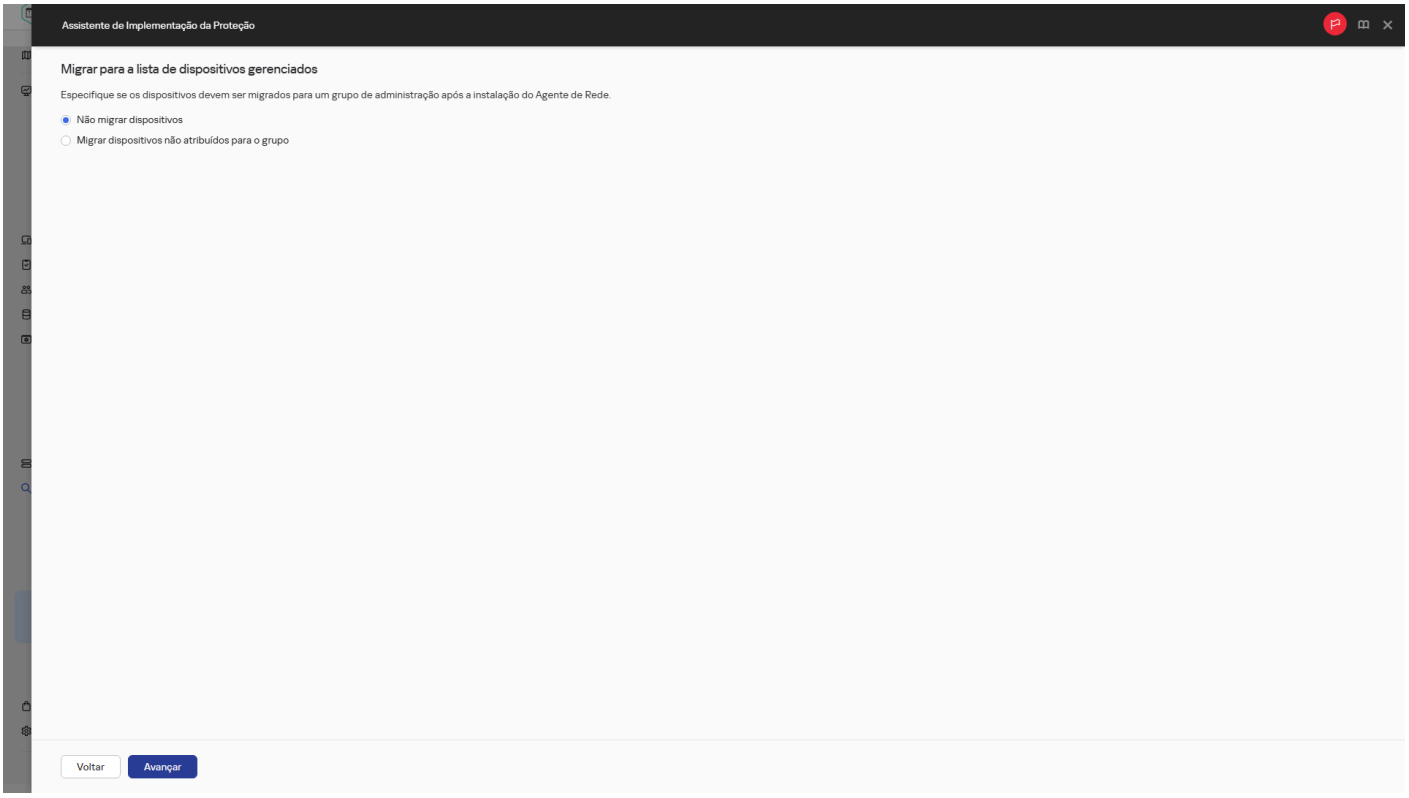
- **Não migrar dispositivos**

  Os dispositivos permanecem nos grupos nos quais eles estão atualmente localizados. Os dispositivos que não foram colocados em nenhum grupo continuam não atribuídos.

- **Migrar dispositivos não atribuídos para o grupo**

  Os dispositivos são movidos para o grupo de administração selecionado.

A opção **Não migrar dispositivos** está marcada por padrão. Por motivos de segurança, você pode desejar mover os dispositivos manualmente.



Seleção de uma opção para mover dispositivos para um grupo de administração

Etapa 10. Seleção de contas para acessar dispositivos

Se necessário, adicione as contas que serão usadas para iniciar a tarefa de instalação remota:

- **Nenhuma conta necessária (Agente de Rede instalado)**

  Se essa caixa de seleção estiver selecionada, você não precisará especificar uma conta sob a qual o instalador do aplicativo será executado. A tarefa será executada sob a conta sob a qual o serviço do Servidor de Administração está sendo executado.

  Se o Agente de Rede não tiver sido instalado em dispositivos clientes, esta opção não estará disponível.

- **Conta necessária (Agente de Rede não é usado)**

  Selecione esta opção se o Agente de Rede não estiver instalado nos dispositivos aos quais você atribui a tarefa de instalação remota. Neste caso, é possível especificar uma conta de usuário ou um certificado SSH para instalar o aplicativo.

  - **Conta local ou de domínio**. Se essa opção estiver selecionada, especifique a conta de usuário sob a qual o instalador do aplicativo será executado. Clique no botão **Adicionar**, selecione **Conta local ou de domínio** e, então, especifique as credenciais da conta do usuário.

    É possível especificar várias contas de usuário se, por exemplo, nenhuma delas tiver todos os direitos necessários em todos os dispositivos para os quais você atribui a tarefa. Nesse caso, todas as contas adicionadas são usadas para executar a tarefa, em ordem consecutiva, de cima para baixo.

  - **Certificado SSH**. Se quiser instalar um aplicativo em um dispositivo cliente baseado em Linux, poderá especificar um certificado SSH em vez de uma conta de usuário. Clique no botão **Adicionar**, selecione **Certificado SSH** e, então, especifique as chaves privada e pública do certificado.

Para gerar uma chave privada, você pode usar o utilitário ssh-keygen. Observe que o Kaspersky Security Center Linux é compatível com o formato PEM de chaves privadas, mas o utilitário ssh-keygen gera chaves SSH no formato OPENSSH por padrão. O formato OPENSSH não é compatível com o Kaspersky Security Center Linux. Para criar uma chave privada no formato PEM compatível, adicione a opção -m PEM no comando ssh-keygen. Por exemplo:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail do usuário>"
```



Seleção de contas para acessar dispositivos

Etapa 11. Início da instalação

Essa página é a última etapa do assistente. Nesta etapa, a **Tarefa de instalação remota** foi criada e configurada com sucesso.

Por padrão, a opção **Executar a tarefa após a conclusão do assistente** não está selecionada. Caso esta opção seja selecionada, a **Tarefa de instalação remota** será iniciada imediatamente após a conclusão do assistente. Caso esta opção não seja marcada, a **Tarefa de instalação remota** não será iniciada. Você pode iniciar essa tarefa manualmente mais tarde.

Clique em **OK** para concluir a etapa final do assistente de implementação da proteção.

Atualização do Kaspersky Security Center Linux

É possível instalar a versão 17 do Servidor de Administração em um dispositivo que tenha uma versão anterior do Servidor de Administração instalada (a partir da versão 13). Ao atualizar para a versão 17, todos os dados e configurações da versão anterior do Servidor de Administração são salvos.

Pré-requisitos

- Crie uma cópia de backup dos dados do Servidor de Administração antes de iniciar a atualização.
- Ao atualizar o Servidor de Administração da versão 16 ou anterior para a versão 16.1 ou posterior, a autenticação de dois fatores é ativada. Para obter mais informações, consulte Sobre a autenticação de dois fatores para uma conta.

  Para garantir que os usuários possam fazer login no Web Console com suas contas existentes usando chaves secretas configuradas de autenticação de dois fatores e que os scripts de automação OpenAPI continuem funcionando após a atualização, você deve executar as seguintes etapas:

  - Ativação da autenticação de dois fatores para todos os usuários
  - Os administradores devem configurar a autenticação de dois fatores para suas próprias contas
  - Excluir contas da autenticação de dois fatores

    Se necessário, adicione contas de integração usadas para executar scripts por meio do OpenAPI à lista de exclusão.
- Certifique-se de usar as versões do sistema operacional e do DBMS que são compatíveis com a versão 17 do Servidor de Administração. Se necessário, é possível mover o Servidor de Administração para outro dispositivo com versões mais recentes do sistema operacional e do DBMS.
- Ao atualizar o Servidor de Administração da versão 15.4 ou anterior para a versão 16 ou posterior, crie um banco de dados para o IAM no servidor DBMS. O nome do banco de dados deve ser diferente daquele instalado para uso com o Kaspersky Security Center Linux.

  - Para PostgreSQL, execute o seguinte comando:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```
  - Para MariaDB, execute o seguinte comando:

    ```
    sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
    ```
- Ao atualizar o Servidor de Administração da versão 15.4 ou anterior para a versão 16 ou posterior, prepare o arquivo de resposta com novos parâmetros para o IAM. Para obter a lista dos parâmetros necessários, consulte o artigo Instalando o Kaspersky Security Center Linux no modo silencioso. Adicione a variável de ambiente `KLAUTOANSWERS`. Defina o valor da variável como o caminho para o arquivo de respostas.
- Disponibilize a porta usada pelo processo kliam para a autenticação do protocolo OpenID Connect. O valor padrão é 4444. Consulte a descrição do parâmetro `trusted` no seguinte artigo: Parâmetros de instalação do Kaspersky Security Center Web Console.

Fases

1 Atualização do Servidor de Administração

É possível atualizar uma versão do Servidor de Administração usando um dos seguintes métodos:

- Ao usar o arquivo de instalação do Kaspersky Security Center Linux
- Ao criar o backup de dados do Servidor de Administração, instalando uma nova versão do Servidor de Administração e restaurando os dados do Servidor de Administração do backup

> Durante a atualização, o uso simultâneo do DBMS pelo Servidor de Administração e outro aplicativo é estritamente proibido.

Se sua rede incluir vários Servidores de Administração, você deverá atualizar cada Servidor manualmente. O Kaspersky Security Center Linux não oferece suporte à atualização centralizada.

2 Execução do script postinstall.pl (etapa opcional)

Se o arquivo de respostas não incluir parâmetros de IAM ou se o arquivo de respostas não for encontrado, será exibida uma mensagem no terminal durante a atualização solicitando que você execute o script postinstall.pl.

Nesta etapa do cenário, faça o seguinte:

1. No sistema operacional do Servidor de Administração, crie uma conta de usuário sem privilégios 'ksciam' que deve ser membro do grupo 'kladmins':

   ```
   adduser ksciam
   ```

   ```
   gpasswd -a ksciam kladmins
   ```

   ```
   usermod -g kladmins ksciam
   ```

2. Em uma conta com privilégios de raiz, execute o script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl para configurar o Servidor de Administração após a atualização. Quando for solicitado, digite as seguintes configurações:

   1. Insira o FQDN do Servidor IAM. Você deve usar o nome de DNS do Servidor de Administração que foi especificado ao instalar o Kaspersky Security Center Linux.
   2. Insira o nome da conta para iniciar o serviço IAM. A conta deve ser membro do grupo de segurança digitado. Por padrão, é usada a conta ksciam.
   3. Selecione o DBMS que foi instalado para funcionar com o serviço IAM:
      - Caso tenha instalado o MySQL ou o MariaDB, digite 1.
      - Caso tenha instalado o PostgreSQL ou o Postgres Pro, digite 2.
   4. Insira o endereço do IAM DBMS a ser usado pelo serviço IAM.

5. Insira o número da porta do IAM DBMS. Esta porta é usada para a comunicação com o serviço IAM. Por padrão, as seguintes portas são usadas:

   - Porta 3306 para MySQL ou MariaDB.
   - Porta 5432 para PostgreSQL ou Postgres Pro.

6. Insira o nome do banco de dados do IAM a ser usado pelo serviço do IAM. O nome do banco de dados usado pelo serviço do IAM deve ser diferente do banco de dados usado pelo Servidor de Administração.

3. **Atualizar o Kaspersky Security Center Web Console**
4. **(Opcional) Atualizar o Agente de Rede em dispositivos para uma nova versão.**
5. **Certifique-se de que a lista de permissão da autenticação de dois fatores contenha apenas contas de usuário que devem ter acesso ao Servidor de Administração.**

   Revise a lista de permissão da autenticação de dois fatores e remova quaisquer outras contas dela.

Observe que se o Servidor de Administração for atualizado para a versão 17, não será possível criar novos pacotes de instalação do Agente de Rede versão 15 ou anterior. No entanto, os pacotes de instalação criados anteriormente estarão disponíveis.

Ao atualizar o Kaspersky Security Center Linux de uma versão anterior, todos os plugins instalados dos aplicativos compatíveis são mantidos. Os Plug-ins do Servidor de Administração e do Agente de Rede são atualizados automaticamente.

Atualização da Kaspersky Security Center Linux da versão 16 ou posterior

Esta seção descreve as seguintes opções para atualizar a Kaspersky Security Center Linux da versão 16 ou posterior para a versão mais recente:

- Atualizar usando o arquivo de instalação
- Atualizar usando o backup
- Atualização nos nós de cluster de failover da Kaspersky Security Center Linux

Atualização do Kaspersky Security Center Linux da versão 16 ou posterior usando o arquivo de instalação

Para atualizar o Servidor de Administração da versão 16 ou posterior para a versão mais recente, é possível instalar uma nova versão sobre a anterior usando o arquivo de instalação da Kaspersky Security Center Linux.

Para atualizar a Kaspersky Security Center Linux da versão 16 ou posterior para a versão mais recente usando o arquivo de instalação:

1. Baixe o arquivo de instalação do Kaspersky Security Center Linux com um pacote completo para a versão 17 no site da Kaspersky:

   - Para os dispositivos que executam um sistema operacional baseado em RPM — `ksc64-<version number>.x86_64.rpm`
   - Para os dispositivos que executam um sistema operacional baseado em Debian — `ksc64_<version number>_amd64.deb`

2. Inicie a atualização da Kaspersky Security Center Linux. Execute um dos seguintes comandos no terminal da linha de comando:

   - Para os dispositivos que executam um sistema operacional baseado em RPM:

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - Para os dispositivos com um sistema operacional baseado em Debian:

     ```
     sudo apt-get install ./ksc64_<version number>_amd64.deb
     ```

   Após a execução bem-sucedida do comando, o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` será criado. A mensagem sobre isso será exibida no terminal.

3. Execute o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` para configurar o Servidor de Administração atualizado:

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

4. Leia o Contrato de Licença e a Política de Privacidade, que aparecem no terminal de linha de comando. Se você concordar com todos os termos do Contrato de Licença e da Política de Privacidade:

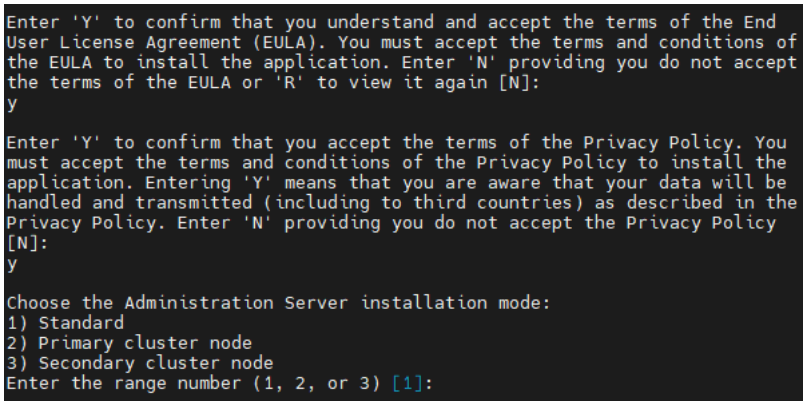
   a. Digite `Y` para confirmar que você leu, entendeu e aceita totalmente os termos e as condições do EULA.

   b. Digite `Y` novamente para confirmar que você leu, entendeu e aceita totalmente a Política de Privacidade que descreve o manuseio de dados.

   A instalação do aplicativo no seu dispositivo continuará após você inserir `Y` duas vezes.

5. Digite `1` para selecionar o modo de instalação padrão do Servidor de Administração.

A imagem abaixo mostra as duas últimas etapas.



Aceitar os termos do EULA e da Política de Privacidade e selecionar o modo de instalação padrão do Servidor de Administração no terminal de linha de comando

Em seguida, o script configura e conclui a atualização do Servidor de Administração. Durante a atualização, não é possível alterar as configurações do Servidor de Administração ajustadas antes da atualização.

6. Atualize o Kaspersky Security Center Web Console para uma nova versão.

7. Para dispositivos nos quais uma versão anterior do Agente de Rede estiver instalada, crie e execute a tarefa para instalação remota da nova versão do Agente de Rede.

   Recomendamos atualizar o Agente de Rede para Linux para a mesma versão da Kaspersky Security Center Linux.

   Após a conclusão da tarefa de instalação remota, a versão do Agente de Rede será atualizada.

   Execute os seguintes comandos em ativos baseados em Linux para remover dependências que não são mais necessárias:

   - Para ativos baseados em Debian, execute um dos seguintes comandos:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Para ativos baseados em RPM, execute um dos seguintes comandos:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Atualização da Kaspersky Security Center Linux da versão 16 ou posterior por meio do backup

Para atualizar o Servidor de Administração da versão 16 ou anterior para uma versão mais recente, é possível criar um backup dos dados do Servidor de Administração e restaurá-los após instalar uma nova versão da Kaspersky Security Center Linux. Se problemas ocorrerem durante a instalação, você poderá restaurar a versão anterior do Servidor de Administração por meio do uso do backup dos dados do Servidor de Administração criados antes da atualização.

Para atualizar a Kaspersky Security Center Linux da versão 16 ou posterior para a versão mais recente por meio do backup:

1. Antes da atualização, faça backup dos dados do Servidor de Administração com uma versão mais antiga do aplicativo.

2. Desinstale a versão mais antiga do Kaspersky Security Center Linux.

3. Instale o Kaspersky Security Center Linux versão 17 no dispositivo em que o Servidor de Administração foi instalado anteriormente.

   Se o esquema do banco de dados na cópia backup diferir daquele usado atualmente pelo Servidor de Administração ou pelo IAM, os dados serão restaurados para o esquema atual.

   Se o esquema público for usado na cópia backup, as seguintes condições são obrigatórias:

   - O esquema de banco de dados público existe no banco de dados.
   - É possível modificar o esquema de banco de dados público usando a conta do DBMS utilizada pelo Servidor de Administração ou pelo IAM para acessar o banco de dados.

   Caso contrário, haverá um erro ao final da restauração dos dados.

4. Restaure os dados do Servidor de Administração do backup criado antes da atualização.

5. Instale o Kaspersky Security Center Web Console.

   Caso o Kaspersky Security Center Web Console tenha sido instalado anteriormente, basta reinstalá-lo com o mesmo arquivo de resposta.

   Faça login no Kaspersky Security Center Web Console com a conta de usuário interna do administrador.

   O processo de inicialização dos dados geralmente leva até 15 minutos após a restauração dos dados do Servidor de Administração, mas esse tempo depende do desempenho do hardware e do tamanho dos dados. Durante esse período, o Kaspersky Security Center Web Console talvez não consiga se conectar e exiba erros.

6. Para dispositivos nos quais uma versão anterior do Agente de Rede estiver instalada, crie e execute a tarefa para instalação remota da nova versão do Agente de Rede.

   Recomendamos atualizar o Agente de Rede para Linux para a mesma versão da Kaspersky Security Center Linux.

   Após a conclusão da tarefa de instalação remota, a versão do Agente de Rede será atualizada.

Execute os seguintes comandos em ativos baseados em Linux para remover dependências que não são mais necessárias:

- Para ativos baseados em Debian, execute um dos seguintes comandos:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- Para ativos baseados em RPM, execute um dos seguintes comandos:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Atualização da Kaspersky Security Center Linux versão 16 ou posterior nos nós de cluster de failover da Kaspersky Security Center Linux

Você pode instalar a versão mais recente do Servidor de Administração em cada nó de cluster de failover da Kaspersky Security Center Linux onde o Servidor de Administração versão 16 ou posterior estiver instalado. Ao atualizar para a versão mais recente, todos os dados e configurações da versão anterior do Servidor de Administração são mantidos.

Caso já tenha instalado o Kaspersky Security Center Linux anteriormente em dispositivos locais, também é possível atualizar o Kaspersky Security Center Linux nesses dispositivos usando o arquivo de instalação ou por meio do backup.

A atualização do Kaspersky Security Center Linux para a versão 17 nos nós de cluster de failover usando um arquivo de instalação não é compatível. Para atualizar de uma versão anterior para a versão 17, crie uma cópia backup dos dados do Servidor de Administração, instale a nova versão do cluster de failover do Kaspersky Security Center Linux e, em seguida, restaure os dados do Servidor de Administração a partir da cópia backup. Essa limitação também se aplica a um cluster geograficamente distribuído.

Para atualizar o Kaspersky Security Center Linux versão 16 ou posterior nos nós de cluster de failover da Kaspersky Security Center Linux:

1. Baixe o arquivo de instalação do Kaspersky Security Center Linux com um pacote completo para a versão 17 no site da Kaspersky:
   - Para dispositivos que executam um sistema operacional baseado em RPM — `ksc64-<version number>-<build number>.x86_64.rpm`
   - Para dispositivos que executam um sistema operacional baseado em Debian — `ksc64_<version number>-<build number>_amd64.deb`

2. Interrompa o cluster.

3. No nó ativo do cluster, execute o seguinte comando no terminal da linha de comando para executar a atualização:

   - Para os dispositivos que executam um sistema operacional baseado em RPM:

     ```
     sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
     ```

   - Para os dispositivos com um sistema operacional baseado em Debian:

     ```
     sudo apt-get install ./ksc64_<version number>-<build number>_amd64.deb
     ```

   Após a execução bem-sucedida do comando, o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` será criado. A mensagem sobre isso será exibida no terminal.

   Se ocorrer algum erro, consulte a solução descrita na Base de conhecimento.

4. Execute o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` para configurar o Servidor de Administração atualizado:

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

5. Leia o Contrato de Licença e a Política de Privacidade, que aparecem no terminal de linha de comando. Se você concordar com todos os termos do Contrato de Licença e da Política de Privacidade:

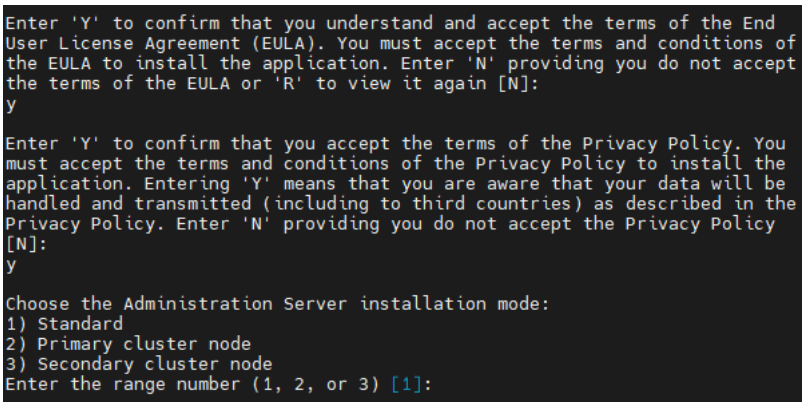
   a. Digite `Y` para confirmar que você leu, entendeu e aceita totalmente os termos e as condições do EULA.

   b. Digite `Y` novamente para confirmar que você leu, entendeu e aceita totalmente a Política de Privacidade que descreve o manuseio de dados.

   A instalação do aplicativo no seu dispositivo continuará após você inserir `Y` duas vezes.

6. Selecione o nó no qual a atualização está ocorrendo digitando `2`.

   A imagem abaixo mostra as duas últimas etapas.



Aceitar os termos do EULA e da Política de Privacidade e selecionar o modo de instalação no terminal de linha de comando

Em seguida, o script configura e conclui a atualização do Servidor de Administração. Durante a atualização, não é possível alterar as configurações do Servidor de Administração ajustadas antes da atualização.

7. Execute as etapas 3 a 5 no nó passivo.

   Na etapa 6, digite `3` para selecionar o nó.

8. Iniciar o cluster.

   > É possível iniciar o cluster em qualquer nó. Se você iniciar o cluster no nó passivo, ele se tornará o nó ativo.

9. Para dispositivos nos quais uma versão anterior do Agente de Rede estiver instalada, crie e execute a tarefa para instalação remota da nova versão do Agente de Rede.

   > Recomendamos atualizar o Agente de Rede para Linux para a mesma versão da Kaspersky Security Center Linux.

   Após a conclusão da tarefa de instalação remota, a versão do Agente de Rede será atualizada.

   Execute os seguintes comandos em ativos baseados em Linux para remover dependências que não são mais necessárias:

   - Para ativos baseados em Debian, execute um dos seguintes comandos:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Para ativos baseados em RPM, execute um dos seguintes comandos:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

   Assim, a versão mais recente do Servidor de Administração foi instalada nos nós de cluster de failover da Kaspersky Security Center Linux.

Atualização da Kaspersky Security Center Linux da versão 15.4 ou anterior

Esta seção descreve as seguintes opções para atualizar a Kaspersky Security Center Linux da versão 15.4 ou anterior para a versão 16 ou posterior:

- Atualizar usando o arquivo de instalação
- Atualizar usando o backup
- Atualização nos nós de cluster de failover da Kaspersky Security Center Linux

Cada opção de atualização da Kaspersky Security Center Linux da versão 15.4 ou anterior para a versão 16 ou posterior inclui etapas para criar e configurar um banco de dados do IAM em um servidor DBMS, criar uma conta 'ksciam' sem privilégios para executar o serviço IAM e adicionar esta conta ao grupo de segurança 'kladmins'.

Atualização da Kaspersky Security Center Linux da versão 15.4 ou anterior usando o arquivo de instalação

Para atualizar o Servidor de Administração das versões 13 a 15.4 para a versão 16 ou posterior, é possível instalar uma nova versão sobre a anterior usando o arquivo de instalação da Kaspersky Security Center Linux.

Antes de começar, verifique os requisitos para um certificado personalizado.

Se você estiver usando um certificado personalizado em vez do autoassinado, antes de atualizar a Kaspersky Security Center Linux para a versão mais recente, certifique-se de que o certificado inclua o Nome alternativo da entidade (SAN). Caso contrário, é importante substituir o certificado antes de atualizar o Kaspersky Security Center Linux. Caso contrário, você não poderá fazer login no Web Console após a atualização.

Para certificar-se de que o certificado inclui o SAN:

1. No dispositivo com o Servidor de Administração instalado, execute o comando:

   - Para um dispositivo baseado em Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - Para um dispositivo baseado em Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Assegure-se de que o Nome alternativo da entidade (SAN) esteja presente na saída do comando e contenha o endereço do dispositivo do Servidor de Administração.

3. Se o Nome alternativo da entidade estiver ausente, use o utilitário klsetsrvcert para substituir o certificado do usuário por um certificado que atenda aos requisitos.

Para atualizar a Kaspersky Security Center Linux da versão 15.4 ou anterior para a versão mais recente usando o arquivo de instalação:

1. Baixe o arquivo de instalação do Kaspersky Security Center Linux com um pacote completo para a versão 17 no site da Kaspersky:

   - Para os dispositivos que executam um sistema operacional baseado em RPM — `ksc64-<version number>.x86_64.rpm`
   - Para os dispositivos que executam um sistema operacional baseado em Debian — `ksc64_<version number>_amd64.deb`

2. No servidor DBMS, crie um banco de dados para o IAM. O nome do banco de dados do IAM deve ser diferente do nome do banco de dados instalado para uso com o Kaspersky Security Center Linux.

   - Para PostgreSQL, execute o seguinte comando:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

- Para MariaDB, execute o seguinte comando:

```
sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
```

3. Crie uma conta sem privilégios 'ksciam', adicione-a ao grupo de segurança 'kladmins' e defina este grupo como o grupo principal para a conta 'ksciam'. Para fazer isso, execute os seguintes comandos em sequência:

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

4. Inicie a atualização da Kaspersky Security Center Linux. Execute um dos seguintes comandos no terminal da linha de comando:

   - Para os dispositivos que executam um sistema operacional baseado em RPM:

   ```
   sudo yum install ./ksc64-<número da versão>.x86_64.rpm
   ```

   - Para os dispositivos com um sistema operacional baseado em Debian:

   ```
   sudo apt-get install ./ksc64_<número da versão>_amd64.deb
   ```

   Após a execução bem-sucedida do comando, o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` será criado. A mensagem sobre isso será exibida no terminal.

5. Execute o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` para configurar o Servidor de Administração atualizado:

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

6. Leia o Contrato de Licença e a Política de Privacidade, que aparecem no terminal de linha de comando. Se você concordar com todos os termos do Contrato de Licença e da Política de Privacidade:

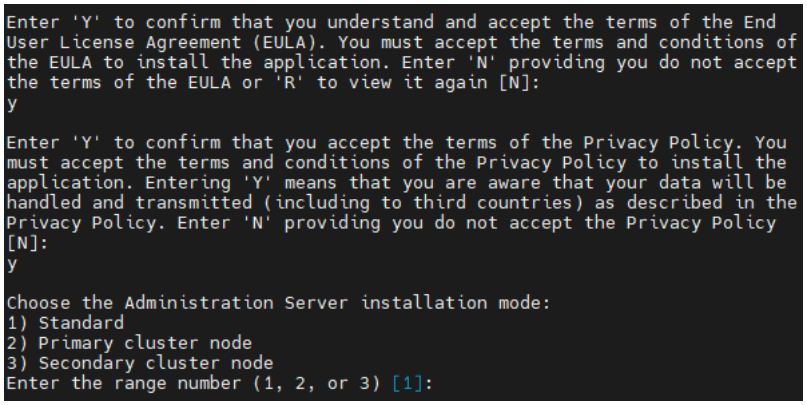
   a. Digite `Y` para confirmar que você leu, entendeu e aceita totalmente os termos e as condições do EULA.

   b. Digite `Y` novamente para confirmar que você leu, entendeu e aceita totalmente a Política de Privacidade que descreve o manuseio de dados.

   A instalação do aplicativo no seu dispositivo continuará após você inserir `Y` duas vezes.

7. Digite `1` para selecionar o modo de instalação padrão do Servidor de Administração.

A imagem abaixo mostra as duas últimas etapas.



Aceitar os termos do EULA e da Política de Privacidade e selecionar o modo de instalação padrão do Servidor de Administração no terminal de linha de comando

8. Em seguida, o script configura e conclui a atualização do Servidor de Administração. Durante a atualização, não é possível alterar as configurações do Servidor de Administração ajustadas antes da atualização. Quando for solicitado, digite as seguintes configurações:

   a. Insira o FQDN do Servidor IAM.

      Você deve usar o nome de DNS do Servidor de Administração que foi especificado ao instalar o Kaspersky Security Center Linux.

   b. Insira o nome da conta para iniciar o serviço IAM. A conta deve ser membro do grupo de segurança digitado. Por padrão, é usada a conta ksciam.

   c. Selecione o DBMS que foi instalado para funcionar com o serviço IAM:

      - Caso tenha instalado o MySQL ou o MariaDB, digite `1`.
      - Caso tenha instalado o PostgreSQL ou o Postgres Pro, digite `2`.

   d. Insira o endereço do IAM DBMS a ser usado pelo serviço IAM.

   e. Insira o número da porta do IAM DBMS. Esta porta é usada para a comunicação com o serviço IAM. Por padrão, as seguintes portas são usadas:

      - Porta 3306 para MySQL ou MariaDB.
      - Porta 5432 para PostgreSQL ou Postgres Pro.

   f. Insira o nome do banco de dados do IAM a ser usado pelo serviço do IAM. O nome do banco de dados usado pelo serviço do IAM deve ser diferente do banco de dados usado pelo Servidor de Administração.

   g. Insira o login e a senha do DBMS a serem utilizados pelo serviço IAM.

   h. Se você instalou o PostgreSQL ou o Postgres Pro, poderá especificar o esquema do banco de dados a ser usado pelo IAM. Para fazer isso, especifique o nome do esquema.

      Se não quiser usar um esquema personalizado, pressione `ENTER` para usar um esquema padrão.

      > O nome do esquema diferencia maiúsculas de minúsculas: use apenas letras minúsculas.
      > Não especifique os nomes de esquema reservados do IAM: `client, iam, ksc, locker, pat, scope, voltron`.

9. Atualize o Kaspersky Security Center Web Console para uma nova versão.

10. Para dispositivos nos quais uma versão anterior do Agente de Rede estiver instalada, crie e execute a tarefa para instalação remota da nova versão do Agente de Rede.

    Recomendamos atualizar o Agente de Rede para Linux para a mesma versão da Kaspersky Security Center Linux.

    Após a conclusão da tarefa de instalação remota, a versão do Agente de Rede será atualizada.

    Execute os seguintes comandos em ativos baseados em Linux para remover dependências que não são mais necessárias:

    - Para ativos baseados em Debian, execute um dos seguintes comandos:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - Para ativos baseados em RPM, execute um dos seguintes comandos:

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

Atualização da Kaspersky Security Center Linux da versão 15.4 ou anterior por meio do backup

Para atualizar o Servidor de Administração das versões 14.2 a 15.4 para a versão 16 ou posterior, é possível criar um backup dos dados do Servidor de Administração e restaurá-lo depois de instalar uma nova versão da Kaspersky Security Center Linux. Se problemas ocorrerem durante a instalação, você poderá restaurar a versão anterior do Servidor de Administração por meio do uso do backup dos dados do Servidor de Administração criados antes da atualização.

Pré-requisitos

1. **Verifique os requisitos para um certificado personalizado.**

   Se você estiver usando um certificado personalizado em vez do autoassinado, antes de atualizar a Kaspersky Security Center Linux para a versão mais recente, certifique-se de que o certificado inclua o Nome alternativo da entidade (SAN). Caso contrário, é importante substituir o certificado antes de atualizar o Kaspersky Security Center Linux. Caso contrário, você não poderá fazer login no Web Console após a atualização.

Para certificar-se de que o certificado inclui o SAN:

1. No dispositivo com o Servidor de Administração instalado, execute o comando:

   - Para um dispositivo baseado em Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - Para um dispositivo baseado em Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Assegure-se de que o Nome alternativo da entidade (SAN) esteja presente na saída do comando e contenha o endereço do dispositivo do Servidor de Administração.

3. Se o Nome alternativo da entidade estiver ausente, use o utilitário klsetsrvcert para substituir o certificado do usuário por um certificado que atenda aos requisitos.

2. Antes da atualização, faça backup dos dados do Servidor de Administração com uma versão mais antiga do aplicativo.

O procedimento de atualização

Para atualizar a Kaspersky Security Center Linux da versão 15.4 ou anterior para a versão mais recente por meio do backup:

1. Desinstale a versão mais antiga do Kaspersky Security Center Linux.

2. No servidor DBMS, crie um banco de dados para o IAM. O nome do banco de dados do IAM deve ser diferente do nome do banco de dados instalado para uso com o Kaspersky Security Center Linux.

   - Para PostgreSQL, execute o seguinte comando:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Para MariaDB, execute o seguinte comando:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Crie uma conta sem privilégios 'ksciam', adicione-a ao grupo de segurança 'kladmins' e defina este grupo como o grupo principal para a conta 'ksciam'. Para fazer isso, execute os seguintes comandos em sequência:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. Instale o Kaspersky Security Center Linux versão 17 no dispositivo em que o Servidor de Administração foi instalado anteriormente.

   Se o esquema do banco de dados na cópia backup diferir daquele usado atualmente pelo Servidor de Administração ou pelo IAM, os dados serão restaurados para o esquema atual.

Se o esquema público for usado na cópia backup, as seguintes condições são obrigatórias:

- O esquema de banco de dados público existe no banco de dados.
- É possível modificar o esquema de banco de dados público usando a conta do DBMS utilizada pelo Servidor de Administração ou pelo IAM para acessar o banco de dados.

Caso contrário, haverá um erro ao final da restauração dos dados.

5. Restaure os dados do Servidor de Administração do backup criado antes da atualização.
6. Configure a verificação de certificado pelo Servidor de Administração e pelo Servidor IAM.
7. Instale o Kaspersky Security Center Web Console.

   Caso o Kaspersky Security Center Web Console tenha sido instalado anteriormente, basta reinstalá-lo com o mesmo arquivo de resposta.

   Faça login no Kaspersky Security Center Web Console com a conta de usuário interna do administrador.

   O processo de inicialização dos dados geralmente leva até 15 minutos após a restauração dos dados do Servidor de Administração, mas esse tempo depende do desempenho do hardware e do tamanho dos dados. Durante esse período, o Kaspersky Security Center Web Console talvez não consiga se conectar e exiba erros.
8. Para dispositivos nos quais uma versão anterior do Agente de Rede estiver instalada, crie e execute a tarefa para instalação remota da nova versão do Agente de Rede.

   Recomendamos atualizar o Agente de Rede para Linux para a mesma versão da Kaspersky Security Center Linux.

   Após a conclusão da tarefa de instalação remota, a versão do Agente de Rede será atualizada.

   Execute os seguintes comandos em ativos baseados em Linux para remover dependências que não são mais necessárias:

   - Para ativos baseados em Debian, execute um dos seguintes comandos:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Para ativos baseados em RPM, execute um dos seguintes comandos:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Atualização da Kaspersky Security Center Linux da versão 15.4 ou anterior nos nós de cluster de failover da Kaspersky Security Center Linux

Você pode instalar o Servidor de Administração versão 16 ou posterior em cada nó de cluster de failover da Kaspersky Security Center Linux onde o Servidor de Administração versões 14 a 15.4 estiver instalado. Ao atualizar, todos os dados e configurações da versão anterior do Servidor de Administração são mantidos.

Antes de começar, verifique os requisitos para um certificado personalizado.

Se você estiver usando um certificado personalizado em vez do autoassinado, antes de atualizar a Kaspersky Security Center Linux para a versão mais recente, certifique-se de que o certificado inclua o Nome alternativo da entidade (SAN). Caso contrário, é importante substituir o certificado antes de atualizar o Kaspersky Security Center Linux. Caso contrário, você não poderá fazer login no Web Console após a atualização.

Para certificar-se de que o certificado inclui o SAN:

1. No dispositivo com o Servidor de Administração instalado, execute o comando:

   - Para um dispositivo baseado em Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Para um dispositivo baseado em Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Assegure-se de que o Nome alternativo da entidade (SAN) esteja presente na saída do comando e contenha o endereço do dispositivo do Servidor de Administração.

3. Se o Nome alternativo da entidade estiver ausente, use o utilitário klsetsrvcert para substituir o certificado do usuário por um certificado que atenda aos requisitos.

Caso já tenha instalado o Kaspersky Security Center Linux anteriormente em dispositivos locais, também é possível atualizar o Kaspersky Security Center Linux nesses dispositivos usando o arquivo de instalação ou por meio do backup.

Para atualizar a Kaspersky Security Center Linux da versão 15.4 ou anterior nos nós de cluster de failover da Kaspersky Security Center Linux:

1. Baixe o arquivo de instalação do Kaspersky Security Center Linux com um pacote completo para a versão 17 no site da Kaspersky:

   - Para dispositivos que executam um sistema operacional baseado em RPM — `ksc64-<version number>-<build number>.x86_64.rpm`
   - Para dispositivos que executam um sistema operacional baseado em Debian — `ksc64_<version number>-<build number>_amd64.deb`

2. Interrompa o cluster.

3. No servidor DBMS, crie um banco de dados para o IAM. O nome do banco de dados do IAM deve ser diferente do nome do banco de dados instalado para uso com o Kaspersky Security Center Linux.

   - Para PostgreSQL, execute o seguinte comando:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Para MariaDB, execute o seguinte comando:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. Crie uma conta sem privilégios 'ksciam', adicione-a ao grupo de segurança 'kladmins' e defina este grupo como o grupo principal para a conta 'ksciam'. Para fazer isso, execute os seguintes comandos em sequência:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

5. No nó ativo do cluster, execute um dos seguintes comandos na linha de comando para iniciar a atualização:

   - Para os dispositivos que executam um sistema operacional baseado em RPM:

     ```
     sudo yum install ./ksc64-<número da versão>-<número da compilação>.x86_64.rpm
     ```

   - Para os dispositivos com um sistema operacional baseado em Debian:

     ```
     sudo apt-get install ./ksc64_<número da versão>-<número da compilação>_amd64.deb
     ```

   Após a execução bem-sucedida do comando, o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` será criado. A mensagem sobre isso será exibida no terminal.

6. Execute o script `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` para configurar o Servidor de Administração atualizado:

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

7. Leia o Contrato de Licença e a Política de Privacidade, que aparecem no terminal de linha de comando. Se você concordar com todos os termos do Contrato de Licença e da Política de Privacidade:

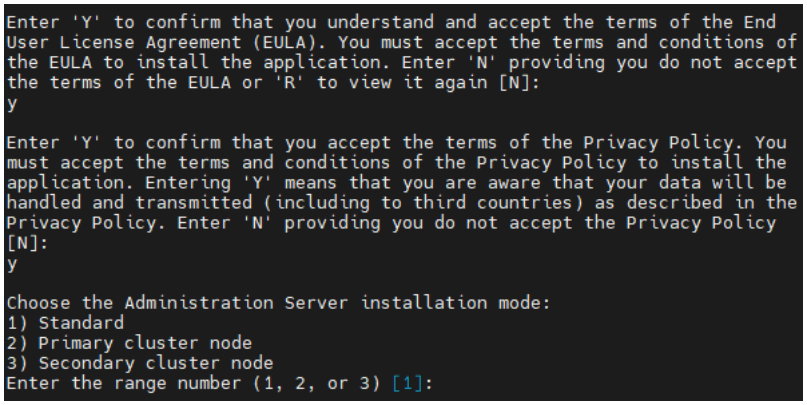
   a. Digite `Y` para confirmar que você leu, entendeu e aceita totalmente os termos e as condições do EULA.

   b. Digite `Y` novamente para confirmar que você leu, entendeu e aceita totalmente a Política de Privacidade que descreve o manuseio de dados.

   A instalação do aplicativo no seu dispositivo continuará após você inserir `Y` duas vezes.

8. Selecione o nó no qual a atualização está ocorrendo digitando `2`.

A imagem abaixo mostra as duas últimas etapas.



Aceitar os termos do EULA e da Política de Privacidade e selecionar o modo de instalação no terminal de linha de comando

9. Em seguida, o script configura e conclui a atualização do Servidor de Administração. Durante a atualização, não é possível alterar as configurações do Servidor de Administração ajustadas antes da atualização. Quando for solicitado, digite as seguintes configurações:

   a. Insira o FQDN do Servidor IAM.

      Você deve usar o nome de DNS do Servidor de Administração que foi especificado ao instalar o Kaspersky Security Center Linux.

   b. Insira o nome da conta para iniciar o serviço IAM. A conta deve ser membro do grupo de segurança digitado. Por padrão, é usada a conta ksciam.

   c. Selecione o DBMS que foi instalado para funcionar com o serviço IAM:

      - Caso tenha instalado o MySQL ou o MariaDB, digite `1`.
      - Caso tenha instalado o PostgreSQL ou o Postgres Pro, digite `2`.

   d. Insira o endereço do IAM DBMS a ser usado pelo serviço IAM.

   e. Insira o número da porta do IAM DBMS. Esta porta é usada para a comunicação com o serviço IAM. Por padrão, as seguintes portas são usadas:

      - Porta 3306 para MySQL ou MariaDB.
      - Porta 5432 para PostgreSQL ou Postgres Pro.

   f. Insira o nome do banco de dados do IAM a ser usado pelo serviço do IAM. O nome do banco de dados usado pelo serviço do IAM deve ser diferente do banco de dados usado pelo Servidor de Administração.

   g. Insira o login e a senha do DBMS a serem utilizados pelo serviço IAM.

10. Execute a etapa 5 no nó passivo.

    Na etapa 6, digite `3` para selecionar o nó.

11. Iniciar o cluster.

> É possível iniciar o cluster em qualquer nó. Se você iniciar o cluster no nó passivo, ele se tornará o nó ativo.

12. Para dispositivos nos quais uma versão anterior do Agente de Rede estiver instalada, crie e execute a tarefa para instalação remota da nova versão do Agente de Rede.

    Recomendamos atualizar o Agente de Rede para Linux para a mesma versão da Kaspersky Security Center Linux.

    Após a conclusão da tarefa de instalação remota, a versão do Agente de Rede será atualizada.

    Execute os seguintes comandos em ativos baseados em Linux para remover dependências que não são mais necessárias:

    - Para ativos baseados em Debian, execute um dos seguintes comandos:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - Para ativos baseados em RPM, execute um dos seguintes comandos:

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

    Assim, a versão mais recente do Servidor de Administração foi instalada nos nós de cluster de failover da Kaspersky Security Center Linux.

Atualizar o Kaspersky Security Center Web Console

Este artigo descreve como atualizar o Kaspersky Security Center Web Console Server (também conhecido como Kaspersky Security Center Web Console) em dispositivos que executam o sistema operacional Linux.

Caso precise atualizar o Kaspersky Security Center Web Console no Astra Linux no modo de ambiente de software fechado, siga as instruções específicas para o Astra Linux.

Use um dos seguintes arquivos de instalação que corresponda à distribuição Linux instalada em seu dispositivo:

- Para sistemas operacionais baseados em Debian: ksc-web-console-<número_da_compilação>.x86_64.deb
- Para sistemas operacionais baseados em RPM: ksc-web-console-<número_da_compilação>.x86_64.rpm

Para receber o arquivo de instalação, baixe-o do site da Kaspersky.

Para atualizar o Kaspersky Security Center Web Console:

1. Verifique e confirme se o dispositivo no qual deseja instalar o Kaspersky Security Center Web Console está executando uma das distribuições Linux compatíveis.

2. Leia e aceite o Contrato de Licença de Usuário Final (EULA). Caso o kit de distribuição do Kaspersky Security Center Linux não inclua um arquivo TXT com o texto do EULA, é possível baixá-lo pelo site da Kaspersky. Caso não aceite os termos do Contrato de Licença, não atualize o Kaspersky Security Center Web Console usando o arquivo de instalação.

3. Use o mesmo arquivo de resposta que foi preparado antes de instalar o Kaspersky Security Center Web Console. O nome do arquivo de resposta é ksc-web-console-setup.json. O arquivo está localizado em /etc/ksc-web-console-setup.json.

   > Se, ao instalar o Kaspersky Security Center Web Console, você especificou os valores dos parâmetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` e `natsMessageQueueAccount`, certifique-se de que todos esses parâmetros estejam especificados no arquivo de resposta.

   Caso o arquivo de resposta não exista, crie um arquivo de resposta que contenha os parâmetros para conectar o Kaspersky Security Center Web Console ao Servidor de Administração. Nomeie o arquivo ksc-web-console-setup.json e coloque-o no diretório /etc.

   Exemplo de um arquivo de resposta que contém o conjunto mínimo de parâmetros

   O conjunto de parâmetros do arquivo de resposta depende da versão do Servidor de Administração ao qual o Kaspersky Security Center Web Console se conecta:

   - Servidor de Administração versão 16 ou posterior

     Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 16 ou posterior:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - Servidor de Administração versão 15.4 ou posterior

     Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 15.4 ou anterior:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

É possível instalar o Kaspersky Security Center Web Console no mesmo dispositivo que o Servidor de Administração ou em um dispositivo diferente. Se o Kaspersky Security Center Web Console for instalado em um dispositivo diferente, o endereço do Kaspersky Security Center Web Console (especificado por `address`) e o endereço do Servidor de Administração (especificado por `iamHost` ou `kscHost`) serão diferentes. Se o Kaspersky Security Center Web Console for instalado no mesmo dispositivo que o Servidor de Administração, esses parâmetros terão os mesmos valores.

O valor `iamHost` deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Para obter informações detalhadas, consulte o artigo: Parâmetros de instalação do Kaspersky Security Center Web Console.

Você pode adicionar vários Servidores de Administração de versões diferentes à lista de servidores confiáveis. Nesse caso, os Servidores podem usar métodos de autenticação diferentes.

Caso queira atualizar o Kaspersky Security Center Web Console conectado ao Servidor de Administração instalado nos nós de cluster de failover da Kaspersky Security Center Linux, no arquivo de resposta, especifique o parâmetro de instalação confiável para permitir que o cluster de failover da Kaspersky Security Center Linux se conecte ao Kaspersky Security Center Web Console.

Componentes do **parâmetro de instalação** `trusted`

Se você se conectar ao Cluster de failover da Kaspersky Security Center Linux usando autenticação do domínio com SSO, especifique o parâmetro de instalação confiável da seguinte forma: Se você conectar o Kaspersky Security Center Web Console ao Servidor de Administração versão 16 ou posterior, será usada a autenticação do domínio com conexão única (SSO) fornecida pelo Identity and Access Manager (IAM). Nesse caso, especifique o parâmetro de instalação `trusted` da seguinte forma:

```
"trusted":  {
  "<Nome do Servidor de Administração>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<pasta de dados compartilhada>/iam/main_certificate.pem",
    "iamPATPath": "<pasta de dados compartilhada>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<pasta de dados compartilhada>/1093/cert/klserver.cer"
  }
}
```

onde:

- O < `nome do Servidor de Administração` > é o nome do cluster de failover do Kaspersky Security Center Linux a ser exibido na janela de login do Kaspersky Security Center Web Console.

- `iamHost` é o endereço do dispositivo onde o Servidor de Administração e o IAM estão instalados. Se você criou um adaptador de rede secundário ao preparar os nós de cluster, use o FQDN ou o nome do host do adaptador como o endereço do Cluster de failover da Kaspersky Security Center Linux. Caso contrário, especifique o FQDN ou o nome do host do balanceador de carga de terceiros em uso.

  O valor `iamHost` deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado:

  ```
  grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
  ```

- `iamOAuthPort` é a porta utilizada para trocar tokens de autenticação por meio do protocolo de autenticação OpenID Connect (o valor padrão é 4444). Esta porta é utilizada tanto para a comunicação entre o Kaspersky Security Center Web Console Server e o Servidor de Administração, quanto entre o navegador (utilizado com o Kaspersky Security Center Web Console) e o Servidor de Administração.

- `iamProxyPort` é a porta usada para conectar o Kaspersky Security Center Web Console Server ao Servidor de Administração (o valor padrão é 9050).

- `iamCertPath` é o caminho para o certificado IAM. O certificado IAM é criado automaticamente na primeira vez que você executa o Servidor de Administração. O certificado está localizado no dispositivo no qual o Servidor de Administração está instalado. O caminho padrão para o certificado é: < `pasta de dados compartilhada` >`/iam/main_certificate.pem`. O certificado está localizado no armazenamento de dados compartilhado do cluster de failover do Kaspersky Security Center Linux. O certificado IAM autoassinado é rotacionado automaticamente.

- `iamPATPath` é o caminho para o token usado para o registro do Kaspersky Security Center Web Console como um cliente OAuth no IAM. Este arquivo é gerado automaticamente na primeira vez que você executa o Servidor de Administração. O token está localizado no dispositivo no qual o Servidor de Administração está instalado. O caminho padrão para o token é: <pasta de dados compartilhada>/iam/initial_token.txt. O token está localizado no armazenamento de dados compartilhado do cluster de failover do Kaspersky Security Center Linux. A validade do token é indefinida e não requer rotação.

- `kscPort` é a porta OpenAPI que o Kaspersky Security Center Web Console usa para se conectar ao Servidor de Administração (o valor padrão é 13299).

- `kscCertPath` é o certificado do Servidor de Administração localizado no armazenamento de dados compartilhado do cluster de failover do Kaspersky Security Center Linux. O caminho padrão para o arquivo de certificado é: < `pasta de dados compartilhada` >`\1093\cert\klserver.cer`.

  Copie o arquivo de certificado do Servidor de Administração (especificado por `kscCertPath`), o arquivo de certificado IAM (especificado por `iamCertPath`) e o arquivo de token (especificado por `iamPATPath`) do armazenamento de dados compartilhado para o dispositivo no qual o Kaspersky Security Center Web Console será instalado. Especifique o caminho local para o certificado do Servidor de Administração.

Se você conectar o Kaspersky Security Center Web Console ao Servidor de Administração versão 15.4 ou anterior, será usada a autenticação especificando o nome e a senha do usuário do domínio ou do usuário interno. Nesse caso, especifique o parâmetro de instalação confiável, conforme a seguir:

```
"trusted":  {
  "<Nome do Servidor de Administração>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<pasta de dados compartilhada>/1093/cert/klserver.cer"
  }
}
```

onde:

- O < `nome do Servidor de Administração` > é o nome do cluster de failover do Kaspersky Security Center Linux a ser exibido na janela de login do Kaspersky Security Center Web Console.

- `kscHost` é o endereço do Servidor de Administração (FQDN ou nome do host). Se você criou um adaptador de rede secundário ao preparar os nós de cluster, use o endereço desse adaptador como o endereço do cluster de failover da Kaspersky Security Center Linux. Caso contrário, especifique o endereço do balanceador de carga de terceiros em uso.

- `kscPort` é a porta OpenAPI utilizada pelo Kaspersky Security Center Web Console para se conectar ao Servidor de Administração (o valor padrão é 13299).

- `kscCertPath` é o certificado do Servidor de Administração localizado no armazenamento de dados compartilhado do cluster de failover do Kaspersky Security Center Linux. O caminho padrão para o arquivo de certificado é: `< pasta de dados compartilhada >\1093\cert\klserver.cer`. Copie o arquivo de certificado do armazenamento de dados compartilhado para o dispositivo onde o Kaspersky Security Center Web Console foi instalado. Especifique o caminho local para o certificado do Servidor de Administração.

O Kaspersky Security Center Web Console não pode ser atualizado por meio do mesmo arquivo de instalação. Caso queira alterar as configurações em um arquivo de resposta e usar esse arquivo para reinstalar o aplicativo, primeiro remova o aplicativo e, em seguida, instale-o novamente com o novo arquivo de resposta.

4. Em uma conta com privilégios de raiz, use a linha de comando para executar o arquivo de configuração com a extensão .deb ou .rpm, dependendo da sua distribuição Linux.

   Para atualizar de uma versão anterior do Kaspersky Security Center Web Console, execute um dos seguintes comandos:

   - Para os dispositivos que executam um sistema operacional baseado em RPM:
     ```
     sudo yum install ksc-web-console-<número_da_compilação>.x86_64.rpm
     ```
   - Para os dispositivos com um sistema operacional baseado em Debian:
     ```
     sudo apt-get install ksc-web-console-<número da compilação>.x86_64.deb
     ```

   Essa ação inicia a descompactação do arquivo de configuração. Espere até que a instalação seja concluída.

5. Reinicie os serviços do Kaspersky Security Center Web Console executando o seguinte comando:
   ```
   sudo systemctl restart KSC*
   ```

Quando a atualização estiver concluída, será possível usar o navegador para abrir e fazer login no Kaspersky Security Center Web Console.

Atualização do Kaspersky Security Center Web Console no Astra Linux no modo de ambiente de software fechado

Este artigo descreve como atualizar o Kaspersky Security Center Web Console Server (também conhecido como Kaspersky Security Center Web Console) no sistema operacional Astra Linux Special Edition.

Para atualizar o Kaspersky Security Center Web Console:

1. Verifique e confirme se o dispositivo no qual deseja instalar o Kaspersky Security Center Web Console está executando uma das distribuições Linux compatíveis.

2. Leia e aceite o Contrato de Licença de Usuário Final (EULA). Caso o kit de distribuição do Kaspersky Security Center Linux não inclua um arquivo TXT com o texto do EULA, é possível baixá-lo pelo site da Kaspersky. Caso não aceite os termos do Contrato de Licença, não atualize o Kaspersky Security Center Web Console usando o arquivo de instalação.

3. Use o mesmo arquivo de resposta que foi preparado antes de instalar o Kaspersky Security Center Web Console. O nome do arquivo de resposta é ksc-web-console-setup.json. O arquivo está localizado em /etc/ksc-web-console-setup.json.

   Caso o arquivo de resposta não exista, crie um arquivo de resposta que contenha os parâmetros para conectar o Kaspersky Security Center Web Console ao Servidor de Administração. Nomeie o arquivo ksc-web-console-setup.json e coloque-o no diretório /etc.

   Exemplo de um arquivo de resposta que contém o conjunto mínimo de parâmetros

   O conjunto de parâmetros do arquivo de resposta depende da versão do Servidor de Administração ao qual o Kaspersky Security Center Web Console se conecta:

   - Servidor de Administração versão 16 ou posterior

     Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 16 ou posterior:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   - Servidor de Administração versão 15.4 ou posterior

     Exemplo de um arquivo de resposta com o conjunto mínimo de parâmetros para fazer login no Servidor de Administração versão 15.4 ou anterior:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
              "Administration Server v15.4": {
                  "kscHost": "ksc.example.com",
                  "kscPort": 13299,
                  "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
              }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

   É possível instalar o Kaspersky Security Center Web Console no mesmo dispositivo que o Servidor de Administração ou em um dispositivo diferente. Se o Kaspersky Security Center Web Console for instalado em um dispositivo diferente, o endereço do Kaspersky Security Center Web Console (especificado por `address`) e o endereço do Servidor de Administração (especificado por `iamHost` ou `kscHost`) serão diferentes. Se o Kaspersky Security Center Web Console for instalado no mesmo dispositivo que o Servidor de Administração, esses parâmetros terão os mesmos valores.

   O valor `iamHost` deve corresponder ao endereço do IAM especificado ao instalar o Servidor de Administração. Para obter o endereço do IAM especificado, execute o seguinte comando no dispositivo com o Servidor de Administração instalado:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Para obter informações detalhadas, consulte o artigo: Parâmetros de instalação do Kaspersky Security Center Web Console.

Você pode adicionar vários Servidores de Administração de versões diferentes à lista de servidores confiáveis. Nesse caso, os Servidores podem usar métodos de autenticação diferentes.

4. Verifique e confirme se no arquivo `/etc/digsig/digsig_initramfs.conf`, o parâmetro `DIGSIG_ELF_MODE` é especificado da seguinte forma:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Verifique e confirme se o pacote de compatibilidade `astra-digsig-oldkeys` está instalado.

   Caso o pacote não esteja instalado, execute o seguinte comando:

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

6. Crie um diretório para a chave do aplicativo, caso ele não exista:

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

7. Coloque a chave do aplicativo /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg no diretório criado na etapa anterior:

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

   Se o kit de distribuição do Kaspersky Security Center Linux não incluir a chave do aplicativo kaspersky_astra_pub_key.gpg, você poderá baixá-lo clicando no link: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Atualize os discos RAM:

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

   Reinicialize o sistema.

9. Em uma conta com privilégios de raiz, use a linha de comando para executar o arquivo de instalação. Para receber o arquivo de instalação, baixe-o do site da Kaspersky.

   Para atualizar de uma versão anterior do Kaspersky Security Center Web Console, execute o seguinte comando:

   ```
   sudo apt-get install ksc-web-console-<número da compilação>.x86_64.deb
   ```

   Essa ação inicia a descompactação do arquivo de configuração. Espere até que a instalação seja concluída.

10. Reinicie os serviços do Kaspersky Security Center Web Console executando o seguinte comando:

    ```
    sudo systemctl restart KSC*
    ```

Quando a atualização estiver concluída, será possível usar o navegador para abrir e fazer login no Kaspersky Security Center Web Console.

Migração para o Kaspersky Security Center Linux

Use o **Cenário de migração para o Kaspersky Security Center** se todas as condições forem atendidas:

- Você não precisa instalar o Servidor de Administração e o DBMS em dispositivos separados.
- O sistema operacional do Servidor de Administração é Ubuntu, Astra Linux, CentOS ou RED OS.
- O PostgreSQL é adequado para o novo Servidor de Administração.
- O Servidor de Administração antigo usava PostgreSQL ou Microsoft SQL Server como DBMS.

Selecione **Guia geral de migração para um novo servidor do Kaspersky Security Center Linux** se pelo menos uma das condições for atendida:

- Você precisa instalar o Servidor de Administração e o DBMS em dispositivos separados.
- O novo Servidor de Administração deve usar um DBMS diferente do PostgreSQL.
- O sistema operacional do Servidor de Administração não é Ubuntu, Astra Linux, CentOS nem RED OS.

Selecione **Migração para o Kaspersky Security Center usando o Assistente de migração** se:

- O tipo de DBMS do antigo Servidor de Administração do Kaspersky Security Center é diferente daquele do novo servidor, e o Microsoft SQL Server não é usado.
- Você tem experiência em transferir os dispositivos gerenciados para o novo Servidor de Administração usando tarefas e utilitários do Kaspersky Security Center.

Consulte os manuais para obter detalhes sobre considerações especiais e limitações.

Guia geral para migração para um novo servidor do Kaspersky Security Center Linux

Você pode usar uma cópia backup de dados para migrar dados de um Servidor de Administração do Kaspersky Security Center Windows ou do Kaspersky Security Center Linux para um novo servidor do Kaspersky Security Center Linux ao migrar a solução ou substituir o hardware.

Antes de migrar dados do Kaspersky Security Center Windows, certifique-se de que os recursos necessários do Kaspersky Security Center Windows são compatíveis com o Kaspersky Security Center Linux.

O guia geral de migração considera o cenário em que o novo Servidor de Administração recebe um novo nome DNS. Para restaurar a conexão dos dispositivos gerenciados, é necessário alterar o registro DNS do servidor antigo. Se você tiver experiência suficiente na configuração das soluções, poderá criar seu próprio cenário para atribuir o endereço antigo ao novo servidor durante a instalação. A presença do antigo Servidor de Administração na rede pode causar falhas no gerenciamento de dispositivos e interferir no processo de login na Web Console do novo Servidor de Administração. Ela também pode fazer com que a tarefa de instalação do Agente de Rede se conecte ao servidor antigo.

Limitações:

- Os DBMSs abaixo podem realizar a migração:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- Você precisa especificar o tipo de DBMS de destino no utilitário de backup ao migrar do Microsoft SQL Server. Em outros cenários de migração, a compatibilidade dos bancos de dados é determinada pelo parágrafo acima.
- A versão do DBMS no novo Servidor de Administração não deve ser anterior à versão do DBMS usado no Servidor de Administração anterior.
- O Kaspersky Security Center Windows deve ser atualizado para a versão mais recente antes da criação de uma cópia backup para a migração de dados.
- Caso use o MySQL ou o MariaDB como um DBMS para o Kaspersky Security Center Windows e para o Kaspersky Security Center Linux, o parâmetro `lower_case_table_names` deve corresponder ao DBMS atual e ao novo.

1 Preparação para criar uma cópia backup

Esta etapa contém instruções para preparar um Servidor de Administração configurado anteriormente para a posterior migração para o novo Servidor de Administração do Kaspersky Security Center Linux. As etapas preliminares são as seguintes:

1. Verifique a versão do Servidor de Administração para criar uma cópia backup compatível com o Kaspersky Security Center Linux.

   Todas as versões atuais do **Kaspersky Security Center Linux** oferecem suporte à migração de dados durante a atualização para uma versão mais recente do aplicativo. As cópias backup só podem ser criadas e restauradas no mesmo tipo de SGBD.

   Para o **Kaspersky Security Center Windows**, verifique a versão do Servidor de Administração em **Propriedades** → **Geral** → **Versão**. Se a versão for anterior à 15.1.0.22239, atualize o Kaspersky Security Center Windows para a versão mais recente.

Atualização do Kaspersky Security Center Windows para a versão mais recente

1. From the Kaspersky website, download the distribution package corresponding to the localization language of your installed Administration Server: `Version 15.1.0.22239 | Windows | Full distributive`.

   The executable file is saved to your **Downloads** folder with the following name: `ksc_15.1_<build number>_full_<language>.exe`.

2. Copie o pacote de distribuição para o Servidor de Administração.

3. Run the `ksc_15.1_<build number>_full_<language>.exe` executable file as administrator.

4. Na janela exibida, clique no link **Instalar o Kaspersky Security Center**.

   O Assistente de instalação do Servidor de Administração é iniciado.

5. Leia o Contrato de Licença e a Política de Privacidade. Se você concordar com todos os termos e condições do Contrato de Licença de Usuário Final e da Política de Privacidade, marque as seguintes caixas de seleção em **Confirmo que li por completo, entendo e aceito os termos e condições dos seguintes**:

   - **Os termos e condições deste EULA**.
   - **Política de Privacidade que descreve o manuseio de dados**.

6. Selecione **Efetuar upgrade do Servidor de Administração e do console baseado na Web (recomendado)** e avance para a próxima etapa.

7. Crie uma nova cópia backup selecionando **Quero criar uma cópia backup dos dados** e concluindo o assistente de backup.

8. Clique em **Efetuar upgrade**.

9. Durante a atualização, confirme todas as etapas do assistente de instalação do Web Console para atualizar a versão.

   O processo de atualização leva algum tempo. Após a conclusão do assistente de instalação, o Console de Administração pode não aceitar conexões até que o banco de dados seja inicializado.

10. Aguarde até que a atualização seja concluída.

2. Verifique se o certificado do Servidor de Administração está em conformidade.

   Antes de criar uma cópia backup, verifique se o certificado contém o Subject Alternative Name (SAN). Se não contiver, é importante substituir o certificado. Caso contrário, você não poderá fazer login no Web Console após restaurar uma cópia backup.

   Para verificar se o certificado inclui um Subject Alternative Name:

   - Para um dispositivo baseado em Windows:

     a. No Console de Administração, selecione o Servidor de Administração que deseja verificar.

     b. No menu de contexto, selecione **Propriedades → Geral → Exibir certificado do Servidor de Administração**.

     c. Na janela exibida, verifique o valor de **Subject Alternative Name**.

- Para um dispositivo Linux, execute o seguinte comando:

```
sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
```

Verifique se o Subject Alternative Name contém o nome de domínio (DNS) do host do Servidor de Administração.

Se o valor contiver apenas um endereço IP ou estiver ausente, substitua manualmente o certificado por um que atenda aos requisitos para trabalhar com o Kaspersky Security Center Linux. Substitua o certificado geral do Servidor de Administração usando o utilitário klsetsrvcert.

Substituição do certificado geral do Servidor de Administração usando o utilitário klsetsrvcert

1. Crie um novo certificado com uma data posterior para o início de seu uso nos dispositivos executando o seguinte comando:

   - Para o Kaspersky Security Center Windows:

   ```
   "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
   <oldksc.example.internal>" -o "RsaKeyLen:2048"
   ```

   - Para o Kaspersky Security Center Linux:

   ```
   /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
   ```

   em que `"<oldksc.example.internal>"` é o FQDN da conexão com o Servidor de Administração.

   > Não use um endereço IP para esse valor.

2. Defina a data de início do novo certificado em todos os hosts executando o seguinte comando:

   - Para o Kaspersky Security Center Windows:

   ```
   "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
   ```

   - Para o Kaspersky Security Center Linux:

   ```
   /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
   ```

   em que a data `"DD-MM-YYYY hh:mm"` é pelo menos 30 dias posterior à data atual. Por padrão, o período de distribuição de um novo certificado (`CR`) é de 90 dias.

   > Quando chegar a data configurada, você precisará reinstalar o Web Console para restaurar o acesso a ele e atualizar seu certificado.

3. Se necessário, após a migração para um novo Servidor de Administração, execute o utilitário klmover para restaurar a conexão dos hosts com o Servidor de Administração. Talvez seja necessário executar o utilitário se o host tiver permanecido desligado durante todo o período de distribuição do certificado ou se não tiver se conectado ao Servidor de Administração.

2 Criar uma cópia backup da instalação antiga do Servidor de Administração

Criar uma cópia backup do Kaspersky Security Center Windows

1. No menu **Iniciar** → **Kaspersky Security Center** → **Utilitário de Backup da Kaspersky**, execute o utilitário `klbackup.exe` na pasta de instalação do Kaspersky Security Center Linux.

   O Assistente de Instalação é iniciado. No Microsoft Windows em modo Server Core, use a versão de console do utilitário klbackup.

2. Na primeira etapa, selecione **Executar backup de dados do Servidor de Administração**.

3. Na etapa **Configurações de backup**:

   a. Clique no botão **Procurar** e crie uma nova pasta para salvar a cópia backup fora do diretório padrão, por exemplo, `C:\kscbackups`.

   b. Se você estiver usando o Microsoft SQL Server, selecione a opção **Migração do banco de dados** → **Migrar para o formato Postgres** para usar com o script de instalação rápida. Com o método usual de implantação do Kaspersky Security Center Linux, você também pode migrar os dados para um banco de dados MySQL/MariaDB.

   c. Defina uma senha para a cópia backup a fim de proteger os dados contra acesso não autorizado.

4. Aguarde a criação da cópia backup e saia do utilitário.

Um novo diretório é criado no diretório com o carimbo de data e hora da cópia backup.

Criar uma cópia backup do Kaspersky Security Center Linux

1. No dispositivo do Servidor de Administração, insira o seguinte comando na linha de comando:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. Aguarde até que a cópia backup seja criada.

No diretório especificado em `-path`, é criado um novo diretório com o carimbo de data e hora da cópia backup.

Depois de criar uma cópia backup do Servidor de Administração antigo, desative o dispositivo no qual ele está instalado.

Desativar o dispositivo do Servidor de Administração

1. Copie a cópia backup resultante para transferir os dados para a estação de trabalho do administrador.

2. Desligue o sistema operacional do dispositivo do Servidor de Administração.

3. Desconecte o adaptador de rede da rede corporativa.

4. Libere o endereço IP do dispositivo se quiser usá-lo na nova instalação do Kaspersky Security Center Linux.

5. Verifique se o dispositivo está completamente desconectado.

A presença do antigo Servidor de Administração na rede pode causar falhas no gerenciamento de dispositivos e interferir no processo de login na Web Console do novo Servidor de Administração. Ela também pode fazer com que a tarefa de instalação do Agente de Rede se conecte ao servidor antigo.

3 Instalação inicial do Kaspersky Security Center Linux

- **Preparação para implementação**

  Antes de prosseguir com a instalação, prepare o seguinte:

  - A imagem de disco de instalação do sistema operacional e o repositório de pacotes de aplicativos.
  - Um app autenticador para autenticação de dois fatores (2FA) ao fazer login no Web Console.
  - Novo FQDN (por exemplo, *ksclinux.example.com*). Se você tiver experiência suficiente na configuração das soluções, poderá elaborar seu próprio procedimento para atribuir o FQDN antigo ao novo servidor durante a instalação. Nesse caso, na etapa 5, "Configuração do aplicativo após a restauração de uma Cópia backup", ignore a etapa 4. "Restauração da conexão dos dispositivos gerenciados ao FQDN do Servidor de Administração anterior".
  - A estação de trabalho do administrador com um navegador para acessar a Internet, baixar pacotes de distribuição e gerenciar o Web Console.
  - Verifique se o servidor DNS e o servidor de horário (NTP) estão disponíveis para os componentes do aplicativo.
  - Dependendo do cenário, libere o endereço IP antigo se ele tiver sido usado para as conexões dos dispositivos gerenciados.
  - Configure o equipamento de rede e o servidor proxy de acordo com os requisitos:
    - Portas para comunicação entre os componentes do aplicativo.
    - Acesso aos servidores da Kaspersky.
    - Guia de proteção.

- **Escolha de uma configuração, configuração e instalação**

  a. Prepare o equipamento para o Servidor de Administração, o DBMS e o Web Console de acordo com os requisitos de hardware e software e os recursos de hardware calculados, para permitir o gerenciamento do número necessário de dispositivos sob a carga projetada.

  Para melhorar a segurança dos componentes da solução, inclua o aplicativo Kaspersky Endpoint Security for Linux nos cálculos de dimensionamento e instale-o nos nós do Kaspersky Security Center Linux.

  b. Instale e configure o sistema operacional e os componentes da solução Kaspersky Security Center de acordo com as instruções para a implementação inicial da solução.

- **Como efetuar login no Web Console pela primeira vez**

  1. No navegador, abra o endereço de conexão com o Web Console: `https://<FQDN>:8080`

     em que `<FQDN>` é o endereço do Servidor de Administração definido nas configurações de instalação do script, por exemplo, *https://ksclinux.example.com:8080*.

  2. Para efetuar login no Web Console, use o nome de usuário e a senha exibidos na saída do script.

  3. Configure o aplicativo autenticador:

     a. Copie a chave secreta para obter códigos de uso único no aplicativo ou verifique o código QR no assistente de configuração da autenticação do Web Console.

     b. Insira o código gerado para se autenticar e efetuar login no Web Console.

  4. Leia o Guia de proteção e confirme que você o leu.

  5. Configure o Servidor de Administração no assistente de início rápido se não pretende restaurar os dados do Servidor de Administração a partir de uma cópia backup.

4 Restauração a partir de uma cópia backup do Servidor de Administração

A restauração a partir de uma cópia backup do Servidor de Administração envolve as seguintes etapas:

1. Transferência da cópia backup para o Servidor de Administração

Transfira a cópia backup do Servidor de Administração antigo para o dispositivo do novo Servidor de Administração usando uma mídia removível ou pela rede.

Para transferir a cópia backup para o Servidor de Administração pela rede:

> A possibilidade de usar o utilitário scp para copiar os dados depende de o serviço SSH estar instalado e em execução no sistema operacional do dispositivo do Servidor de Administração e da política de segurança da sua organização.

1. Na linha de comando do dispositivo, use o comando *cd* para acessar o diretório que contém os arquivos da cópia backup do Servidor de Administração antigo, por exemplo:

   Windows

   ```
   cd C:\kscbackups
   ```

   Linux

   ```
   cd /root/kscbackups
   ```

2. Copie o diretório que contém os arquivos da cópia backup usando o utilitário scp:

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   onde:

`<klbackup202x-xx-xx>` é o diretório com os arquivos da cópia backup.

`<administrator>` é o usuário privilegiado no novo Servidor de Administração com permissão para conexão SSH.

`<kscLinux.example.com>` é o FQDN do novo Servidor de Administração.

O diretório com a cópia backup é copiado para o diretório pessoal do usuário especificado.

2. Procedimento de restauração a partir de uma cópia backup

1. No dispositivo do novo Servidor de Administração, abra a linha de comando.
2. Durante a restauração dos dados de uma cópia backup, conceda temporariamente privilégios de superusuário do PostgreSQL às contas padrão klserver e kliam que o Servidor de Administração usa para se conectar ao SGBD:

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
   ```

3. Use o utilitário klbackup para iniciar a restauração dos dados da cópia backup do Servidor de Administração antigo:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
   ```

   onde `</home/administrator/klbackup202x-xx-xx>` é o caminho completo para o diretório que contém os arquivos da cópia backup.

4. Se nenhuma senha tiver sido definida para a cópia backup, quando a senha da cópia backup for solicitada, pressione **Enter** sem digitar uma senha.
5. Aguarde até que o utilitário termine.

   Instalações grandes podem levar muito tempo.

6. Restaure as permissões originais das contas do PostgreSQL que o Servidor de Administração usa para se conectar ao DBMS.

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
   ```

5 Configuração do aplicativo após a restauração de uma cópia backup

Ignore esta etapa se você não restaurou os dados de uma cópia backup.

O procedimento para configurar o aplicativo após a restauração de uma cópia backup envolve as seguintes etapas:

1. Restaurar o Web Console

1. Obtenha o endereço do servidor antigo no arquivo de configuração do Servidor IAM:

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Exemplo

```
ksc_address: "oldksc.example.internal"
```

2. Verifique se o endereço FQDN do Servidor de Administração antigo está sendo convertido corretamente para o endereço IP de loopback do novo Servidor de Administração. Para fazer isso:

   a. Execute o comando `ping` com o endereço do Servidor de Administração antigo.

   Exemplo de obtenção bem-sucedida de um endereço IP de loopback

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. Adicione o endereço do Servidor de Administração antigo ao arquivo `[[/etc/hosts]]` do sistema operacional do novo Servidor de Administração se o endereço não tiver sido obtido ou se tiver sido obtido um endereço IP externo. Para fazer isso:

   - Abra o arquivo /etc/hosts para edição:

```
sudo nano /etc/hosts
```

   - Insira o nome do servidor antigo como um codinome adicional para o endereço do dispositivo do Servidor de Administração.

   Exemplo

```
127.0.0.1       localhost
127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
<...>
```

3. Reinstale o Web Console.

   a. Exclua o Web Console Server local:

   Dependendo da distribuição do Kaspersky Security Center Linux, execute um dos seguintes comandos:

   - Para um dispositivo com um sistema operacional baseado em Debian:

```
sudo apt remove ksc-web-console -y
```

   - Para um dispositivo com um sistema operacional baseado em Red Hat Enterprise Linux:

```
sudo dnf remove ksc-web-console -y
```

b. Inicie a instalação do pacote do Web Console a partir do diretório que contém os pacotes de distribuição:

- Em um dispositivo com um sistema operacional baseado em Debian:

```
sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
```

- Para um dispositivo com um sistema operacional baseado em Red Hat Enterprise Linux:

```
sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
```

2. Restaurar o acesso do usuário kscadmin para a migração do Kaspersky Security Center Windows

O banco de dados de usuários foi sobrescrito; crie o usuário kscadmin e configure a autenticação de dois fatores do zero.

1. Abra a linha de comando no sistema operacional do dispositivo do Servidor de Administração e execute o seguinte comando para criar um usuário:

```
sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
```

Depois de pressionar **Enter**, defina uma senha e, em seguida, digite-a novamente.

2. No navegador, abra o endereço para se conectar ao Web Console:

```
https://<FQDN>:8080
```

em que `<FQDN>` é o endereço do Servidor de Administração definido nas configurações de instalação do script, por exemplo, *https://ksclinux.example.com:8080*.

3. Use o nome de usuário e a senha gerados para fazer login no Web Console.

4. Configure um app autenticador. Para fazer isso:

a. Exclua o perfil antigo da conta de usuário kscadmin que estava configurado no seu app autenticador antes de iniciar a restauração da cópia backup do Servidor de Administração.

b. Copie a chave secreta para obter códigos de uso único no aplicativo ou verifique o código QR no assistente de configuração da autenticação do Web Console.

c. Insira o código gerado para se autenticar e efetuar login no Web Console.

3. Testar o Servidor de Administração

1. Teste a interface do Web Console como o usuário kscadmin e como outros usuários.

2. Execute as seguintes tarefas em sequência:

- Baixar atualizações para o repositório do Servidor de Administração
- Manutenção do Servidor de Administração
- Backup de dados do Servidor de Administração

Substitua os caminhos do Windows nas configurações das tarefas pelos caminhos do Linux do novo Servidor de Administração ou exclua as tarefas e configure novas tarefas do zero.

3. Analise os resultados das tarefas e, se necessário, altere as configurações das tarefas, as políticas de gerenciamento e as configurações do Servidor de Administração.

4. Restaurar a conexão dos dispositivos gerenciados com o FQDN do Servidor de Administração anterior

Se você atribuiu um novo endereço FQDN ao novo Servidor de Administração (por exemplo, ksclinux.example.com), adicione um dos seguintes tipos de registros DNS:

- Um registro CNAME que mapeia o nome antigo do Servidor de Administração para o novo nome do Servidor de Administração.

  Para obter mais informações sobre como configurar os registros necessários, consulte a documentação do servidor DNS.

- Um registro A e um registro AAAA para o endereço antigo do Servidor de Administração que apontam para o novo endereço IP do Servidor de Administração.

  Para um serviço DNS baseado no Windows Server, execute os comandos com valores aplicáveis à sua infraestrutura.

Para adicionar um registro DNS A a um serviço DNS baseado no Windows Server, execute os comandos usando valores aplicáveis à sua infraestrutura:

1. Conecte-se ao servidor DNS.
2. Abra o PowerShell e obtenha o endereço IP do registro A existente executando o seguinte comando:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. Altere o endereço IP no registro A executando os seguintes comandos:

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. Verifique se o endereço IP no registro A foi atualizado executando o seguinte comando:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

A saída do comando exibe o endereço IP do Servidor de Administração do Kaspersky Security Center Linux. Os dispositivos gerenciados restabelecerão suas conexões após a atualização do cache DNS local.

6 Configurar a proteção antivírus do Servidor de Administração

Para implementar as diretrizes de proteção antivírus do Guia de proteção no Servidor de Administração, instale os aplicativos da Kaspersky no Servidor de Administração e configure as políticas de gerenciamento para os aplicativos instalados.

A instalação e a configuração envolvem as seguintes etapas:

1. Criar um grupo de administração separado

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Hierarquia de grupos**.
2. Marque a caixa de seleção ao lado do grupo **Dispositivos gerenciados**.
3. Clique em **Adicionar**.
4. Na janela exibida, insira um nome para o novo grupo (por exemplo, *kscserver*) e confirme a criação clicando no botão **Adicionar**.

2. Criar uma política para o Agente de Rede sem herança de configurações

1. Na janela principal do Web Console, acesse a seção **Gerenciamento de ativos** → **Políticas**.
2. Em seguida, clique no botão **Adicionar**.
3. No Assistente de nova política, selecione o aplicativo **Agente de Rede do Kaspersky Security Center Linux** e clique em **Avançar**.
4. Desative a opção **Herdar configurações da política principal** e clique em **Salvar**.

3. Instalar o plug-in de gerenciamento do Kaspersky Endpoint Security for Linux pelo Kaspersky Security Center Linux ou manualmente

Você pode instalar o plug-in de gerenciamento do Kaspersky Endpoint Security for Linux das seguintes maneiras:

- Da lista de pacotes de distribuição disponíveis no Web Console
- Manualmente a partir de um arquivo

Para instalar o plug-in de gerenciamento do Kaspersky Endpoint Security pela lista de pacotes de distribuição disponíveis no Web Console:

1. Na janela principal do Web Console, selecione **Configurações** → **Plug-ins da Web**.

   Isso abre a lista de plug-ins da web instalados.

2. Em seguida, clique no botão **Adicionar**.

   A lista de plug-ins de gerenciamento disponíveis é exibida. Essa lista é atualizada automaticamente sempre que uma nova versão de um plug-in da web é lançada.

3. Na lista de plug-ins disponíveis, selecione a versão mais recente do plug-in da web do Kaspersky Endpoint Security for Linux.

4. Na janela de descrição do plug-in da web exibida, clique no botão **Instalar plug-in**.

5. Aguarde até que a instalação seja concluída e clique no botão **OK** na janela de informações.

O novo plug-in é adicionado à lista de plug-ins da web instalados.

Vídeo: instalação do plug-in da web usando o assistente



Para instalar o plug-in de gerenciamento do Kaspersky Endpoint Security manualmente a partir de um arquivo:

1. Baixe o arquivo com o plug-in da web na página de download do aplicativo, na seção Kaspersky Endpoint Security for Linux: **Plug-in do Controle de Aplicativos** → **Plug-in do Web Console**.

2. Descompacte o arquivo baixado localmente.

3. Na janela principal do Web Console, selecione **Configurações** → **Plug-ins da Web**.

   Isso abre a lista de plug-ins da web instalados.

4. Clique no botão **Adicionar do arquivo**.

5. Na janela exibida, insira o caminho para o arquivo plugin.zip e o caminho para o arquivo signature.txt.

   Esses arquivos estão na pasta em que você descompactou o arquivo que contém o plug-in da web.

6. Em seguida, clique no botão **Adicionar**.

7. Aguarde até que a instalação seja concluída e clique no botão **OK** na janela de informações.

O novo plug-in aparece na lista de plug-ins da web instalados (**Configurações** → **Plug-ins da Web**).

Vídeo: instalação do plug-in da web de gerenciamento em redes isoladas



4. Criação de uma política para o Kaspersky Endpoint Security for Linux sem herança de configurações

Ao usar o Kaspersky Endpoint Security for Linux com o Kaspersky Security Center Linux, é necessário configurar a política de acordo com as recomendações dos especialistas da Kaspersky.

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Selecione um grupo de administração para o Servidor de Administração.
3. Clique em **Adicionar**.

   O Assistente de nova política é iniciado.
4. Na janela exibida, selecione o aplicativo Kaspersky Endpoint Security for Linux na lista.
5. Especifique o **Modo Standard ou modo do Endpoint Detection and Response Agent** para o Kaspersky Endpoint Security for Linux.
6. Decida se deseja usar a Kaspersky Security Network.
7. Consulte as diretrizes de otimização para dispositivos gerenciados.
8. No nome da política, indique que ela pertence ao Servidor de Administração.
9. Desative a opção **Herdado da política principal**.
10. Salve as alterações.

Vídeo: criação de uma política



5. Criação de uma tarefa de grupo de atualização para o Kaspersky Endpoint Security for Linux

1. Na janela principal do Web Console, selecione a seção **Tarefas**.
2. Selecione um grupo de administração para o Servidor de Administração.
3. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.
4. Na janela exibida, selecione o aplicativo Kaspersky Endpoint Security for Linux na lista.
5. Especifique o tipo de tarefa *Atualização* e avance pelas próximas etapas sem alterar nenhuma configuração.

   Isso abre a janela de propriedades da tarefa.
6. Na seção **Configurações do aplicativo** → **Fontes de atualizações**, habilite a fonte Kaspersky Security Center e aumente sua prioridade.

Em uma rede isolada, use o Kaspersky Update Utility para criar um repositório para tarefas de atualização.

Vídeo: configurando as atualizações centralizadas do banco de dados



6. Adicionar uma chave de licença ao repositório do Servidor de Administração com distribuição automática

1. Na janela principal do Kaspersky Security Center Web Console, selecione a seção **Licenças**.
2. Clique em **Adicionar**.
3. Selecione a opção **Código de ativação** e clique em **Enviar**.

   Em uma rede isolada, use um arquivo de chave que pode ser solicitado por meio do serviço em https://keyfile.kaspersky.com/en.
4. Na lista de licenças, clique no nome da licença.
5. Marque a caixa de seleção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.
6. Salve as alterações.

Vídeo: ativando o aplicativo com um código de ativação



Vídeo: ativando o aplicativo com um arquivo de chave



7. Criar pacotes de instalação para o Agente de Rede e o Kaspersky Endpoint Security for Linux

1. Na janela principal do Web Console, selecione **Gerenciamento de software → Pacotes de instalação**.
2. Clique em **Adicionar**.

   O Assistente de novo pacote inicia.

3. Selecione **Criar um pacote de instalação para um aplicativo da Kaspersky**.

4. Na lista de aplicativos, localize a versão mais recente do Kaspersky Endpoint Security for Linux e clique no nome do aplicativo.

5. Na barra lateral, clique no botão **Baixar e criar o pacote de instalação** para iniciar o download.

   Leia e aceite os Contratos de Licença para começar a usar os aplicativos.

6. Retorne à lista de aplicativos e baixe a versão mais recente do Agente de Rede da Kaspersky para Linux.

   Leia e aceite os Contratos de Licença para começar a usar os aplicativos.

7. Na janela principal do Web Console, na lista de aplicativos baixados, clique nos nomes dos aplicativos.

Em uma rede isolada, baixe os pacotes de distribuição do site da Kaspersky e, no Assistente de novo pacote, selecione a opção **Criar um pacote de instalação a partir de um arquivo**.

Vídeo: criação automática de um pacote de instalação no Kaspersky Security Center



Vídeo: criação manual de um pacote de instalação a partir de um arquivo no Kaspersky Security Center



8. Instalação do Agente de Rede para Linux

1. Na janela principal do Web Console, selecione **Gerenciamento de software → Pacotes de instalação**.

2. Marque a caixa de seleção ao lado do pacote **Agente de Rede da Kaspersky para Linux**.

3. Clique em **Implantar**.

   O assistente de implementação da proteção é iniciado.

4. Selecione a opção **Usando um pacote autônomo**.

5. Na etapa **Mover dispositivos para a pasta Dispositivos gerenciados**, ignore a configuração das regras para mover dispositivos para um grupo de administração. Esta opção não se aplica ao dispositivo do Servidor de Administração.

6. Na etapa **Resultado da criação do pacote de instalação independente**, selecione e copie o caminho completo para o script de instalação do aplicativo.

7. Abra a linha de comando do sistema operacional do Servidor de Administração.

8. Inicie a instalação do pacote autônomo:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   onde `</var/opt/.../stand-alone_package_sh>` é o caminho completo, copiado anteriormente, para o arquivo de script do pacote de instalação independente.

   Se a instalação for bem-sucedida, uma notificação será exibida informando isso.

9. Mova o dispositivo do Servidor de Administração (por exemplo, *ksclinux*) do grupo **Dispositivos gerenciados** para o grupo de administração preparado anteriormente (por exemplo, *kscserver*).

9. Instalação do Kaspersky Endpoint Security for Linux

1. Na janela principal do Web Console, selecione **Gerenciamento de software → Pacotes de instalação**.

2. Marque a caixa de seleção do pacote do Kaspersky Endpoint Security for Linux.

3. Clique em **Implantar**.

   O assistente de implementação da proteção é iniciado.

4. Selecione a opção **Usando um pacote autônomo**.

5. Na etapa **Resultado da criação do pacote de instalação independente**, selecione e copie o caminho completo para o script de instalação do aplicativo.

6. Abra a linha de comando do sistema operacional do Servidor de Administração.

7. Inicie a instalação do pacote autônomo:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   onde `</var/opt/.../stand-alone_package_sh>` é o caminho completo, copiado anteriormente, para o arquivo de script do pacote de instalação independente.

   Se a instalação for bem-sucedida, uma notificação será exibida informando isso.

8. Na janela principal do Web Console, na seção **Tarefas**, selecione o nó raiz com o nome do Servidor de Administração na lista de grupos de administração.

9. Na lista de tarefas do Servidor de Administração, inicie as seguintes tarefas em sequência:
    - "Baixar atualizações no repositório do Servidor de Administração"
    - Atualização (Kaspersky Endpoint Security for Linux)
10. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Dispositivos gerenciados**.
11. Clique no nome do objeto de dispositivo do Servidor de Administração.
12. Verifique os valores dos principais indicadores do status do dispositivo:
    - Última atualização dos bancos de dados de antivírus (atualizados)
    - Conectado ao Servidor de Administração (atualizado)
    - Status da proteção (Em execução)
    - Evento *Chave adicionada com sucesso* (presente)

Siga o cenário de implementação do Kaspersky Endpoint Security for Linux para implementar o aplicativo nos dispositivos da sua rede.

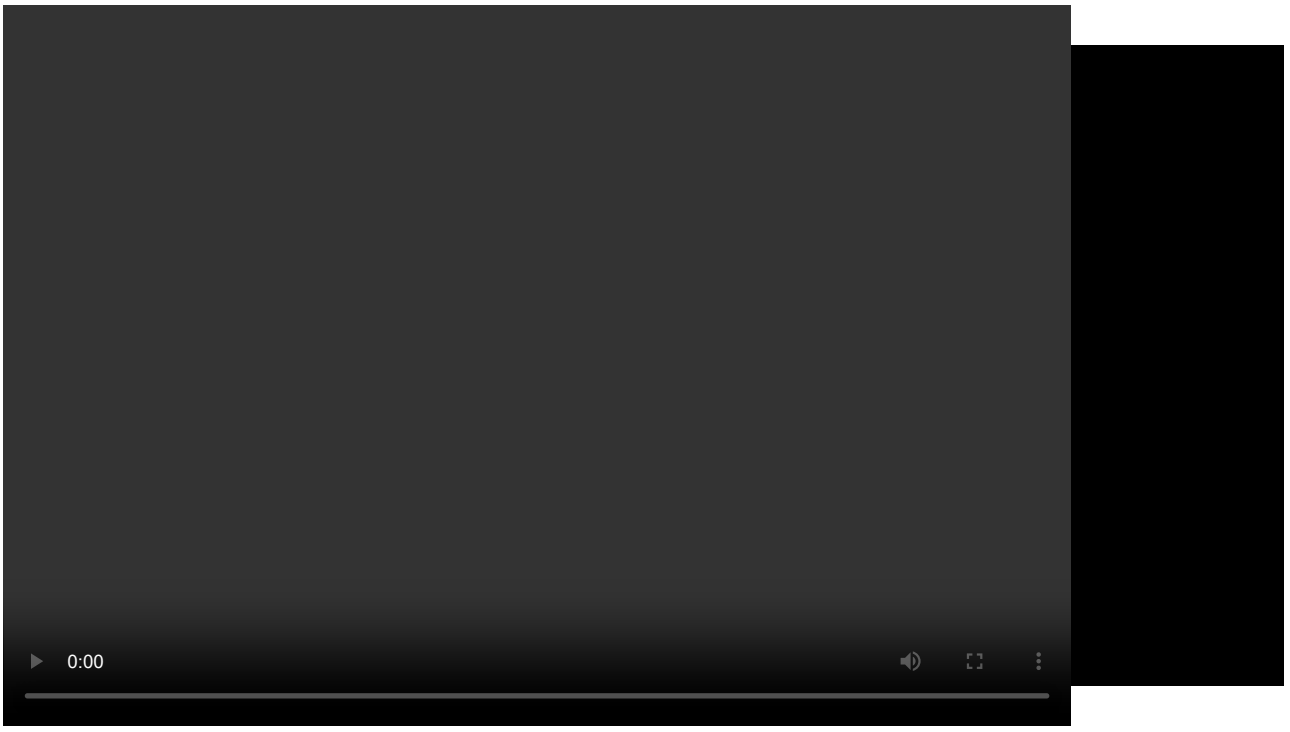
Tutorial em vídeo: Migração para o Kaspersky Security Center Linux utilizando o backup de dados do Servidor de Administração

Assista ao vídeo para saber como migrar os dados do Servidor de Administração do Kaspersky Security Center Windows para o Kaspersky Security Center Linux utilizando o backup de dados do Servidor de Administração (com o utilitário klbackup).

Para permitir a migração de dados para PostgreSQL ou Postgres Pro, solicite um dos seguintes patches ao Suporte Técnico da Kaspersky e instale-o:

- Para o Kaspersky Secure Mobility Management baseado no Kaspersky Security Center 14.2 Windows: 14.2.0.48079-pf5
- Para o Kaspersky Security Center 15.1 Windows: 15.1.0.20748-pf2

A migração de dados para PostgreSQL ou Postgres Pro também fica disponível após a atualização do Kaspersky Security Center Windows para a versão 15.1.0.22239.



Migração para o Kaspersky Security Center Linux utilizando o backup de dados do Servidor de Administração. Vídeo

Migração para o Kaspersky Security Center usando o Assistente de migração

Seguindo este cenário, é possível transferir a estrutura do grupo de administração, inclusive os dispositivos gerenciados e outros objetos de grupo (políticas, tarefas, tarefas globais, tags e seleções de dispositivos) do Kaspersky Security Center Windows sob o gerenciamento do Kaspersky Security Center Linux.

A migração de dados para o Kaspersky Security Center é possível com o Kaspersky Security Center Windows versão 15.1.0.22239 ou posterior.

Recursos do método de migração

- Migração parcial dos dados do Servidor de Administração
- A seleção de objetos para migração está disponível
- O grupo ou subgrupo de administração a ser migrado não pode conter mais de 10 mil dispositivos
- Usado para transferir parcialmente os dados do Servidor de Administração, incluindo apenas os objetos de grupo dentro do escopo de migração; objetos de grupo fora do escopo de migração devem ser restaurados manualmente

Escopo da migração

- Estrutura de grupos de administração
- Dispositivos gerenciados incluídos em grupos de administração (até 10 mil dispositivos)
- Tags atribuídas a dispositivos em migração

- Tarefas globais do Agente de Rede e de aplicativos gerenciados (não para o Servidor de Administração)
- Tarefas de grupo do Agente de Rede e de aplicativos gerenciados
- Políticas dos aplicativos gerenciados
- Modelos de relatório
- Função de usuário
- Usuários internos e grupos de segurança
- Categorias de aplicativos personalizados com conteúdo adicionado manualmente
- Seleções de dispositivos personalizados

Limitações:

- A migração só é possível do Kaspersky Security Center Windows versão 15.1 ou posterior para o Kaspersky Security Center Linux versão 15 ou posterior.
- Só é possível executar este cenário com o uso do Kaspersky Security Center Web Console.
- Os seguintes escopos não podem ser migrados:
  - Tarefas globais do Servidor de Administração
  - Eventos salvos no Servidor de Administração
  - Repositório dos pacotes de distribuição de aplicativos para instalação remota
  - Certificado do Servidor de Administração
  - Chaves de licença usadas pelo Servidor de Administração e aplicativos gerenciados
  - Servidores de Administração virtual
  - Configurações de política do Agente de Rede
  - Regras de migração de dispositivos
  - Regras para identificar dispositivos automaticamente
  - Pontos de distribuição
  - Configurações do aplicativo da Kaspersky salvas no Servidor de Administração

Antes de começar, saiba mais sobre os recursos e limitações do Kaspersky Security Center Linux:

- Diferenças funcionais entre o Kaspersky Security Center Windows e o Kaspersky Security Center Linux
- Lista de aplicativos e soluções Kaspersky compatíveis com o Kaspersky Security Center Linux

Fases

O cenário de migração continua em estágios:

1 Etapas preliminares

Esta etapa contém instruções para preparar um Servidor de Administração configurado anteriormente para a posterior migração para o novo Servidor de Administração do Kaspersky Security Center Linux. As etapas preliminares são as seguintes:

1. Verifique a versão do Servidor de Administração para criar uma cópia backup compatível com o Kaspersky Security Center Linux.

   Todas as versões atuais do **Kaspersky Security Center Linux** oferecem suporte à migração de dados durante a atualização para uma versão mais recente do aplicativo. As cópias backup só podem ser criadas e restauradas no mesmo tipo de SGBD.

   Para o **Kaspersky Security Center Windows**, verifique a versão do Servidor de Administração em **Propriedades** → **Geral** → **Versão**. Se a versão for anterior à 15.1.0.22239, atualize o Kaspersky Security Center Windows para a versão mais recente.

   Atualização do Kaspersky Security Center Windows para a versão mais recente

   1. From the Kaspersky website, download the distribution package corresponding to the localization language of your installed Administration Server: `Version 15.1.0.22239 | Windows | Full distributive`.

      The executable file is saved to your **Downloads** folder with the following name: `ksc_15.1_<build number>_full_<language>.exe`.

   2. Copie o pacote de distribuição para o Servidor de Administração.

   3. Run the `ksc_15.1_<build number>_full_<language>.exe` executable file as administrator.

   4. Na janela exibida, clique no link **Instalar o Kaspersky Security Center**.

      O Assistente de instalação do Servidor de Administração é iniciado.

   5. Leia o Contrato de Licença e a Política de Privacidade. Se você concordar com todos os termos e condições do Contrato de Licença de Usuário Final e da Política de Privacidade, marque as seguintes caixas de seleção em **Confirmo que li por completo, entendo e aceito os termos e condições dos seguintes**:

      - **Os termos e condições deste EULA**.
      - **Política de Privacidade que descreve o manuseio de dados**.

   6. Selecione **Efetuar upgrade do Servidor de Administração e do console baseado na Web (recomendado)** e avance para a próxima etapa.

   7. Crie uma nova cópia backup selecionando **Quero criar uma cópia backup dos dados** e concluindo o assistente de backup.

   8. Clique em **Efetuar upgrade**.

9. Durante a atualização, confirme todas as etapas do assistente de instalação do Web Console para atualizar a versão.

   O processo de atualização leva algum tempo. Após a conclusão do assistente de instalação, o Console de Administração pode não aceitar conexões até que o banco de dados seja inicializado.

10. Aguarde até que a atualização seja concluída.

2. Verifique se o certificado do Servidor de Administração está em conformidade.

   Antes de criar uma cópia backup, verifique se o certificado contém o Subject Alternative Name (SAN). Se não contiver, é importante substituir o certificado. Caso contrário, você não poderá fazer login no Web Console após restaurar uma cópia backup.

   Para verificar se o certificado inclui um Subject Alternative Name:

   - Para um dispositivo baseado em Windows:

     a. No Console de Administração, selecione o Servidor de Administração que deseja verificar.

     b. No menu de contexto, selecione **Propriedades → Geral → Exibir certificado do Servidor de Administração**.

     c. Na janela exibida, verifique o valor de **Subject Alternative Name**.

   - Para um dispositivo Linux, execute o seguinte comando:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   Verifique se o Subject Alternative Name contém o nome de domínio (DNS) do host do Servidor de Administração.

   Se o valor contiver apenas um endereço IP externo, sem um nome de domínio (DNS), ou estiver ausente, substitua manualmente o certificado por um que atenda aos requisitos para o funcionamento com o Kaspersky Security Center Linux. Substitua o certificado geral do Servidor de Administração usando o utilitário klsetsrvcert.

   Substituição do certificado geral do Servidor de Administração usando o utilitário klsetsrvcert

   1. Crie um novo certificado com uma data posterior para o início de seu uso nos dispositivos executando o seguinte comando:

      - Para o Kaspersky Security Center Windows:

        ```
        "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
        <oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      - Para o Kaspersky Security Center Linux:

        ```
        /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      em que `"<oldksc.example.internal>"` é o FQDN da conexão com o Servidor de Administração.

      > Não use um endereço IP para esse valor.

2. Defina a data de início do novo certificado em todos os hosts executando o seguinte comando:

   - Para o Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - Para o Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   em que a data `"DD-MM-YYYY hh:mm"` é pelo menos 30 dias posterior à data atual. Por padrão, o período de distribuição de um novo certificado (`CR`) é de 90 dias.

   > Quando chegar a data configurada, você precisará reinstalar o Web Console para restaurar o acesso a ele e atualizar seu certificado.

3. Se necessário, após a migração para um novo Servidor de Administração, execute o utilitário klmover para restaurar a conexão dos hosts com o Servidor de Administração. Talvez seja necessário executar o utilitário se o host tiver permanecido desligado durante todo o período de distribuição do certificado ou se não tiver se conectado ao Servidor de Administração.

2 Escolha um método de migração

É possível migrar para o Kaspersky Security Center Linux pelo assistente de migração. As etapas do assistente de migração dependem de os Servidores de Administração do Kaspersky Security Center Windows e do Kaspersky Security Center Linux estarem organizados em uma hierarquia:

- Migração com o uso de uma hierarquia de Servidores de Administração

  Escolha esta opção se o Servidor de Administração do Kaspersky Security Center Windows atuar como secundário para o Servidor de Administração do Kaspersky Security Center Linux. O processo de migração também é gerenciado e alterna entre servidores em uma única instância do Kaspersky Security Center Web Console. Caso prefira esta opção, é possível organizar os Servidores de Administração em uma hierarquia para simplificar o procedimento de migração. Para fazer isso, crie a hierarquia antes de iniciar a migração.

- Migração com o uso de um arquivo de exportação (arquivo ZIP)

  Escolha esta opção caso os Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux não estejam organizados em uma hierarquia. O processo de migração é gerenciado com duas instâncias do Kaspersky Security Center Web Console, uma instância para o Kaspersky Security Center Windows e outra para o Kaspersky Security Center Linux. Nesse caso, será necessário usar o arquivo de exportação criado e baixado durante a exportação do Kaspersky Security Center Windows e esse arquivo deverá ser importado para o Kaspersky Security Center Linux.

3 Faça backup do certificado e da chave privada do Servidor de Administração do Kaspersky Security Center Windows (etapa opcional)

É possível colocar os dispositivos gerenciados sob gerenciamento do Servidor de Administração do Kaspersky Security Center Linux ao restaurar o certificado e a chave privada do Servidor de Administração por meio de uma cópia de backup. Nesse caso, faça backup do certificado e da chave privada do Servidor de Administração do Kaspersky Security Center Windows. Em seguida, no estágio 7, você deve restaurar o certificado e a chave privada.

4 Exporte os dados do Kaspersky Security Center Windows

Abra o Kaspersky Security Center Windows e execute o Assistente de migração.

5 Importe os dados do Kaspersky Security Center Linux

Continue o assistente de migração para importar os dados exportados para o Kaspersky Security Center Linux. Caso os Servidores estejam organizados em uma hierarquia, a importação será iniciada automaticamente após uma exportação bem-sucedida dentro do mesmo assistente. Caso os Servidores não estejam organizados em uma hierarquia, o assistente de migração continua depois de alternar para o Kaspersky Security Center Linux.

6 Execute as ações adicionais para transferir manualmente objetos e configurações do Kaspersky Security Center Windows para o Kaspersky Security Center Linux (etapa opcional)

O usuário também poderá desejar transferir os objetos e configurações que não podem ser transferidos pelo assistente de migração. Por exemplo, também é possível fazer o seguinte:

- Transferir as chaves de licença usadas pelo Servidor de Administração e aplicativos gerenciados
- Configurar as tarefas globais do Servidor de Administração
- Definir as configurações de política do Agente de Rede
- Criar pacotes de instalação de aplicativos
- Criar Servidores virtuais
- Configurar regras para mover dispositivos
- Configurar as regras para identificar dispositivos automaticamente
- Criar categorias de aplicativos

- Atribuir e configurar pontos de distribuição

  Se o usuário mover um dispositivo que atua como um ponto de distribuição para outro Servidor de Administração, os dispositivos incluídos no escopo do ponto de distribuição não serão movidos automaticamente. É necessário mover cada dispositivo individualmente. Se um ponto de distribuição estiver atuando como gateway, será necessário executar o script `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` para que o ponto de distribuição não sirva mais como um gateway.

7 Mover os dispositivos gerenciados importados sob gerenciamento do Kaspersky Security Center Linux

Para concluir a migração e mover os dispositivos gerenciados e importados sob gerenciamento do Kaspersky Security Center Linux. É possível fazer isso usando um dos seguintes métodos:

- No utilitário klmover

  Use o utilitário klmover e especifique as configurações de conexão para o novo Servidor de Administração.

- Pela tarefa *Alterar o Servidor de Administração*

  Crie uma tarefa *Alterar o Servidor de Administração*, especifique os dispositivos gerenciados importados, o novo Servidor de Administração e outras configurações da tarefa. Em seguida, execute a tarefa para colocar os dispositivos gerenciados sob o gerenciamento do Servidor de Administração do Kaspersky Security Center Linux.

- Pela remoção (se já instalado) e posterior instalação do Agente de Rede nos dispositivos gerenciados

  Crie um novo pacote de instalação do Agente de Rede e especifique as configurações de conexão para o novo Servidor de Administração nas propriedades do pacote de instalação. Remova o Agente de Rede nos dispositivos gerenciados importados e use o pacote de instalação para instalar o Agente de Rede nos dispositivos gerenciados importados por meio de uma tarefa de instalação remota. Também é possível criar e usar um pacote de instalação independente para instalar localmente o Agente de Rede. Para obter mais informações, consulte Alternando de dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux.

- Por meio da restauração do certificado e da chave privada do Servidor de Administração de uma cópia de backup (apenas para migração para o Kaspersky Security Center Linux versão 15.1 ou posterior)

  Atribua ao dispositivo com o Servidor de Administração do Kaspersky Security Center Linux o mesmo endereço de rede que o Servidor de Administração do Kaspersky Security Center Windows. Para restaurar o certificado do Servidor de Administração e a chave privada da cópia backup salva no estágio 3, execute o utilitário klbackup com o parâmetro `-cert_only`. Na linha de comando, execute o seguinte comando: `/opt/kaspersky/ksc64/sbin/klbackup -path <caminho para a cópia de backup do certificado do Servidor de Administração> -restore -cert_only`.

8 Atualize o Agente de Rede para a versão mais recente

Atualize o Agente de Rede para Linux para a mesma versão do Kaspersky Security Center.

9. Verifique e confirme se os dispositivos gerenciados estão visíveis no novo Servidor de Administração

No Servidor de Administração Kaspersky Security Center Linux, abra a lista de dispositivos gerenciados (**Gerenciamento de ativos → Dispositivos gerenciados**) e verifique os valores nas colunas **Visível**, **Agente de Rede instalado** e as colunas **Última conexão com o Servidor de Administração**.

Outros métodos de migração de dados

Além do Assistente de migração, existem outros métodos para transferir seus objetos atuais, mas esses métodos permitem transferir somente políticas e tarefas:

- Exporte as tarefas do Kaspersky Security Center Windows e, em seguida, importe as tarefas para o Kaspersky Security Center Linux.
- Exporte as políticas específicas do Kaspersky Security Center Windows e, em seguida, importe as políticas no Kaspersky Security Center Linux. Os perfis de política relacionados são exportados e importados juntamente com as políticas selecionadas.

Exportação de objetos de grupo a partir do Kaspersky Security Center Windows

A migração da estrutura do grupo de administração, incluindo os dispositivos gerenciados e outros objetos de grupo, do Kaspersky Security Center Windows para o Kaspersky Security Center Linux requer, primeiramente, a seleção dos dados para exportação e criação de um arquivo de exportação. O arquivo de exportação contém informações sobre todos os objetos de grupo que deseja migrar. O arquivo de exportação será usado para a importação subsequente para o Kaspersky Security Center Linux.

É possível exportar os seguintes objetos:

- Tarefas e políticas de aplicativos gerenciados
- Tarefas globais
- Seleções de dispositivos personalizados
- Estrutura do grupo de administração e dispositivos incluídos
- Tags atribuídas aos dispositivos a serem migrados

Antes de iniciar a exportação, leia as informações gerais sobre a migração para o Kaspersky Security Center Linux. Escolha o método de migração com ou sem a hierarquia de Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux.

Para exportar os dispositivos gerenciados e objetos de grupo relacionados por meio do assistente de migração:

1. Dependendo se os Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux estiverem ou não organizados em uma hierarquia, siga um destes procedimentos:

   - Caso os servidores estejam organizados em uma hierarquia, abra o Kaspersky Security Center Web Console e alterne para o servidor do Kaspersky Security Center Windows.

   - Caso os servidores não estejam organizados em uma hierarquia, abra o Kaspersky Security Center Web Console conectado ao Kaspersky Security Center Windows.

2. No menu principal, vá para **Operações** → **Migração**.

3. Selecione **Migrar para o Kaspersky Security Center Linux ou Open Single Management Platform** para iniciar o assistente e seguir seus passos.

4. Selecione o grupo de administração ou o subgrupo para exportar. Certifique-se de que o grupo ou o subgrupo de administração selecionado não contenha mais de 10.000 dispositivos.

5. Selecione os aplicativos gerenciados cujas tarefas e políticas serão exportadas. Selecione apenas os aplicativos compatíveis com o Kaspersky Security Center Linux. Os objetos de aplicativos incompatíveis ainda serão exportados, mas não poderão ser operados.

6. Use os links à esquerda para selecionar as tarefas globais, as seleções de dispositivos e os relatórios a serem exportados. O link **Objetos do grupo** permite excluir da exportação funções personalizadas, usuários internos e grupos de segurança, bem como categorias de aplicativos personalizadas.

O arquivo de exportação (arquivo ZIP) é criado. Dependendo se a execução da migração é feita com suporte à hierarquia do Servidor de Administração ou não, o arquivo de exportação é salvo da seguinte forma:

- Caso os Servidores estejam organizados em uma hierarquia, o arquivo de exportação será salvo na pasta temporária no Kaspersky Security Center Web Console Server.

- Caso os Servidores não estejam organizados em uma hierarquia, o arquivo de exportação será baixado para o seu dispositivo.

Para migração com suporte à hierarquia do Servidor de Administração, a importação começa automaticamente após uma exportação bem-sucedida. Para migração sem suporte à hierarquia do Servidor de Administração, é possível importar manualmente o arquivo de exportação salvo para o Kaspersky Security Center Linux.

Importação do arquivo de exportação no Kaspersky Security Center Linux

Para transferir informações sobre dispositivos gerenciados, objetos e suas configurações exportadas do Kaspersky Security Center Windows, é necessário importá-las para o para o Kaspersky Security Center Linux ou Kaspersky Next XDR Expert.

Para importar os dispositivos gerenciados e objetos de grupo relacionados usando o assistente de migração:

1. Dependendo se os Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux estiverem ou não organizados em uma hierarquia, siga um destes procedimentos:

   - Caso os Servidores estejam organizados em uma hierarquia, prossiga para a próxima etapa do assistente de migração após a conclusão da exportação. A importação é iniciada automaticamente após uma exportação bem-sucedida dentro deste assistente (consulte a etapa 2 desta instrução).

   - Caso os Servidores não estejam organizados em uma hierarquia:

     a. Abra o aplicativo Kaspersky Security Center Web Console conectado ao Kaspersky Security Center Linux ou ao Kaspersky Next XDR Expert.

     b. No menu principal, vá para **Operações** → **Migração**.

     c. Selecione o arquivo de exportação (arquivo ZIP) criado e baixado durante a exportação do Kaspersky Security Center Windows. O upload do arquivo de exportação é iniciado.

2. Depois que o arquivo de exportação for carregado com êxito, será possível continuar a importação. Caso queira especificar outro arquivo de exportação, clique no link **Alterar** e selecione o arquivo desejado.

3. A hierarquia inteira de grupos de administração do Kaspersky Security Center Linux é exibida.

   Marque a caixa de seleção ao lado do grupo de administração de destino para o qual os objetos do grupo de administração exportado (dispositivos gerenciados, políticas, tarefas e outros objetos de grupo) devem ser restaurados.

4. A importação de objetos do grupo é iniciada. Não é possível minimizar o assistente de Migração nem executar nenhuma operação simultânea durante a importação. Aguarde até que os ícones de atualização (🔄) ao lado de todos os itens na lista de objetos sejam substituídos por marcas de seleção verdes (✓) e a importação será concluída.

5. Quando a importação for concluída, a estrutura exportada dos grupos de administração, inclusive os detalhes dos dispositivos, aparecerá no grupo de administração de destino selecionado. Se o nome do objeto restaurado for idêntico ao nome de um objeto existente, será adicionado ao objeto restaurado um sufixo incremental.

> Se em uma tarefa migrada os detalhes da conta sob a qual a tarefa é executada forem especificados, será necessário abrir a tarefa e inserir a senha novamente após a conclusão da importação.

Caso a importação tenha sido concluída com um erro, será possível executar uma das seguintes ações:

- Para a migração com suporte à hierarquia do Servidor de Administração, é possível começar a importar o arquivo de exportação novamente.

- Para a migração sem suporte à hierarquia do Servidor de Administração, é possível iniciar o assistente de migração para selecionar outro arquivo de exportação e importá-lo novamente.

É possível verificar se os objetos do grupo incluídos no escopo da exportação foram importados com êxito para o Kaspersky Security Center Linux. Para fazer isso, vá para a seção **Gerenciamento de ativos**, verifique e confirme se os objetos importados aparecem nas subseções correspondentes.

Observe que os dispositivos gerenciados importados são exibidos na subseção **Dispositivos gerenciados**, mas eles são invisíveis na rede e o Agente de Rede não está instalado e em execução neles (o valor *No* nas colunas **Visível**, **Agente de Rede instalado** e **Agente de Rede em execução**).

Para concluir a migração, é preciso mudar os dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux.

Alternância entre dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux

Após uma importação bem-sucedida das informações sobre os dispositivos gerenciados, objetos e suas configurações para o Kaspersky Security Center Linux, é preciso mudar os dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux para concluir a migração.

É possível migrar os dispositivos gerenciados para o Kaspersky Security Center Linux com o uso de um dos seguintes métodos:

- Uso do utilitário klmover.
- Com o uso da tarefa *alterar o Servidor de Administração*.
- Com a restauração do certificado e da chave privada do Servidor de Administração de uma cópia de backup (somente para migração para o Kaspersky Security Center Linux 15.1 ou posterior).

  Para obter detalhes, consulte a etapa "Mover os dispositivos gerenciados importados para serem gerenciados pelo Kaspersky Security Center Linux" no cenário principal de migração de dados.
- Instalação do Agente de Rede nos dispositivos gerenciados por meio de uma tarefa de instalação remota.

Para mudar os dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux pela instalação do Agente de Rede:

1. Remova o Agente de Rede nos dispositivos gerenciados importados que serão alternados sob o gerenciamento do Kaspersky Security Center Linux.
2. Mude para o Servidor de Administração do Kaspersky Security Center Windows.
3. Vá para **Gerenciamento de software** → **Pacotes de instalação** e abra as propriedades de um pacote de instalação existente do Agente de Rede.

   Caso o pacote de instalação do Agente de Rede esteja ausente na lista de pacotes, baixe um novo.

   Também é possível criar e usar um pacote de instalação independente para instalar localmente o Agente de Rede.
4. Na guia **Configurações**, selecione a seção **Conexão**. Especifique as configurações de conexão do Servidor de Administração do Kaspersky Security Center Linux.

5. Crie uma tarefa de instalação remota para os dispositivos gerenciados importados e especifique o pacote de instalação do Agente de Rede reconfigurado.

   É possível instalar o Agente de Rede por meio do Servidor de Administração do Kaspersky Security Center Windows ou por meio de um dispositivo baseado no Windows que atue como um ponto de distribuição. Caso use o Servidor de Administração, ative a opção **Usando recursos do sistema operacional através do Servidor de Administração**. Caso use um ponto de distribuição, ative a opção **Usando recursos do sistema operacional através de pontos de distribuição**.

6. Executar a tarefa de instalação remota.

Depois que a tarefa de instalação remota for concluída com êxito, vá para o Servidor de Administração do Kaspersky Security Center Linux, verifique e confirme se os dispositivos gerenciados estão visíveis na rede e se o Agente de Rede está instalado e sendo executado neles (o valor *Yes* nas colunas **Visível**, **Agente de Rede instalado** e **Agente de Rede em execução**).

Configurando o Servidor de Administração

Esta seção descreve o processo de configuração e as propriedades do Servidor de Administração.

Configuração do endereço de conexão do Servidor de Administração

O endereço de conexão do Servidor de Administração é o endereço de rede usado para os seguintes propósitos:

- Como um endereço padrão ao criar os pacotes de instalação do Agente de Rede

  Após a instalação do Agente de Rede, os dispositivos gerenciados se conectam ao Servidor de Administração neste endereço.

- Como o endereço de servidor proxy da KSN

  Os dispositivos gerenciados se conectam ao servidor proxy da KSN usando esse endereço.

Para configurar o endereço de conexão do Servidor de Administração:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Geral**.

3. Na janela aberta, no campo **Endereço de conexão do Servidor de Administração**, especifique o novo endereço de conexão do Servidor de Administração.

   O comprimento máximo do endereço de conexão é de 255 caracteres.

   Você pode especificar o endereço de conexão do Servidor de Administração como o nome NetBIOS, FQDN ou o endereço IP do Servidor de Administração.

4. Clique no botão **Salvar**.

O endereço especificado é usado como o endereço do Servidor de Administração e do servidor proxy da KSN.

Configuração da conexão do Kaspersky Security Center Web Console ao Servidor de Administração

É possível configurar a conexão do Kaspersky Security Center Web Console ao Servidor de Administração por meio das propriedades do Servidor de Administração ou por meio das configurações de política do Servidor de Administração.

Para definir as portas de conexão por meio das propriedades do Servidor de Administração:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Portas de conexão**.

3. Caso necessário, especifique a configuração da **Porta SSL para o Web Console** ou especifique outras portas de conexão do Servidor de Administração.

As principais configurações de conexão do Servidor selecionado são especificadas.

Para definir as portas de conexão por meio das configurações de política do Servidor de Administração:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.

2. Clique no nome da política do Servidor de Administração e vá para a guia **Configurações do aplicativo**.

3. Caso necessário, especifique a configuração da **Porta SSL para o Web Console** ou especifique outras portas de conexão do Servidor de Administração.

   Caso a opção **Abrir a porta para o Web Console** seja desativada e essa configuração de política seja aplicada ao dispositivo, não será possível se conectar ao Servidor de Administração com o uso do Kaspersky Security Center Web Console. Nesse caso, a conexão será encerrada. Se você tiver um Servidor de Administração no qual essa política não é aplicada, poderá se reconectar a esse Servidor de Administração por meio do Kaspersky Security Center Web Console.

As principais configurações de conexão do Servidor selecionado são especificadas.

Configuração de uma lista de permissão de endereços IP para conexão com o Kaspersky Security Center Linux

Por padrão, as conexões com o Kaspersky Security Center Linux são permitidas de qualquer dispositivo. Por exemplo, é possível instalar o Kaspersky Security Center Web Console Server em qualquer dispositivo que atenda aos requisitos e o Kaspersky Security Center Web Console Server se comunicará com o Kaspersky Security Center Linux. No entanto, só será possível configurar o Servidor de Administração para que as conexões sejam permitidas dos dispositivos com os endereços IP especificados. Nesse caso, se um invasor tentar se conectar ao Kaspersky Security Center Linux por meio do Kaspersky Security Center Web Console Server instalado em um dispositivo que não estiver incluído na lista de permissão, ele não conseguirá fazer login no Kaspersky Security Center Linux.

O endereço IP é verificado quando um usuário faz login no Kaspersky Security Center Linux ou executa um aplicativo que interage com o Servidor de Administração por meio da OpenAPI do Kaspersky Security Center Linux. Neste momento, um aplicativo no dispositivo tenta estabelecer uma conexão com o Servidor de Administração. Caso o endereço IP do dispositivo não esteja na lista de permissão, ocorrerá um erro de autenticação e o evento KLAUD_EV_SERVERCONNECT notifica que uma conexão com o Servidor de Administração não foi estabelecida.

Requisitos para uma lista de permissão de endereços IP

Os endereços IP são verificados apenas quando os seguintes aplicativos tentam se conectar ao Servidor de Administração:

- Kaspersky Security Center Web Console Server

  Caso entre no Kaspersky Security Center Linux pelo Kaspersky Security Center Web Console, será possível configurar um firewall no dispositivo no qual o Kaspersky Security Center Web Console Server está instalado com o uso dos meios padrão do sistema operacional. Então, caso alguém tente fazer login no Kaspersky Security Center Linux em um dispositivo e o Kaspersky Security Center Web Console Server seja instalado em outro dispositivo, um firewall ajudará a evitar a interferência de invasores.

- Aplicativos com interação com o Servidor de Administração por meio de objetos de automação klakaut

- Aplicativos que interagem com o Servidor de Administração via OpenAPI, como Kaspersky Anti Targeted Attack Platform ou Kaspersky Security for Virtualization

Portanto, especifique os endereços dos dispositivos nos quais os aplicativos listados acima estão instalados.

É possível definir os endereços IPv4 e IPv6. Não é possível especificar os intervalos de endereços IP.

Como estabelecer uma lista de permissão de endereços IP

Caso não tenha definido uma lista de permissão anteriormente, siga as instruções abaixo.

Para estabelecer uma lista de permissão de endereços IP para fazer login no Kaspersky Security Center Linux:

1. No dispositivo do Servidor de Administração, execute o prompt de comando do Windows em uma conta com direitos de administrador.

2. Altere o diretório atual para a pasta de instalação do Kaspersky Security Center Linux (geralmente, /opt/kaspersky/ksc64/sbin).

3. Digite o seguinte comando na conta root:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s`

   Especifique os endereços IP que atendem aos requisitos listados acima. Muitos endereços IP devem ser separados por um ponto e vírgula.

   Exemplo de como permitir que apenas um dispositivo se conecte ao Servidor de Administração:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Exemplo de como permitir que vários dispositivos se conectem ao Servidor de Administração:

   `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. Reinicie o serviço do Servidor de Administração.

É possível descobrir se a lista de permissão de endereços IP no Log de Eventos do Syslog do Servidor de Administração foi configurada com êxito.

Como alterar uma lista de permissão de endereços IP

É possível alterar uma lista de permissão exatamente como foi feito na primeira vez. Para isso, execute o mesmo comando e especifique uma nova lista de permissão:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP
addresses>" -t s
```

Caso queira excluir alguns endereços IP da lista de permissão, basta reescrevê-los. Por exemplo, a lista de permissão inclui os seguintes endereços IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. O usuário deseja excluir o endereço IP 198.51.100.0. Para fazer isso Digite o seguinte comando no prompt de comando:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0;
203.0.113.0" -t s
```

Não se esqueça de reiniciar o serviço do Servidor de Administração.

Como redefinir uma lista de permissão de endereços IP configurada

Para redefinir uma lista de permissão de endereços IP já configurada:

1. Digite o seguinte comando no prompt de comando na conta root:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. Reinicie o serviço do Servidor de Administração.

Depois disso, os endereços IP não serão mais verificados.

Definição das configurações de acesso à Internet para o Servidor de Administração

É preciso configurar o acesso à Internet para usar a Kaspersky Security Network e baixar atualizações de bancos de dados de antivírus para o Kaspersky Security Center Linux e aplicativos Kaspersky gerenciados.

Para especificar as configurações de acesso à Internet para o Servidor de Administração:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurando acesso à internet**.

3. Ative a opção **Usar o servidor proxy** caso queira usar um servidor proxy para se conectar com a Internet. Caso essa opção esteja ativada, os campos estarão disponíveis para inserir as configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:

   Endereço do servidor proxy

   Endereço do servidor proxy usado para conexão do Kaspersky Security Center Linux à Internet.

Número da porta

Número da porta pela qual a conexão proxy do Kaspersky Security Center Linux será estabelecida.

Ignorar servidor proxy para endereços locais

Nenhum servidor proxy será usado para conectar-se aos dispositivos na rede local.

Autenticação do servidor proxy

Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

Este campo de entrada está disponível se a caixa de seleção **Usar o servidor proxy** estiver marcada.

Nome do usuário

Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

Senha

A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

Para ver a senha inserida, mantenha pressionado o botão **Mostrar** pelo tempo que você desejar.

Também é possível configurar o acesso à Internet usando o assistente de início rápido.

Hierarquia de Servidores de Administração

Algumas empresas cliente, por exemplo MSP, podem executar vários Servidores de Administração. Pode ser inconveniente administrar diversos Servidores de Administração separados, portanto uma hierarquia pode ser aplicada. Em uma hierarquia, um Servidor de Administração baseado em Linux pode funcionar tanto como um servidor primário quanto como um servidor secundário. O servidor primário baseado em Linux pode gerenciar servidores secundários baseados em Linux e em Windows. Um servidor principal baseado em Windows pode gerenciar um servidor secundário baseado em Linux.

Uma configuração de "principal / secundário" para dois Servidores de Administração fornece as seguintes opções:

- Um Servidor de Administração secundário herda as políticas, tarefas, funções de usuário e pacotes de instalação do Servidor de Administração principal, prevenindo assim a duplicação das configurações.
- As seleções de dispositivos no Servidor de Administração principal podem incluir dispositivos de Servidores de Administração secundários.
- Os Relatórios no Servidor de Administração principal podem conter dados (incluindo informações detalhadas) de Servidores de Administração secundários.
- Um Servidor de Administração principal pode ser usado como uma origem de atualizações para um Servidor de Administração secundário.

O Servidor de Administração principal somente recebe dados de Servidores de Administração secundários não virtuais dentro do escopo das opções listadas acima. Essa limitação não se aplica aos Servidores de Administração virtuais, que compartilham o banco de dados com seu Servidor de Administração principal.

A hierarquia de Servidores de Administração fornece suporte para o modo de multilocação. Este modo permite que um administrador principal gerencie de forma centralizada vários clientes de forma independente. Cada organização cliente ou escritório é isolado de outros e é referido como uma locação. É possível alocar vários dispositivos gerenciados junto com seus dados, configurações, políticas e tarefas associados a uma locação e configurar os direitos do usuário por locação.

Um Servidor de Administração principal, instalado na infraestrutura principal da organização, atua como uma locação principal. O Servidor de Administração principal permite que os Servidores de Administração secundários ou virtuais (suas locações isoladas) recebam e processem de forma independente seus próprios eventos e trabalhem com seus próprios recursos, serviços e configurações.

Um provedor de serviços que tem várias organizações clientes pode fornecer a funcionalidade do Kaspersky Security Center Linux, incluindo agregação de alertas e ações de resposta, para cada organização cliente de forma independente. Para conseguir isso, o provedor de serviços conecta Servidores de Administração secundários ou virtuais como locatários para cada organização cliente. O provedor de serviços fornece serviços por meio de equipe e recursos próprios.

Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário

Em uma hierarquia, um Servidor de Administração baseado em Linux pode funcionar tanto como um servidor primário quanto como um servidor secundário. O servidor primário baseado em Linux pode gerenciar servidores secundários baseados em Linux e em Windows. Um servidor principal baseado em Windows pode gerenciar um servidor secundário baseado em Linux.

Adição de Servidor de Administração secundário (executada no futuro Servidor de Administração principal)

Você pode adicionar um Servidor de Administração como um Servidor de Administração secundário, portanto, estabelecendo uma hierarquia "principal/secundário".

Para adicionar um Servidor de Administração secundário que está disponível para conexão por meio do Kaspersky Security Center Web Console:

1. Verifique se a porta 13000 do futuro Servidor de Administração principal está disponível.

   Essa porta será usada para a interação entre os Servidores de Administração principal e secundário após a criação da hierarquia.

2. Vá para as propriedades do futuro Servidor de Administração principal:

   a. No menu principal, selecione uma seção (exceto para **Marketplace**, **Navegação do console** e **Configurações**), e então, na parte superior da página, clique no botão **Mostrar a hierarquia**.

   b. No painel de navegação exibido, passe o cursor do mouse sobre o nome do Servidor de Administração desejado e clique no ícone de configurações (⚙).

      Como alternativa, é possível clicar no nome do Servidor de Administração e, depois que o nome for exibido no menu principal, clicar nele para abrir a janela de propriedades do servidor.

3. Na página de propriedades exibida, clique na guia **Servidores de Administração**.

4. Ative a caixa de seleção ao lado do nome do grupo de administração ao qual deseja adicionar o Servidor de Administração.

5. Na linha de menu, clique em **Conectar Servidor de Administração secundário**.

   O assistente para Adicionar Servidor de Administração secundário é iniciado. Prossiga pelo Assistente usando o botão **PRÓXIMO**.

6. Preencha os campos a seguir:

   Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ

   Selecione esta opção se o Servidor de Administração secundário estiver em uma zona desmilitarizada (DMZ).

   Caso esta opção seja selecionada, o Servidor de Administração principal inicia a conexão com o Servidor de Administração secundário. Caso contrário, o Servidor de Administração secundário inicia a conexão com o Servidor de Administração principal.

   Nome de exibição do Servidor secundário

   O nome designado para o Servidor de Administração secundário será exibido na hierarquia. Se desejar, você pode inserir o endereço IP como um nome ou pode usar um nome como "Servidor secundário para o grupo 1".

   Endereço do Servidor secundário

   Especifique o endereço IP ou o nome de domínio do Servidor de Administração secundário.

   Esse parâmetro será obrigatório se a opção **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ** estiver ativada.

   Porta SSL do servidor

   Especifique o número da porta SSL a ser usada para a interação entre os Servidores de Administração principal e secundário após a criação da hierarquia. O número da porta padrão é 13000.

   Porta API do servidor

   O número da porta que o Web Console usará para receber conexões do Servidor de Administração secundário por meio da OpenAPI. O número da porta padrão é 13299.

   Durante a criação da hierarquia, o Web Console se conecta ao futuro Servidor de Administração secundário, solicita as credenciais, recupera o certificado público e executa a configuração inicial.

   Depois que a hierarquia de Servidores de Administração for criada, a porta 13299 não será mais usada. Os Servidores de Administração interagirão pela porta 13000.

   Certificado do Servidor de Administração secundário

   Adicione um arquivo de certificado. Você pode carregar manualmente o certificado do seu dispositivo ou obtê-lo do Servidor de Administração secundário.

7. Especifique as configurações de conexão e autenticação:

   - Insira o endereço do futuro Servidor de Administração principal.

   - Selecione a opção **Usar o servidor proxy** se você usar um servidor proxy para se conectar ao Servidor de Administração secundário.

Nesta caixa, é preciso também especificar as seguintes configurações do servidor proxy:

- **Endereço do servidor proxy**
- **Nome do usuário**
- **Senha**

8. Insira as credenciais do usuário que possui direitos de acesso no futuro Servidor de Administração secundário.

O assistente é concluído, a conexão com o futuro Servidor secundário é estabelecida e a hierarquia "principal/secundário" é criada.

A conexão entre os Servidores de Administração principal e secundário é estabelecida pela porta 13000. As tarefas e as políticas do Servidor de Administração principal são recebidas e aplicadas. O Servidor de Administração secundário é exibido no Servidor de Administração principal, no grupo de administração ao qual foi adicionado.

A conexão falha nos seguintes casos:

- As configurações de conexão estão incorretas.

  Você precisa verificar as configurações ou especificar manualmente o certificado do futuro Servidor secundário.

- O futuro Servidor secundário é autenticado com um certificado autoassinado gerado automaticamente pelo Kaspersky Security Center Linux. Como resultado, o navegador pode bloquear o download do certificado autoassinado.

  Você pode realizar uma das seguintes ações:

  - Para o futuro Servidor secundário, crie um certificado confiável na infraestrutura e que atenda aos requisitos para certificados personalizados.
  - Adicione o certificado autoassinado do futuro Servidor secundário à lista de certificados de navegador confiáveis. Recomendamos usar essa opção somente se não puder criar um certificado personalizado. Para obter informações sobre como adicionar um certificado à lista de certificados confiáveis, consulte a documentação do seu navegador.

Adição de Servidor de Administração secundário (executada no futuro Servidor de Administração principal)

Se não se conseguir conectar ao futuro Servidor de Administração secundário (por exemplo, porque estava temporariamente desconectado ou indisponível ou porque o arquivo do certificado do Servidor de Administração secundário está autoassinado), ainda é possível adicionar um Servidor de Administração secundário.

Para adicionar como secundário um Servidor de Administração que não está disponível para a conexão através do Kaspersky Security Center Web Console:

1. Envie o arquivo de certificado do futuro Servidor de Administração principal para o administrador do sistema do escritório onde o futuro Servidor de Administração secundário está localizado. (Você pode, por exemplo, gravar o arquivo em um dispositivo externo, como um pendrive, ou enviá-lo por e-mail.)

   O arquivo de certificado está localizado no futuro servidor de Administração principal, em /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Solicita que administrador de sistema responsável pelo futuro Servidor de Administração secundário faça o seguinte:

   a. Clique no nome do Servidor de Administração.

   b. Na página de propriedades que se abre, prossiga para a seção **Hierarquia de Servidores de Administração** da guia **Geral**.

   c. Selecione a opção **Esse Servidor de Administração é secundário na hierarquia**.

   d. Selecione o tipo de Servidor de Administração principal.

   e. No campo **Endereço do Servidor de Administração principal**, insira o nome da rede do Servidor de Administração principal futuro.

   f. Selecione o arquivo salvo anteriormente que contém o certificado do futuro Servidor de Administração principal clicando em **Especifique o certificado do Servidor de Administração principal**.

   g. Se necessário, marque a caixa de seleção **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ**.

   h. Caso a conexão ao futuro Servidor de Administração principal seja executada por meio de um servidor proxy, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão.

   i. Clique no botão **Salvar**.

A hierarquia "principal/secundário" é construída. O Servidor de Administração principal começa a receber a conexão do Servidor de Administração secundário usando a porta 13000. As tarefas e as políticas do Servidor de Administração principal são recebidas e aplicadas. O Servidor de Administração secundário é exibido no Servidor de Administração principal, no grupo de administração ao qual foi adicionado.

Visualizar a lista de Servidores de administração secundários

Para visualizar a lista de Servidores de administração secundários (incluindo virtuais):

1. No menu principal, selecione uma seção (com exceção de **Marketplace**, **Navegação do console** e **Configurações**).

2. Na parte superior da página, clique no botão **Mostrar a hierarquia**.

No painel de navegação que é aberto, a lista dos Servidores de Administração secundários (incluindo virtuais) é exibida. Você pode prosseguir para qualquer um desses Servidores de Administração clicando no nome.

Você não poderá prosseguir para os Servidores de Administração virtuais se tiver aberto o painel de navegação pelas seções **Intervalos de IPs** e **Objetos excluídos**.
Os grupos de administração também são exibidos. Os grupos estarão disponíveis para gerenciamento se você tiver aberto o painel de navegação pelas seguintes seções: **Dispositivos gerenciados**, **Políticas**, **Tarefas** e **Pontos de distribuição**. Caso contrário, os grupos estarão esmaecidos.

Se você estiver conectado ao seu Servidor de Administração principal no Kaspersky Security Center Web Console e não puder se conectar a um Servidor de Administração virtual gerenciado por um Servidor de Administração secundário, poderá usar uma das seguintes formas:

- **Modifique a instalação existente do Kaspersky Security Center Web Console para adicionar o Servidor secundário à lista de Servidores de Administração confiáveis.** Depois disso, você poderá se conectar ao Servidor de Administração virtual no Kaspersky Security Center Web Console.

  1. No dispositivo no qual o Kaspersky Security Center Web Console está instalado, execute o arquivo de instalação que correspondente à distribuição do Linux instalada em seu dispositivo. Faça o procedimento com uma conta com privilégios administrativos.

     O Assistente de Instalação será iniciado. Navegue pelo assistente usando o botão **Avançar**.

  2. Selecione a opção **Atualizar**.

  3. Na etapa **Tipo de modificação**, selecione a opção **Editar as configurações de conexão**.

  4. Na etapa **Servidores de Administração confiáveis**, adicione o Servidor de Administração secundário necessário.

  5. Na última etapa, clique em **Modificar** para aplicar as novas configurações.

  6. Após a conclusão com êxito da reconfiguração do aplicativo, clique no botão **Concluir**.

- Use o Kaspersky Security Center Web Console para conectar-se diretamente ao Servidor de Administração secundário em que o servidor virtual foi criado. Em seguida, você poderá trocar o Servidor de Administração virtual no Kaspersky Security Center Web Console.

Gerenciar Servidores de Administração virtuais

Esta seção descreve as seguintes ações para gerenciar Servidores de Administração virtuais:

- Criar Servidores de Administração virtuais
- Ativar ou desativar de Servidores de Administração virtuais
- Atribuir um administrador para um Servidor de Administração virtual
- Alterar o Servidor de Administração para dispositivos cliente
- Excluir Servidores de Administração virtuais

Criar um Servidor de Administração virtual

Você pode criar Servidores de Administração virtuais e adicioná-los a grupos de administração.

Quando um Servidor de Administração virtual é criado, ele herda a lista de usuários e todos os direitos de usuário do Servidor de Administração principal. Caso um usuário tenha direitos de acesso ao servidor principal, esse usuário também terá direitos de acesso ao servidor virtual. Após a criação, é necessário configurar os direitos de acesso para os Servidores de maneira independente.

Para criar e adicionar um Servidor de Administração virtual:

1. No menu principal, clique no nome do Servidor de Administração.
2. Na página que se abre, prossiga para a guia **Servidores de Administração**.
3. Selecione o grupo de administração ao qual você deseja adicionar um Servidor de Administração virtual.
   O Servidor de Administração virtual gerenciará os dispositivos do grupo selecionado (incluindo os subgrupos).
4. Na linha de menu, clique em **Novo Servidor de Administração virtual**.
5. Na página que se abre, defina as propriedades do novo Servidor de Administração virtual:
   - **Nome do Servidor de Administração virtual**.
   - **Endereço de conexão do Servidor de Administração**.
     É possível especificar o nome ou o endereço IP do Servidor de Administração.
6. Na lista de usuários, selecione o administrador do Servidor de Administração virtual. Se quiser, você poderá editar uma das contas existentes antes de atribuir a ela a função de administrador ou criar uma nova conta de usuário.
   Se necessário, é possível criar uma nova conta que atuará como gerente do Servidor de Administração virtual usando o utilitário kladduser. Para fazer isso, use o seguinte comando:

   ```
   kladduser -n <user_name> -p <password> -vs <virtual_server_name>
   ```

   em que virtual_server_name é o nome do Servidor de Administração virtual.
7. Clique no botão **Salvar**.

O novo Servidor de Administração virtual é criado, adicionado ao grupo de administração e exibido na guia **Servidores de Administração**.

Se você estiver conectado ao seu Servidor de Administração principal no Kaspersky Security Center Web Console e não puder se conectar a um Servidor de Administração virtual gerenciado por um Servidor de Administração secundário, poderá usar uma das seguintes formas:

- **Modifique a instalação existente do Kaspersky Security Center Web Console para adicionar o Servidor secundário à lista de Servidores de Administração confiáveis.** Depois disso, você poderá se conectar ao Servidor de Administração virtual no Kaspersky Security Center Web Console.
  1. No dispositivo no qual o Kaspersky Security Center Web Console está instalado, execute o arquivo de instalação que correspondente à distribuição do Linux instalada em seu dispositivo. Faça o procedimento com uma conta com privilégios administrativos.
     O Assistente de Instalação será iniciado. Navegue pelo assistente usando o botão **Avançar**.
  2. Selecione a opção **Atualizar**.
  3. Na etapa **Tipo de modificação**, selecione a opção **Editar as configurações de conexão**.
  4. Na etapa **Servidores de Administração confiáveis**, adicione o Servidor de Administração secundário necessário.

5. Na última etapa, clique em **Modificar** para aplicar as novas configurações.

6. Após a conclusão com êxito da reconfiguração do aplicativo, clique no botão **Concluir**.

- Use o Kaspersky Security Center Web Console para conectar-se diretamente ao Servidor de Administração secundário em que o servidor virtual foi criado. Em seguida, você poderá trocar o Servidor de Administração virtual no Kaspersky Security Center Web Console.

Ativando ou desativando um Servidor de Administração virtual

Ao criar um novo Servidor de Administração virtual, ele é ativado por padrão. Você pode desativá-lo ou ativá-lo novamente a qualquer momento. Desativar ou ativar um Servidor de Administração virtual é igual a desligar ou ligar um Servidor de Administração físico.

Para ativar ou desativar um Servidor de Administração virtual:

1. No menu principal, clique no nome do Servidor de Administração.

2. Na página que se abre, prossiga para a guia **Servidores de Administração**.

3. Selecione o Servidor de Administração virtual que deseja ativar ou desativar.

4. Na linha do menu, clique no botão **Ativar/desativar Servidor de Administração virtual**.

O estado do Servidor de Administração virtual é alterado para ativado ou desativado, dependendo da condição anterior. O estado atualizado é exibido próximo ao nome do Servidor de Administração.

Atribuição de um administrador para um Servidor de Administração virtual

Ao usar Servidores de Administração virtuais em sua organização, convém atribuir um administrador dedicado para cada Servidor de Administração virtual. Por exemplo, isso pode ser útil quando os Servidores de Administração virtuais são criados para gerenciar escritórios ou departamentos separados de sua organização, ou se você for um provedor de MSP e gerenciar locatários por meio de Servidores de Administração virtuais.

Quando um Servidor de Administração virtual é criado, ele herda a lista de usuários e todos os direitos de usuário do Servidor de Administração principal. Caso um usuário tenha direitos de acesso ao servidor principal, esse usuário também terá direitos de acesso ao servidor virtual. Após a criação, é preciso configurar os direitos de acesso aos Servidores de forma independente. Caso queira apenas atribuir um administrador para um Servidor de Administração virtual, verifique e confirme se o administrador não tem os direitos de acesso no Servidor de Administração principal.

É possível atribuir um administrador para um Servidor de Administração virtual concedendo os direitos de acesso de administrador ao Servidor de Administração virtual. É possível conceder os direitos de acesso necessários das seguintes formas:

- Configure os direitos de acesso para o administrador manualmente

- Atribua uma ou mais funções de usuário ao administrador

Para entrar no Kaspersky Security Center Web Console, um administrador de um Servidor de Administração virtual especifica nome, nome de usuário e senha do Servidor de Administração virtual. O Kaspersky Security Center Web Console autentica o administrador e abre o Servidor de Administração virtual ao qual o administrador tem direitos de acesso. O administrador não pode alternar entre os Servidores de Administração.

Pré-requisitos

Antes de iniciar, certifique-se de que as seguintes condições sejam atendidas:

- O Servidor de Administração virtual foi criado.
- No Servidor de Administração principal, o usuário criou uma conta para o administrador ao qual ele deseja atribuir o Servidor de Administração virtual.
- O usuário tem o direto de **Modificar os objetos ACLs** na área funcional **Recursos gerais** → **Permissões do usuário**.

Configuração dos direitos de acesso manualmente

Para atribuir um administrador para um Servidor de Administração virtual:

1. Alterne para o Servidor de Administração virtual desejado:
   a. No menu principal, selecione uma seção (exceto para **Marketplace**, **Navegação do console** e **Configurações**), e então, na parte superior da página, clique no botão **Mostrar a hierarquia**.
   b. No painel de navegação exibido, clique no nome do Servidor de Administração virtual desejado.

      > Não é possível alternar para um Servidor de Administração virtual por meio das seções **Intervalos de IPs** e **Objetos excluídos**.

      No menu principal, o Servidor de Administração muda para aquele selecionado.
2. Vá para as propriedades do Servidor de Administração clicando no nome dele no menu principal.

   Como alternativa, no painel de navegação, passe o cursor do mouse sobre o nome do Servidor de Administração virtual desejado e clique no ícone de configurações (⚙).

   A janela Propriedades do Servidor de Administração é aberta.
3. Na guia **Direitos de acesso**, clique no botão **Adicionar**.

   Uma lista unificada de usuários do Servidor de Administração principal e do Servidor de Administração virtual atual é aberta.
4. Na lista de usuários, selecione a conta do administrador que deseja atribuir ao Servidor de Administração virtual e clique no botão **OK**.

   O aplicativo adiciona o usuário selecionado à lista de usuários na aba **Direitos de acesso**.
5. Marque a caixa de seleção ao lado de conta adicionada e clique no botão **Direitos de acesso**.

6. Configure os direitos que o administrador terá no Servidor de Administração virtual.

   Para uma autenticação bem-sucedida, no mínimo, o administrador deve ter os seguintes direitos:

   - Direito de **Ler** na área funcional **Recursos gerais → Funcionalidade básica**
   - Direito de **Ler** na área funcional **Recursos gerais → Servidores de Administração virtuais**

O aplicativo salva os direitos de usuário modificados na conta do administrador.

Para atribuir um administrador para vários Servidores de Administração virtuais:

1. No menu principal, clique no nome do Servidor de Administração principal.
2. Na página exibida, acesse a guia **Direitos de acesso** e clique em **Atribuir**.

   Na janela **Adicionar usuários ou grupos** exibida, marque a caixa de seleção próxima ao usuário que se deseja atribuir como administrador.
3. É possível alternar para a guia **Grupos** para selecionar os grupos de usuários.
4. Clique em **Avançar**.
5. Selecione os servidores aos quais você deseja atribuir um administrador e clique em **Avançar**.
6. Selecione as funções de administrador que você deseja definir para o usuário, se necessário.

   Se você quiser definir funções personalizadas para o usuário no Servidor de Administração atual, acesse as propriedades do Servidor de Administração necessário, clique em **Definir funções** e selecione as funções personalizadas.
7. Clique em **Finalizar** para aplicar as alterações.

Agora, o administrador com as funções selecionadas está atribuído a vários Servidores de Administração virtuais.

Para revogar os direitos de acesso do administrador:

1. Mude para o Servidor de Administração desejado.
2. No menu principal, clique no nome do Servidor de Administração.
3. Na página exibida, prossiga para a guia **Direitos de acesso**.
4. Marque a caixa de seleção ao lado do usuário cujos direitos de acesso deseja revogar.
5. Clique em **Revogar** e confirme sua ação.

Os direitos de acesso do usuário selecionado foram revogados.

Configuração de direitos de acesso com a atribuição de uma função de usuário

Como alternativa, é possível conceder direitos de acesso a um administrador do Servidor de Administração virtual por meio de funções de usuário. Por exemplo, isso pode ser útil caso se queira atribuir vários administradores no mesmo Servidor de Administração virtual. Se esse for o caso, é possível atribuir às contas dos administradores a mesma função de usuário, em vez de configurar os mesmos direitos de usuário para vários administradores.

Para atribuir um administrador para um Servidor de Administração virtual por meio da atribuição da função de usuário:

1. No Servidor de Administração principal, crie uma nova função de usuário e especifique todos os direitos de acesso necessários que um administrador deve ter no Servidor de Administração virtual. É possível criar várias funções, por exemplo, caso queira separar o acesso a diferentes áreas funcionais.

2. Alterne para o Servidor de Administração virtual desejado:

   a. No menu principal, selecione uma seção (exceto para **Marketplace**, **Navegação do console** e **Configurações**), e então, na parte superior da página, clique no botão **Mostrar a hierarquia**.

   b. No painel de navegação exibido, clique no nome do Servidor de Administração virtual desejado.

   > Não é possível alternar para um Servidor de Administração virtual por meio das seções **Intervalos de IPs** e **Objetos excluídos**.

   No menu principal, o Servidor de Administração muda para aquele selecionado.

3. Atribuir a nova função ou diversas funções à conta de administrador.

   O aplicativo atribui as funções à conta de administrador.

Configuração de direitos de acesso no nível do objeto

Além de atribuir os direitos de acesso no nível de uma área funcional, é possível configurar o acesso a objetos específicos no Servidor de Administração virtual, por exemplo, para um grupo de administração específico ou uma tarefa. Para isso, alterne para o Servidor de Administração virtual e configure os direitos de acesso nas propriedades do objeto.

Alterar o Servidor de Administração para dispositivos cliente

É possível alterar o Servidor de Administração que gerencia os dispositivos cliente por outro, usando a tarefa *Alterar o Servidor de Administração*. Após a conclusão da tarefa, os dispositivos clientes selecionados serão colocados sob o gerenciamento do Servidor de Administração especificado por você.

> Não é possível usar a tarefa *Alterar o Servidor de Administração* para dispositivos cliente conectados ao Servidor de Administração por meio de gateways de conexão. Para esses dispositivos, é necessário reconfigurar o Agente de Rede ou reinstalar o Agente de Rede e especificar o gateway de conexão.

Para alterar o Servidor de Administração que gerencia dispositivos cliente para outro servidor:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na etapa **Novas configurações de tarefa** do assistente, especifique as seguintes configurações:

   a. Na lista suspensa **Aplicativo**, selecione **Kaspersky Security Center**.

   b. No campo **Tipo de tarefa**, selecione **Alterar o Servidor de Administração**.

   c. No campo **Nome da tarefa**, especifique o nome para a tarefa que vai criar.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).

   d. Selecione os dispositivos aos quais a tarefa será atribuída:

   Atribuir tarefa a um grupo de administração

   A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

   Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

   Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

   Especificar endereços de dispositivos manualmente ou importar endereços de uma lista

   Você pode especificar nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

   Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

   Atribuir tarefa a uma seleção de dispositivos

   A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

   Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.
4. Na etapa **Escopo da tarefa** do assistente, especifique um grupo de administração, dispositivos com endereços específicos ou uma seleção de dispositivos gerenciados.
5. Na próxima etapa do assistente, confirme que concorda com os termos de alteração do Servidor de Administração para dispositivos do cliente.
6. Na próxima etapa do assistente, selecione o Servidor de Administração que deseja usar para gerenciar os dispositivos selecionados:

   Mudar para outro Servidor de Administração principal

Para mover dispositivos cliente para outro Servidor de Administração principal, especifique as seguintes configurações de conexão do Servidor de Administração:

1. No campo **Endereço do Servidor de Administração**, especifique o endereço do novo Servidor de Administração principal.

2. No campo **Número da porta**, especifique o número da porta para conexão com o Servidor de Administração.

   O número da porta padrão é 14000.

3. No campo **Porta SSL**, especifique o número da porta SSL no Servidor de Administração principal.

   O número da porta padrão é 13000.

4. Se necessário, ative a opção **Usar o servidor proxy**.

   Se essa opção estiver desativada, a conexão direta será usada para conectar o dispositivo ao Servidor de Administração.

   Se essa opção estiver ativada, especifique os parâmetros do servidor proxy:

   - **Endereço do servidor proxy**
   - **Porta do servidor proxy**

   Se o servidor proxy exigir autenticação, nos campos **Nome do usuário** e **Senha**, especifique as credenciais da conta sob a qual a conexão com o servidor proxy será estabelecida. Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

5. Se necessário, carregue um novo certificado do Servidor de Administração.

Mudar para outro Servidor de Administração virtual neste Servidor principal

Selecione essa opção para mover dispositivos cliente para o Servidor de Administração virtual no Servidor de Administração principal atual. Para fazer isso, na lista suspensa **Nome do Servidor de Administração virtual**, selecione o Servidor de Administração virtual desejado.

7. Na etapa **Selecionar uma conta para executar a tarefa**, especifique as configurações da conta:

Conta padrão

A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

Por padrão, esta opção está selecionada.

Especificar conta

Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

Conta

Conta sob a qual a tarefa é executada.

Senha

Senha da conta sob a qual a tarefa será executada.

8. Se você quiser alterar as configurações padrão da tarefa, na etapa **Concluir a criação da tarefa** do assistente, ative a opção **Abrir detalhes da tarefa quando a criação for concluída**.

   Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode alterar as configurações padrão depois, a qualquer momento.

9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.

10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

11. Se você quiser alterar as configurações padrão da tarefa, na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com suas necessidades.

12. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

13. Execute a tarefa criada.

Após a conclusão da tarefa, os dispositivos cliente, para os quais a mesma foi criada, são colocados sob gerenciamento pelo Servidor de Administração especificado nas configurações da tarefa.

Excluindo um Servidor de Administração virtual

Ao excluir um Servidor de Administração virtual, todos os objetos criados no Servidor de Administração, incluindo políticas e tarefas, também são excluídos. Os dispositivos gerenciados dos grupos de administração gerenciados pelo Servidor de Administração virtual serão removidos dos grupos de administração. Para retornar os dispositivos sob gerenciamento do Kaspersky Security Center Linux, execute a sondagem de rede e migre os dispositivos encontrados do grupo Dispositivos não atribuídos para os grupos de administração.

Para excluir um Servidor de Administração virtual:

1. Alterne para o Servidor de Administração físico principal ao qual pertence o Servidor de Administração virtual que será excluído:

   a. No menu principal, selecione qualquer seção (exceto para **Marketplace**, **Navegação do console** e **Configurações**), e então, na parte superior da página, clique no botão **Mostrar a hierarquia**.

   b. No painel de navegação que é aberto, clique no nome do Servidor de Administração físico principal.

      No menu principal, o Servidor de Administração muda para aquele selecionado.

2. Acesse as propriedades do Servidor de Administração físico principal por um dos seguintes métodos:

   - no painel de navegação, posicione o cursor do mouse sobre o nome do Servidor de Administração desejado e, em seguida, clique no ícone de configurações (⚙).

   - No menu principal, clique no nome do Servidor de Administração.

3. Na página de propriedades exibida, vá para a guia **Servidores de Administração**.

4. Selecione o Servidor de Administração virtual que deseja excluir.

5. Na linha do menu, clique no botão **Excluir**.

O Servidor de Administração virtual é excluído.

Configuração do registro em log de eventos de conexão do Servidor de Administração

O histórico das conexões e tentativas de conexão ao Servidor de Administração durante a operação pode ser salvo em um arquivo de registro. As informações no arquivo permitem que você rastreie não só as conexões dentro sua infraestrutura de rede, mas também as tentativas não autorizadas de acessar o servidor.

Para registrar eventos da conexão ao Servidor de Administração:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Portas de conexão**.

3. Ative a opção **Criar log de eventos de conexão do Servidor de Administração**.

Todos os eventos adicionais das conexões de entrada com o Servidor de Administração, resultados de autenticação e erros de SSL serão salvos no arquivo /var/opt/kaspersky/klnagent_srv/logs/SC.syslog.

Configuração do número máximo de eventos no repositório de eventos

Na seção **Repositório de eventos** da janela Propriedades do Servidor de Administração, você pode editar as configurações de armazenamento do evento no banco de dados do Servidor de Administração ao limitar o número de registros de evento ou o tempo de armazenamento do registro. Quando você especifica o número máximo de eventos, o aplicativo calcula um volume aproximado do espaço de armazenamento necessário para o número especificado. Você pode usar esse cálculo aproximado para avaliar se você tem espaço livre suficiente no disco para evitar sobrecarga do banco de dados. A capacidade padrão do banco de dados do Servidor de Administração é de 400.000 eventos. A capacidade máxima recomendada do banco de dados é de 45 milhões de eventos.

O aplicativo verifica o banco de dados a cada 10 minutos. Caso o número de eventos atinja o valor máximo especificado em mais de 10.000, o aplicativo exclui os eventos mais antigos para que apenas o número máximo de eventos especificado permaneça.

Quando o Servidor de Administração exclui eventos antigos, não pode salvar novos eventos no banco de dados. Durante esse período, as informações sobre eventos rejeitados são gravadas no log do sistema operacional. Os novos eventos são colocados em fila e salvos no banco de dados depois que a operação de exclusão é concluída. Por padrão, a fila de eventos é limitada a 20 mil eventos. É possível personalizar o limite da fila ao editar o valor do sinalizador KLEVP_MAX_POSTPONED_CNT.

Para limitar o número de eventos que podem ser armazenados no repositório de eventos no Servidor de Administração:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Repositório de eventos**. Especifique o número máximo de eventos armazenados no banco de dados.

3. Clique no botão **Salvar**.

Você também pode fazer o seguinte:

- Alterar as configurações de qualquer tarefa para salvar eventos relacionados ao andamento da tarefa ou salvar apenas os resultados de execução da tarefa.

- Reduzir ou desabilitar o período de armazenamento para os eventos do Servidor de Administração, Agente de Rede e aplicativos da Kaspersky instalados em dispositivos gerenciados.

Ao fazer isso, você reduzirá o número de eventos no banco de dados, aumentará a velocidade da execução dos cenários associados com a análise da tabela de eventos no banco de dados e abaixará o risco de que os eventos críticos sejam substituídos por um grande número de eventos.

Mover Servidor de Administração para outro dispositivo

Se precisar usar o Servidor de Administração em um novo dispositivo, poderá movê-lo de uma das seguintes maneiras:

- Mova o Servidor de Administração e o servidor de banco de dados para um novo dispositivo (o servidor de banco de dados pode ser instalado no novo dispositivo juntamente com o Servidor de Administração ou em outro dispositivo).

- Mantenha o servidor de banco de dados no dispositivo anterior e mova apenas o Servidor de Administração para um novo dispositivo.

Para mover o Servidor de Administração e um servidor de banco de dados para um novo dispositivo:

1. No dispositivo anterior, crie um backup de dados do Servidor de Administração.

   Para fazer isso, você pode executar a tarefa de backup de dados por meio do Kaspersky Security Center Web Console ou executar o utilitário klbackup.

2. No dispositivo anterior, desconecte o Servidor de Administração da rede.

3. Selecione um novo dispositivo no qual instalar o Servidor de Administração. Certifique-se de que o hardware e o software do dispositivo selecionado atendam aos requisitos para Servidor de Administração, Kaspersky Security Center Web Console e Agente de Rede. Verifique também se as portas usadas no Servidor de Administração estão disponíveis.

4. Atribua o mesmo endereço ao novo dispositivo.

   O novo Servidor de Administração pode ser atribuído ao nome NetBIOS, FQDN e endereço IP estático. Isso depende de qual endereço do Servidor de Administração foi definido no pacote de instalação do Agente de Rede quando os Agentes de Rede foram implementados. Como alternativa, é possível usar o endereço de conexão que determina o Servidor de Administração ao qual o Agente de Rede se conecta (esse endereço pode ser obtido em dispositivos gerenciados usando o utilitário klnagchk).

5. Caso necessário, em outro dispositivo, instale o sistema de gerenciamento de banco de dados (DBMS) a ser usado pelo Servidor de Administração.

   O banco de dados pode ser instalado no novo dispositivo juntamente com o Servidor de Administração ou em outro dispositivo. Verifique e confirme se este dispositivo atende aos requisitos de hardware e software. Ao selecionar um DBMS, considere o número de dispositivos cobertos pelo Servidor de Administração.

6. Instale o Servidor de Administração no novo dispositivo.

   Observe que, se o servidor de banco de dados for movido para outro dispositivo, especifique o endereço local como o endereço IP do dispositivo no qual o banco de dados estiver instalado (o item "h" na instrução Instalação do Kaspersky Security Center Linux). Se precisar manter o servidor de banco de dados no dispositivo anterior, digite o endereço IP do dispositivo anterior no item "h" das instruções de Instalação do Kaspersky Security Center Linux.

7. Após a conclusão da instalação, recupere os dados do Servidor de Administração no novo dispositivo usando o utilitário klbackup.

8. Abra o Kaspersky Security Center Web Console e conecte-se ao Servidor de Administração.

9. Verifique se todos os dispositivos gerenciados estão conectados com o Servidor de Administração.

10. Desinstale o Servidor de Administração e o servidor de banco de dados do dispositivo anterior.

Alteração do nome do Servidor de Administração

As etapas para alterar o nome do servidor podem variar dependendo do ambiente. Você pode escolher um dos seguintes cenários para alterar o nome do servidor:

- Preservação das conexões pela adição de um novo registro DNS.
- Preservação das conexões pela mudança para conectividade baseada em endereço IP.
- Restauração de conexões interrompidas após a alteração do nome do servidor.

Se você tiver dificuldade para alterar o nome do servidor, entre em contato com o Suporte Técnico.

Preservação das conexões pela adição de um novo registro DNS

Neste cenário, os dispositivos gerenciados e o Kaspersky Security Center Web Console continuam se conectando ao endereço antigo do Servidor de Administração após a renomeação do Servidor de Administração. Para configurar isso, adicione um dos seguintes tipos de registro DNS:

- Um registro A para o endereço antigo do Servidor de Administração que aponta para o novo endereço IP do Servidor de Administração.
- Um registro CNAME que mapeia o nome antigo do Servidor de Administração para o novo nome do Servidor de Administração.

  Para obter mais informações sobre como configurar os registros necessários, consulte a documentação do servidor DNS.

Para preservar as conexões adicionando um novo registro DNS:

1. **Altere o nome do Servidor.**

   Devido à forma como os componentes são configurados durante a instalação, não é possível alterar o nome do Servidor de Administração sem reinstalar o Servidor de Administração.

   Para alterar o nome do servidor:

   1. Crie um novo backup do Servidor de Administração usando o utilitário klbackup.
   2. Desinstale o Kaspersky Security Center Linux e o Kaspersky Security Center Web Console em todas as estações de trabalho de administrador.
   3. Exclua manualmente o banco de dados do Servidor de Administração e o banco de dados do IAM. O Servidor de Administração não o exclui automaticamente durante a desinstalação.
   4. Renomeie o dispositivo no sistema operacional do Servidor de Administração, de acordo com a documentação do seu sistema operacional.
   5. Instale o Servidor de Administração do Kaspersky Security Center Linux usando o novo FQDN do Servidor de Administração.
   6. Restaure o backup do Servidor de Administração preparado anteriormente após a instalação.
   7. Verifique a configuração do Servidor IAM e, se necessário, adicione o endereço do Servidor de Administração ao arquivo de configuração do Servidor IAM.
   8. Instale o Web Console em todas as estações de trabalho dos administradores especificando o novo FQDN do Servidor de Administração no arquivo de resposta.

2. Adicione um novo registro DNS para o endereço antigo do Servidor de Administração.
3. Especifique o novo endereço nas configurações do Servidor de Administração no Kaspersky Security Center Web Console.
4. Execute a tarefa **Alterar o Servidor de Administração** nos dispositivos com visibilidade direta do Servidor de Administração. Depois disso, os dispositivos gerenciados poderão se conectar ao Servidor de Administração usando o novo nome.

Não execute a tarefa em dispositivos sem visibilidade direta do servidor; caso contrário, eles perderão a conexão com o Servidor de Administração e com os gateways de conexão.

Os dispositivos gerenciados conectados por meio de gateways de conexão não verificam o nome do Servidor de Administração. Portanto, nenhuma ação adicional é necessária para esses dispositivos. As informações sobre o endereço do Servidor de Administração não serão atualizadas na saída do comando de diagnóstico klnagchk.

A conexão com o Servidor de Administração é preservada após a alteração do nome do servidor.

Depois de alterar o nome do servidor, as informações do certificado ficarão desatualizadas. Como isso não afeta a operação dos componentes, não recomendamos substituir os certificados autoassinados fora do cronograma. Esses certificados são gerados durante a instalação do Kaspersky Security Center e renovados automaticamente pelo servidor. Eles serão reemitidos com o novo nome do Servidor de Administração durante a próxima substituição automática dos certificados.

Durante a reinstalação, novos certificados serão emitidos para o Servidor IAM e o Web Console Server. Se necessário, substitua-os por certificados personalizados emitidos pela sua Autoridade de Certificação para o novo nome do Servidor de Administração. Consulte o seguinte artigo para obter detalhes: Sobre os certificados do Kaspersky Security Center Linux.

Preservação das conexões pela mudança para a conectividade baseada em endereço IP

Neste cenário, a forma como os dispositivos gerenciados se conectam ao Servidor de Administração é alterada. Os dispositivos se conectam usando o endereço IP do Servidor de Administração em vez do nome do Servidor de Administração. Alternar todos os dispositivos gerenciados pode levar algum tempo, dependendo do número de dispositivos e da frequência com que eles aparecem na rede com o Servidor de Administração.

Para preservar conexões alternando para a conectividade baseada em endereço IP:

1. **Prepare a infraestrutura do Kaspersky Security Center antes de alterar o nome do Servidor de Administração.**

    1. Conecte os dispositivos gerenciados ao Servidor de Administração usando um endereço IP. Após alterar o nome do Servidor de Administração, os dispositivos que usam esse nome para conexão serão desconectados do Servidor. Para se conectar por meio de um endereço IP, execute a tarefa Alterar Servidor de Administração em dispositivos com visibilidade direta do Servidor de Administração, incluindo dispositivos que atuam como gateways de conexão.

        Não execute a tarefa em dispositivos sem visibilidade direta do servidor; caso contrário, eles perderão a conexão com o Servidor de Administração e com os gateways de conexão.

        Os dispositivos gerenciados conectados por meio de gateways de conexão não verificam o nome do Servidor de Administração. Portanto, nenhuma ação adicional é necessária para esses dispositivos. As informações sobre o endereço do Servidor de Administração não serão atualizadas na saída do comando de diagnóstico klnagchk.

2. Certifique-se de que todos os dispositivos gerenciados estejam conectados ao Servidor de Administração por meio do endereço IP. Para fazer isso, verifique o seguinte:

   - Os resultados do comando de diagnóstico klnagchk na linha de endereço do Servidor de Administração em dispositivos gerenciados com acesso direto ao Servidor de Administração.

   - As informações de propriedades do pacote de instalação do Agente de Rede no momento da instalação nos dispositivos.

     O Agente de Rede deve ser configurado inicialmente para se conectar ao Servidor de Administração usando um endereço IP.

     > Se você instalar o Agente de Rede sobre a instalação existente sem desinstalá-lo primeiro, o endereço de conexão do Servidor de Administração e o certificado especificados na configuração do Agente de Rede não serão atualizados.

3. Especifique um novo nome nos perfis de conexão existentes do Servidor de Administração.

4. Se você estiver usando a função de Gerenciamento de Dispositivos Móveis (gerenciamento de dispositivos Android e iOS), siga as instruções Como alterar o endereço do Servidor de Administração em dispositivos móveis que usam o Kaspersky Endpoint Security for Android com a função MDM ou KSMM.

2. **Altere o nome do Servidor.**

Devido à forma como os componentes são configurados durante a instalação, não é possível alterar o nome do Servidor de Administração sem reinstalar o Servidor de Administração.

Para alterar o nome do servidor:

1. Crie um novo backup do Servidor de Administração usando o utilitário klbackup.

2. Desinstale o Kaspersky Security Center Linux e o Kaspersky Security Center Web Console em todas as estações de trabalho de administrador.

3. Exclua manualmente o banco de dados do Servidor de Administração e o banco de dados do IAM. O Servidor de Administração não o exclui automaticamente durante a desinstalação.

4. Renomeie o dispositivo no sistema operacional do Servidor de Administração, de acordo com a documentação do seu sistema operacional.

5. Instale o Servidor de Administração do Kaspersky Security Center Linux usando o novo FQDN do Servidor de Administração.

6. Restaure o backup do Servidor de Administração preparado anteriormente após a instalação.

7. Verifique a configuração do Servidor IAM e, se necessário, adicione o endereço do Servidor de Administração ao arquivo de configuração do Servidor IAM.

8. Instale o Web Console em todas as estações de trabalho dos administradores especificando o novo FQDN do Servidor de Administração no arquivo de resposta.

3. **Atualize os endereços do Servidor de Administração nas configurações do Servidor de Administração.**

   Depois de alterar o nome do Servidor de Administração, especifique o novo endereço FQDN nas configurações do Servidor de Administração no Kaspersky Security Center Web Console. Para fazer isso, verifique e atualize o endereço FQDN em cada uma das seguintes configurações:

   - Endereço do servidor proxy do Kaspersky Security Network
   - Servidor Web
   - Propriedades dos pacotes de instalação do Agente de Rede
   - Nome do emissor do código de segurança (2FA)

   Além disso, faça o seguinte:

   - Especifique o novo nome do servidor nas políticas e configurações de outros aplicativos Kaspersky.
   - Republique cada pacote autônomo publicado e cada pacote de dispositivos móveis.
   - Reconecte os Servidores de Administração secundários se você usar uma hierarquia de Servidores de Administração e se os servidores estiverem conectados por nome, e não por endereço IP.

4. Execute a tarefa **Alterar o Servidor de Administração** em dispositivos com visibilidade direta do Servidor de Administração para alterar o endereço de conexão nos dispositivos gerenciados para o novo nome do Servidor de Administração.

A conexão com o Servidor de Administração é preservada após a alteração do nome do servidor.

Depois de alterar o nome do servidor, as informações do certificado ficarão desatualizadas. Como isso não afeta a operação dos componentes, não recomendamos substituir os certificados autoassinados fora do cronograma. Esses certificados são gerados durante a instalação do Kaspersky Security Center e renovados automaticamente pelo servidor. Eles serão reemitidos com o novo nome do Servidor de Administração durante a próxima substituição automática dos certificados.

Durante a reinstalação, novos certificados serão emitidos para o Servidor IAM e o Web Console Server. Se necessário, substitua-os por certificados personalizados emitidos pela sua Autoridade de Certificação para o novo nome do Servidor de Administração. Consulte o seguinte artigo para obter detalhes: Sobre os certificados do Kaspersky Security Center Linux.

Restauração de conexões interrompidas após a alteração do nome do servidor

O cenário é relevante nos seguintes casos:

- Se você perdeu a propriedade do nome de domínio do dispositivo do Servidor de Administração, mas ainda tem acesso ao Servidor de Administração.
- Se o Servidor de Administração não estiver mais gerenciando os dispositivos gerenciados.
- Se não for possível adicionar registros DNS para o endereço antigo do Kaspersky Security Center Linux por outros motivos.

Para restaurar conexões interrompidas após alterar o nome do servidor:

1. **Altere o nome do Servidor.**

   Devido à forma como os componentes são configurados durante a instalação, não é possível alterar o nome do Servidor de Administração sem reinstalar o Servidor de Administração.

   Para alterar o nome do servidor:

   1. Crie um novo backup do Servidor de Administração usando o utilitário klbackup.
   2. Desinstale o Kaspersky Security Center Linux e o Kaspersky Security Center Web Console em todas as estações de trabalho de administrador.
   3. Exclua manualmente o banco de dados do Servidor de Administração e o banco de dados do IAM. O Servidor de Administração não o exclui automaticamente durante a desinstalação.
   4. Renomeie o dispositivo no sistema operacional do Servidor de Administração, de acordo com a documentação do seu sistema operacional.
   5. Instale o Servidor de Administração do Kaspersky Security Center Linux usando o novo FQDN do Servidor de Administração.
   6. Restaure o backup do Servidor de Administração preparado anteriormente após a instalação.
   7. Verifique a configuração do Servidor IAM e, se necessário, adicione o endereço do Servidor de Administração ao arquivo de configuração do Servidor IAM.
   8. Instale o Web Console em todas as estações de trabalho dos administradores especificando o novo FQDN do Servidor de Administração no arquivo de resposta.

2. **Atualize os endereços do Servidor de Administração nas configurações do Servidor de Administração.**

   Depois de alterar o nome do Servidor de Administração, especifique o novo endereço FQDN nas configurações do Servidor de Administração no Kaspersky Security Center Web Console. Para fazer isso, verifique e atualize o endereço FQDN em cada uma das seguintes configurações:

   - Endereço do servidor proxy do Kaspersky Security Network
   - Servidor Web
   - Propriedades dos pacotes de instalação do Agente de Rede
   - Nome do emissor do código de segurança (2FA)

   Além disso, faça o seguinte:

   - Especifique o novo nome do servidor nas políticas e configurações de outros aplicativos Kaspersky.
   - Republique cada pacote autônomo publicado e cada pacote de dispositivos móveis.
   - Reconecte os Servidores de Administração secundários se você usar uma hierarquia de Servidores de Administração e se os servidores estiverem conectados por nome, e não por endereço IP.

3. Restaure a conexão com o Servidor de Administração nos dispositivos gerenciados anteriormente:

   - Em dispositivos com visibilidade direta para o Servidor de Administração, use o utilitário klmover para especificar o endereço de conexão com o novo nome do Servidor de Administração. Consulte o artigo a seguir para obter detalhes: Conectar Agentes de Rede ao Servidor de Administração usando o utilitário klmover.

   - Em dispositivos que atuam como gateways de conexão, reinstale o Agente de Rede e reconfigure a função de gateway de conexão. Consulte o seguinte artigo para obter detalhes: Adicionar um gateway de conexão na DMZ como um ponto de distribuição.

   - Os dispositivos conectados por meio de gateways de conexão serão reconectados automaticamente depois que os gateways de conexão forem restaurados. O Agente de Rede não usa o nome do Servidor de Administração ao se conectar a gateways de conexão.

     Não use o utilitário klmover em dispositivos conectados por meio de gateways de conexão. Consulte o seguinte artigo para obter detalhes: Mover dispositivos conectados ao Servidor de Administração por meio de gateways de conexão para outro Servidor de Administração.

A conexão com o Servidor de Administração é restaurada depois que o nome do servidor é alterado.

Depois de alterar o nome do servidor, as informações do certificado ficarão desatualizadas. Como isso não afeta a operação dos componentes, não recomendamos substituir os certificados autoassinados fora do cronograma. Esses certificados são gerados durante a instalação do Kaspersky Security Center e renovados automaticamente pelo servidor. Eles serão reemitidos com o novo nome do Servidor de Administração durante a próxima substituição automática dos certificados.

Durante a reinstalação, novos certificados serão emitidos para o Servidor IAM e o Web Console Server. Se necessário, substitua-os por certificados personalizados emitidos pela sua Autoridade de Certificação para o novo nome do Servidor de Administração. Consulte o seguinte artigo para obter detalhes: Sobre os certificados do Kaspersky Security Center Linux.

Alterando credenciais de DBMS

Às vezes, pode ser necessário alterar as credenciais do DBMS, por exemplo, para realizar a rotatividade de credenciais para fins de segurança.

Alteração das credenciais do banco de dados do Servidor de Administração

Para alterar as credenciais do Servidor de Administração e do banco de dados do IAM em um ambiente Linux:

1. Interromper o Servidor de Administração. Dependendo do tipo de implantação do Kaspersky Security Center Linux, execute um dos seguintes comandos na conta root:

   - Para um cluster de failover do Kaspersky Security Center Linux:

     No nó ativo, execute o seguinte comando:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc
     ```

- Para um cluster de failover geograficamente distribuído do Kaspersky Security Center Linux:

  Em ambos os nós, execute o seguinte comando:

  ```
  crm node standby
  ```

- Para uma implantação do Servidor de Administração sem cluster:

  Execute os seguintes comandos:

  ```
  systemctl stop kladminserver_srv.service
  systemctl stop kliam_srv.service
  ```

2. Conecte-se ao banco de dados do Servidor de Administração com privilégios de superusuário do DBMS e execute o seguinte comando:

   ```
   REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
   ```

   em que `<old_kscdbadmin>` é a conta de usuário antiga do DBMS que o Servidor de Administração usava para se conectar ao banco de dados, e `<new_kscdbadmin>` é a nova conta de usuário do DBMS.

3. Conecte-se ao banco de dados do IAM com privilégios de superusuário do DBMS e execute o seguinte comando:

   ```
   REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
   ```

   em que `<old_iamdbadmin>` é a conta anterior do DBMS usada pelo Servidor de Administração para se conectar ao banco de dados, e `<new_iamdbadmin>` são as novas contas do DBMS.

4. Localize o arquivo de configuração do IAM: /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml

5. Na seção `dbms_iam`, especifique as novas credenciais da conta nos campos de usuário e senha. Verifique se a conta existe no DBMS e está especificada como proprietária do banco de dados do IAM.

6. Executar o Servidor de Administração. Dependendo do tipo de implantação do Kaspersky Security Center Linux, execute um dos seguintes comandos na conta root:

   - Para um cluster de failover do Kaspersky Security Center Linux:

     No nó ativo, execute o seguinte comando:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc
     ```

   - Para um cluster de failover geograficamente distribuído do Kaspersky Security Center Linux:

     Em ambos os nós, execute o seguinte comando:

     ```
     crm node online
     ```

- Para uma implantação do Servidor de Administração sem cluster:

  Execute os seguintes comandos:

  ```
  systemctl start kladminserver_srv.service
  systemctl start kliam_srv.service
  ```

7. Execute o utilitário klsrvconfig:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

8. Especifique um novo nome de conta. Você deve especificar as credenciais de uma conta que existe no DBMS.
9. Insira uma nova senha.
10. Especifique a nova senha para confirmação.
11. Aguarde até que o Servidor de Administração retome a operação e seja exibida uma entrada no syslog do nó ativo informando que o Servidor de Administração está pronto para operações na GUI.

As credenciais do banco de dados do Servidor de Administração são alteradas.

Cópia backup e restauração dos dados do Servidor de Administração

O backup de dados permite mover um Servidor de Administração de um dispositivo para outro, sem perda de dados. Usando o backup, você pode restaurar dados ao mover o banco de dados de um Servidor de Administração para outro dispositivo ou ao atualizar para uma versão mais recente do Kaspersky Security Center. Além disso, é possível usar o backup de dados para mover dados do Servidor de Administração do Kaspersky Security Center Windows sob gerenciamento do Kaspersky Security Center Linux (não há suporte para mover dados do Kaspersky Security Center Linux para o Kaspersky Security Center Windows).

Não é feito backup dos plug-ins de gerenciamento instalados. Depois de restaurar os dados do Servidor de Administração a partir de uma cópia de backup, você precisará fazer download e reinstalar plug-ins para aplicativos gerenciados.

Antes de fazer backup dos dados do Servidor de Administração, execute as seguintes ações:

- **Siga os requisitos para criar um backup no Servidor de Administração 16 ou anterior e restaurá-lo na versão 16.1 ou posterior**

  - Se você criar um backup de dados no Servidor de Administração 16 ou anterior e restaurá-lo no Servidor de Administração 16.1 ou posterior, a autenticação de dois fatores será ativada. Para obter mais informações, consulte Sobre a autenticação de dois fatores para uma conta.

Para garantir que os usuários possam fazer login no Web Console com suas contas existentes usando chaves secretas de autenticação de dois fatores configuradas e que os scripts de automação OpenAPI continuem funcionando após a restauração, você deve executar as seguintes etapas:

- Ativação da autenticação de dois fatores para todos os usuários
- Os administradores devem configurar a autenticação de dois fatores para suas próprias contas
- Excluir contas da autenticação de dois fatores

  Se necessário, adicione contas de integração usadas para executar scripts por meio do OpenAPI à lista de exclusão.

Se não for possível configurar a autenticação de dois fatores antes de criar o backup, as contas de usuário serão adicionadas à lista de permissão da autenticação de dois fatores e os usuários poderão configurá-la ao fazer login no Web Console. Condições mais detalhadas para adicionar uma conta à lista de permissão estão descritas no tópico Permitir que os usuários configurem a autenticação de dois fatores.

- Verifique se um Servidor de Administração virtual é adicionado ao grupo de administração. Caso um Servidor de Administração virtual seja adicionado, verifique e confirme se um administrador foi atribuído para esse Servidor de Administração virtual antes do backup. Não é possível conceder ao administrador direitos de acesso ao Servidor de Administração virtual após o backup. Observe que, caso as credenciais da conta do administrador sejam perdidas, não será possível atribuir um novo administrador ao Servidor de Administração virtual.

- Para realizar o backup ou a restauração de um cluster de failover do Kaspersky Security Center Linux, é necessário parar todo o cluster para manutenção e reiniciá-lo após a conclusão do processo.

Você pode criar uma cópia de backup dos dados do Servidor de Administração em uma das seguintes formas:

- Criando e executando uma tarefa de backup de dados por meio do Kaspersky Security Center Web Console.

- Executando o utilitário klbackup no dispositivo que tenha o Servidor de Administração instalado. Este utilitário está incluído no kit de distribuição do Kaspersky Security Center. Após a instalação do Servidor de Administração, o utilitário estará localizado na raiz da pasta de destino especificada na instalação do aplicativo (geralmente /opt/kaspersky/ksc64/sbin/klbackup).

Os seguintes dados são salvos em uma cópia de backup do Servidor de Administração:

- O banco de dados do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração)

- Detalhes da configuração da estrutura dos grupos de administração e dispositivos cliente

- Repositório dos pacotes de distribuição de aplicativos para instalação remota

- Certificado do Servidor de Administração

- Chaves secretas de autenticação de dois fatores configuradas para contas de usuário
- Lista das contas de usuário excluídas da autenticação de dois fatores

É possível criar uma cópia de backup dos dados do Servidor de Administração criando e executando uma tarefa de backup de dados ou usando o utilitário klbackup. Só é possível fazer a restauração dos dados do Servidor de Administração por meio do utilitário klbackup. A restauração deverá ser executada em uma instância operável do Servidor de Administração que acabou de ser instalado e que tenha a mesma versão (ou posterior) para a qual a cópia de backup foi criada. Não use nenhuma ferramenta de terceiros para fazer backup ou restauração e, se possível, não remova a instalação anterior do Kaspersky Security Center Linux até que a configuração e a transferência dos dados sejam totalmente concluídas.

Criando uma tarefa de backup de dados do Servidor de Administração

As tarefas de backup são tarefas do Servidor de Administração, criadas através do Assistente de Início Rápido. Se uma tarefa de backup criada pelo Assistente de início rápido tiver sido excluída, você pode criar uma manualmente.

A tarefa *Backup de dados do Servidor de Administração* só pode ser criada numa única cópia. Se a tarefa de backup de dados do Servidor de Administração já foi criada para o Servidor de Administração, ela não é exibida na janela de seleção de tipo de tarefa.

Para criar uma tarefa de backup de dados do Servidor de Administração:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Navegue pelo assistente usando o botão **Avançar**.
3. Na lista **Aplicativo**, selecione **Kaspersky Security Center 17** e na lista **Tipo de tarefa**, selecione **Backup de dados do Servidor de Administração**.
4. Na etapa correspondente, especifique as seguintes informações:
   - Pasta para armazenamento de cópias de backup
   - Senha para backup (opcional)
   - Número máximo de cópias de backup a salvar
5. Caso queira modificar as configurações padrão da tarefa, ative a opção **Concluir a criação da tarefa** na etapa **Abrir detalhes da tarefa quando a criação for concluída**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode alterar as configurações padrão depois, a qualquer momento.
6. Clique no botão **Concluir**.

A tarefa é criada e exibida na lista de tarefas.

Usando o utilitário klbackup para fazer backup e recuperar dados

Você copiar os dados do Servidor de Administração para backup e recuperação futura, usando o utilitário klbackup, que está incluído no kit de distribuição do Kaspersky Security Center.

A instância do Servidor de Administração na qual a restauração será executada deve usar um DBMS do mesmo tipo. A versão do Servidor de Administração pode ser a mesma (com uma correção idêntica ou posterior), ou posterior.

Caso tenha feito o backup dos dados do Servidor de Administração incluído no Kaspersky Security Center Linux 15 ou versão anterior ao usar o MariaDB DBMS de uma versão anterior e, em seguida, tenha recuperado os dados em um dispositivo com uma versão posterior do MariaDB, um erro poderá ocorrer. Para obter mais informações, consulte Como restaurar dados do Servidor de Administração de um backup criado em uma versão anterior do DBMS.

Os sinalizadores do agente de rede não são restaurados quando o utilitário klbackup é usado. É preciso configurar manualmente os sinalizadores do agente de rede.

Para criar uma cópia de backup ou recuperar os dados do Servidor de Administração no modo silencioso,

Execute o utilitário klbackup com o conjunto de chaves a partir da linha de comando de um dispositivo que tenha o Servidor de Administração instalado.

A sintaxe da linha de comando do utilitário:

```
klbackup -path <backup path> [-linux_path <DBMS backup path>-node_cert <certificate path>] [-logfile <log file> [-use_ts]|[-restore] [-password <password>] [-cert_only]
```

Se nenhuma senha for especificada na linha de comando do utilitário klbackup, o utilitário solicita a inserção da senha interativamente.

Descrições das chaves:

- `-path <backup path>`. Salve as informações na pasta de backup ou utilize os dados desta pasta para fazer a recuperação (parâmetro obrigatório).
- `-linux_path <DBMS backup path>`. Caminho local para a pasta que contém os dados de backup do DBMS.

  Devem ser concedidas permissões à conta do servidor do banco de dados e ao utilitário klbackup para alterar os dados na pasta de backup do DBMS.
- `-node_cert <certificate path>`. Arquivo de certificado do servidor para configurar o nó do cluster de failover inativo após a recuperação. Se não estiver definido, ele será automaticamente recuperado no servidor.
- `-logfile <log file>`. Salvar um relatório sobre o backup e a recuperação de dados do Servidor de Administração.

  Devem ser concedidas permissões à conta do servidor do banco de dados e ao utilitário klbackup para alterar os dados na pasta de backup.

- `-use_ts`. Ao salvar dados, copie as informações para a pasta de backup, em uma subpasta com um nome no formato `klbackup YYYY-MM-DD # HH-MM-SS`, que inclui a data atual e a hora da operação em UTC. Se nenhuma chave for especificada, as informações são salvas na raiz da pasta de backup.

  Ao tentar salvar informações em uma pasta que já armazena uma cópia de backup, uma mensagem de erro será exibida. Nenhuma informação será atualizada.

  A disponibilidade da chave `-use_ts` permite manter um arquivo de dados do Servidor de Administração. Por exemplo, caso a chave `-path` indique a pasta `/tmp/KLBackups`, a pasta `klbackup 2022/6/19 # 11-30-18` armazenará as informações sobre o status do Servidor de Administração em 19 de junho de 2022, às 11:30:18.

- `-restore` – Recupere os dados do Servidor de Administração. A recuperação de dados é realizada com base nas informações contidas na pasta de backup. Se não houver nenhuma chave disponível, um backup dos dados será feito na pasta de backup.

- `-password <password>` – Senha para proteger os dados confidenciais.

  Uma senha esquecida não pode ser recuperada. Não há requisitos de senha. O comprimento da senha é ilimitado e também é possível um comprimento nulo (sem senha).

  Ao restaurar dados, você deve especificar a mesma senha que foi inserida durante o backup. Se o caminho para uma pasta compartilhada for alterado após o backup, verifique a operação de tarefas que usam os dados restaurados (tarefas de restauração e tarefas de instalação remota). Se necessário, edite as configurações dessas tarefas. Enquanto os dados estão sendo restaurados de um arquivo de backup, ninguém deve acessar a pasta compartilhada do Servidor de Administração. A conta em que o utilitário klbackup é iniciado deve ter acesso completo à pasta compartilhada. Para restaurar os dados do Servidor de Administração do backup, recomendamos executar o utilitário em um Servidor de Administração recentemente instalado.

- `-cert_only` – Salve ou recupere somente o certificado e a chave privada do Servidor de Administração.

  Este sinalizador pode ser útil ao executar a migração do Servidor de Administração do Kaspersky Security Center Windows para o Servidor de Administração do Kaspersky Security Center Linux. Além disso, é possível migrar dispositivos gerenciados entre os Servidores de Administração do Kaspersky Security Center Linux, e entre os Servidores de Administração do Kaspersky Security Center Windows.

É possível usar um backup de dados para migrar os dados do Servidor de Administração do Kaspersky Security Center Windows para que sejam gerenciados pelo Kaspersky Security Center Linux.
Caso use o MySQL ou o MariaDB como um DBMS para o Kaspersky Security Center Windows e para o Kaspersky Security Center Linux, o parâmetro `lower_case_table_names` deve corresponder ao DBMS atual e ao novo.
Antes de criar uma cópia backup dos dados, verifique a configuração `lower_case_table_names`. Então, ao instalar o MySQL ou MariaDB para o Kaspersky Security Center Linux, será necessário definir o parâmetro `lower_case_table_names` com o mesmo valor especificado para este parâmetro no Windows.

Se, durante a restauração, o certificado comum do Servidor de Administração for substituído por outro certificado de um backup, execute as seguintes etapas para assegurar a operação adequada:
1. Reinstale o Web Console para evitar o seguinte erro:
O Servidor de Administração usa um certificado não confiável. Reconfigure o aplicativo especificando um certificado válido ou entre em contato com o administrador principal.
2. Verifique a configuração do Servidor IAM e, se necessário, adicione o endereço do Servidor de Administração ao arquivo de configuração do Servidor IAM.

Uso do utilitário klbackup para alterar dispositivos gerenciados sob gerenciamento de outro Servidor de Administração

O utilitário klbackup permite alterar dispositivos gerenciados sob gerenciamento de outro Servidor de Administração. É possível alterar o Servidor de Administração do Kaspersky Security Center Windows para Kaspersky Security Center Linux usando o utilitário klbackup ao executar a migração. Além disso, é possível migrar dispositivos gerenciados entre os Servidores de Administração do Kaspersky Security Center Linux, e entre os Servidores de Administração do Kaspersky Security Center Windows.

Antes de começar, **verifique os requisitos para um certificado personalizado**.

Se você estiver usando um certificado personalizado em vez do autoassinado, antes de atualizar a Kaspersky Security Center Linux para a versão mais recente, certifique-se de que o certificado inclua o Nome alternativo da entidade (SAN). Caso contrário, é importante substituir o certificado antes de atualizar o Kaspersky Security Center Linux. Caso contrário, você não poderá fazer login no Web Console após a atualização.

Para certificar-se de que o certificado inclui o SAN:

1. No dispositivo com o Servidor de Administração instalado, execute o comando:

   - Para um dispositivo baseado em Linux:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Para um dispositivo baseado em Windows:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Assegure-se de que o Nome alternativo da entidade (SAN) esteja presente na saída do comando e contenha o endereço do dispositivo do Servidor de Administração.

3. Se o Nome alternativo da entidade estiver ausente, use o utilitário klsetsrvcert para substituir o certificado do usuário por um certificado que atenda aos requisitos.

Para alterar dispositivos gerenciados sob gerenciamento de outro Servidor de Administração usando o utilitário klbackup:

1. No dispositivo anterior, crie uma cópia de backup do certificado do Servidor de Administração e da chave privada.

   É possível criar uma cópia de backup por meio de uma das seguintes formas:

   - Usando a interface do utilitário klbackup (somente para o Servidor de Administração do Kaspersky Security Center Windows)

     Execute o utilitário klbackup localizado na pasta de instalação do Kaspersky Security Center e crie um backup usando a opção **Restaurar ou fazer backup somente do certificado do Servidor de Administração**.

- Usando o prompt de comando (para os Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux versão 15.1 ou posterior)

  Execute o utilitário klbackup com a chave `-cert_only` na linha de comando para criar uma cópia de backup do certificado do Servidor de Administração e da chave privada:

  ```
  klbackup -path <path to the backup copy of Administration Server certificate> -cert_only
  ```

2. No dispositivo anterior, desconecte o Servidor de Administração da rede.

3. Atribua o mesmo nome de domínio ao dispositivo com outro Servidor de Administração.

   O novo Servidor de Administração pode ser atribuído ao nome NetBIOS, FQDN e endereço IP estático. Isso depende de qual endereço do Servidor de Administração foi definido no pacote de instalação do Agente de Rede quando os Agentes de Rede foram implementados. Como alternativa, é possível usar o endereço de conexão que determina o Servidor de Administração ao qual o Agente de Rede se conecta (esse endereço pode ser obtido em dispositivos gerenciados usando o utilitário klnagchk).

   Se for impossível atribuir o mesmo endereço ao dispositivo com outro Servidor de Administração, você deve gerar um novo certificado do Servidor de Administração e especificá-lo no arquivo de configuração do IAM. Após a instalação do Servidor de Administração, você precisa mudar manualmente os Agentes de Rede para o novo Servidor de Administração.

4. Em um dispositivo com outro Servidor de Administração, restaure o certificado do Servidor de Administração e a chave privada por meio da cópia de backup.

   É possível restaurar uma cópia de backup por meio de uma das seguintes formas:

   - Usando a interface do utilitário klbackup (somente para o Servidor de Administração do Kaspersky Security Center Windows)

     Execute o utilitário klbackup e, em seguida, restaure um backup com o uso da opção **Restaurar ou fazer backup somente do certificado do Servidor de Administração**.

   - Usando o prompt de comando (para os Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux versão 15.1 ou posterior)

     Execute o utilitário `klbackup` com a opção `-cert_only` na linha de comando para restaurar o certificado do Servidor de Administração e a chave privada a partir de uma cópia backup:

     ```
     klbackup -path <path to the backup copy of Administration Server certificate> -restore -cert_only
     ```

5. Configure a verificação de certificado pelo Servidor de Administração e pelo Servidor IAM.

Os dispositivos gerenciados são colocados sob o gerenciamento de outro Servidor de Administração. É possível ir para o Servidor de Administração e garantir que os dispositivos gerenciados estejam visíveis na rede e se o Agente de Rede está instalado e sendo executado neles (o valor *Sim* nas colunas **Visível**, **Agente de Rede instalado** e **Agente de Rede em execução**).

Backup e restauração de dados do Servidor de Administração ao usar MySQL ou MariaDB

É possível usar um backup de dados para migrar dados do Servidor de Administração do Kaspersky Security Center Windows sob gerenciamento do Kaspersky Security Center Linux. A migração usando o backup de dados do Servidor de Administração é compatível apenas com a migração para o Kaspersky Security Center Linux 15.2 ou posterior por qualquer versão compatível do Kaspersky Security Center Windows.

Caso queira usar o MySQL ou o MariaDB como um DBMS para o Kaspersky Security Center Windows e para o Kaspersky Security Center Linux, o parâmetro `lower_case_table_names` deve corresponder ao DBMS atual e ao novo. Caso contrário, os dados do Servidor de Administração serão migrados incorretamente.

Antes de fazer backup dos dados do Servidor de Administração no Kaspersky Security Center Windows, verifique o valor do parâmetro `lower_case_table_names`. Se você não especificar este parâmetro durante a instalação anterior do DMBS, o valor padrão do parâmetro será utilizado. O valor padrão do parâmetro `lower_case_table_names` para Windows é `1`.

Em seguida, ao instalar o MySQL ou o MariaDB para o Kaspersky Security Center Linux, defina para `lower_case_table_names` o mesmo valor especificado para esse parâmetro no Windows. Para obter detalhes, consulte as instruções no site do MySQL. Caso esse parâmetro não seja especificado, o valor padrão do parâmetro será usado. Para sistemas operacionais baseados em Linux, o valor padrão do parâmetro `lower_case_table_names` é diferente do valor padrão para Windows.

Caso queira instalar o MySQL 8.0, especificar o parâmetro `lower_case_table_names` de acordo com esta instrução pode não funcionar. Nesse caso, primeiro é necessário instalar o MySQL 5.7, especificar o parâmetro `lower_case_table_names` usando a instrução e, em seguida, atualizar o MySQL 5.7 para o MySQL 8.0. Caso o parâmetro `lower_case_table_names` não corresponda aos DBMSs atual e novo, os dados do Servidor de Administração serão restaurados incorretamente.

Manutenção do Servidor de Administração

A manutenção do Servidor de Administração permite liberar espaço na pasta do Servidor de Administração e reduzir o volume do banco de dados excluindo objetos que não são mais necessários. Isso ajuda a melhorar o desempenho e a confiabilidade da operação do aplicativo. Recomendamos efetuar a manutenção do Servidor de Administração ao menos uma vez por semana.

A manutenção do Servidor de Administração é executada usando uma tarefa dedicada. O aplicativo executa as seguintes ações ao efetuar a manutenção do Servidor de Administração:

- Exclui pastas e arquivos desnecessários da pasta de armazenamento.
- Exclui registros desnecessários das tabelas (também conhecidos como "ponteiros pendentes").
- Limpa o cache.

- Mantém o banco de dados (se você usar o PostgreSQL como um DBMS):
  - Reorganiza os índices do banco de dados
  - Atualiza as estatísticas do banco de dados
  - Compacta o banco de dados (caso seja necessário)

A tarefa Manutenção do Servidor de Administração oferece suporte às versões 10.3 e posteriores do MariaDB. Caso as versões 10.2 ou anteriores do MariaDB sejam usadas, os administradores terão que manter esse DBMS por conta própria.

A tarefa Manutenção do Servidor de Administração é criada automaticamente quando o Kaspersky Security Center Linux é instalado. Se a tarefa Manutenção do Servidor de Administração for excluída, você poderá criá-la manualmente.

Para criar uma tarefa Manutenção do Servidor de Administração:

1. No menu principal, vá para **Tarefas**.
2. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia.
3. Na janela **Novas configurações de tarefa** do assistente, selecione **Manutenção do Servidor de Administração** como tipo de tarefa e clique no botão **Avançar**.
4. Siga o restante das instruções do assistente.

A tarefa recém-criada é exibida na lista de tarefas. Somente uma tarefa Manutenção do Servidor de Administração pode ser executada para um único Servidor de Administração. Se uma tarefa de Manutenção do Servidor de Administração já tiver sido criada para um Servidor de Administração, nenhuma nova tarefa de Manutenção do Servidor de Administração poderá ser criada.

Excluir uma hierarquia de Servidores de Administração

Se você não quiser mais ter uma hierarquia de Servidores de Administração, você poderá desconectá-los dessa hierarquia.

Para excluir uma hierarquia de Servidores de Administração:

1. No menu principal, clique no nome do Servidor de Administração.
2. Na página que se abre, prossiga para a guia **Servidores de Administração**.
3. No grupo de administração do qual deseja excluir o Servidor de administração secundário, selecione o Servidor de administração secundário.

4. Na linha de menu, clique em **Excluir**.

5. Na janela que se abre, clique em **OK** para confirmar que deseja excluir o Servidor de administração secundário.

Os antigos Servidores de administração principal e secundário agora são independentes um do outro. A hierarquia não existe mais.

Acesso aos servidores DNS públicos

Caso o acesso aos servidores da Kaspersky que estão usando o DNS do sistema não seja possível, o Kaspersky Security Center Linux poderá usar esses servidores DNS públicos na seguinte ordem:

1. Google Public DNS (8.8.8.8)

2. Cloudflare DNS (1.1.1.1)

3. Alibaba Cloud DNS (223.6.6.6)

4. Quad9 DNS (9.9.9.9)

5. CleanBrowsing (185.228.168.168)

As solicitações para esses servidores DNS podem conter endereços de domínio e o endereço IP público do Servidor de Administração, porque o aplicativo estabelece uma conexão TCP/UDP com o servidor DNS. Caso o Kaspersky Security Center Linux esteja usando um Servidor DNS público, o processamento de dados será regido pela Política de Privacidade do serviço pertinente.

Para configurar o uso de DNS público por meio do utilitário klscflag:

1. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Para desativar o uso do DNS público, execute o seguinte comando com a conta root:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
```

3. Para ativar o uso do DNS público, execute o seguinte comando com a conta root:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
```

Configurar interface

Você pode configurar a interface do Kaspersky Security Center Web Console para exibir e ocultar seções e elementos da interface, dependendo dos recursos que estão sendo usados.

Para configurar a interface do Kaspersky Security Center Web Console de acordo com o conjunto de recursos usados no momento:

1. No menu principal, vá para **Configurações** → **Opções da interface**.
2. Ative ou desative as opções necessárias:
   - **Mostrar a criptografia e proteção de dados**
   - **Mostrar recursos MDR**
   - **Mostrar alertas EDR**
3. Clique no botão **Salvar**.

Depois que as opções necessárias são ativadas, o console exibe as seções correspondentes no menu principal. Por exemplo, se você ativar **Mostrar alertas EDR**, a seção **Monitoramento** → **Alertas** aparecerá no menu principal.

Conexão criptografado a um Servidor de Administração

A troca de dados entre dispositivos clientes e o Servidor de Administração pode ser realizada usando o protocolo TLS (Segurança da Camada de Transporte). O protocolo TLS permite a identificação de partes interagentes, codificação de dados que são transferidos e proteção destes contra modificação durante a transferência. O protocolo TLS usa chaves públicas para autenticar as partes que interagem e os dados criptografados.

Quando um dispositivo cliente se conecta com o Servidor de Administração pela primeira vez, o Agente de Rede no dispositivo baixa uma cópia do certificado do Servidor de Administração e o armazena localmente.

Se você instalar o Agente de Rede em um dispositivo localmente, poderá selecionar o certificado do Servidor de Administração manualmente.

A cópia baixada do certificado é usada para verificar os direitos e permissões do Servidor de Administração durante conexões subsequentes.

Durante sessões futuras, o Agente de Rede solicita o certificado do Servidor de Administração em cada conexão do dispositivo ao Servidor de Administração e o compara com a cópia local. Se as cópias não coincidirem, o dispositivo não terá a permissão para acessar o Servidor de administração.

Criptografar comunicação com TLS

Para a correção de vulnerabilidades na rede corporativa de sua organização, é possível ativar a criptografia de tráfego usando o protocolo TLS. É possível ativar os protocolos de criptografia TLS e os pacotes de codificação compatíveis no Servidor de Administração. O Kaspersky Security Center Linux é compatível com o protocolo TLS versões 1.0, 1.1, 1.2 e 1.3. É possível selecionar o protocolo de criptografia e os pacotes de codificação requeridos.

O Kaspersky Security Center Linux usa certificados autoassinados. Você também pode usar seus próprios certificados. Recomendamos usar certificados emitidos por autoridades de certificação confiáveis.

Para configurar os protocolos de criptografia e pacotes de codificação permitidos no Servidor de Administração:

1. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Use o sinalizador SrvUseStrictSslSettings para configurar os protocolos de criptografia e pacotes de codificação permitidos no Servidor de Administração. Execute o seguinte comando na linha de comando com a conta root:

   ```
   ./klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valor> -t d
   ```

   Especifique o parâmetro <valor> do sinalizador SrvUseStrictSslSettings:

   - `4` - Somente os protocolos TLS 1.2 e TLS 1.3 estão ativados. Além disso, os pacotes de codificação com TLS_RSA_WITH_AES_256_GCM_SHA384 são ativados (esses pacotes de codificação são necessários para a compatibilidade com as versões anteriores do Kaspersky Security Center Linux). Esse é o valor padrão.

     Os pacotes de codificação compatíveis com o protocolo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (pacote de codificação com TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Os pacotes de codificação compatíveis com o protocolo TLS 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - `5` - Somente os protocolos TLS 1.2 e TLS 1.3 estão ativados. Para os protocolos TLS 1.2 e TLS 1.3, os pacotes de codificação específicos listados abaixo são compatíveis.

     Os pacotes de codificação compatíveis com o protocolo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Os pacotes de codificação compatíveis com o protocolo TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Não recomendamos usar 0, 1, 2 ou 3 como o valor do parâmetro do sinalizador SrvUseStrictSslSettings. Esses valores de parâmetro correspondem a versões inseguras do protocolo TLS (TLS 1.0 e TLS 1.1) e pacotes de codificação inseguros. Eles são usados somente para compatibilidade com versões anteriores do Kaspersky Security Center.

3. Reinicie os seguintes serviços do Kaspersky Security Center Linux:
   - Servidor de Administração
   - Servidor Web
   - Proxy de ativação

Como resultado, a criptografia de tráfego usando o protocolo TLS é ativada.

É possível usar os sinalizadores KLTR_TLS12_ENABLED e KLTR_TLS13_ENABLED para ativar o suporte dos protocolos TLS 1.2 e TLS 1.3, respectivamente. Esses sinalizadores são ativados por padrão.

Para ativar ou desativar o suporte dos protocolos TLS 1.2 e TLS 1.3:

1. Execute o utilitário klscflag.

   Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Execute um dos seguintes comandos na linha de comando com a conta root:
   - Use este comando para ativar ou desativar o suporte do protocolo TLS 1.2:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <valor> -t d
     ```

   - Use este comando para ativar ou desativar o suporte do protocolo TLS 1.3:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <valor> -t d
     ```

Especifique o parâmetro < `valor` > do sinalizador:

- `1` – Para ativar o suporte do protocolo TLS.
- `0` – Para desativar o suporte do protocolo TLS.

Configurações de rede para interação com serviços externos

O Kaspersky Security Center Linux usa as seguintes configurações de rede para interagir com serviços externos.

Configurações de rede

Configurações de rede	Endereço	Descrição
Porta: 443 Protocolo: HTTPS	`https://activation-v2.kaspersky.com`	Ativação do aplicativo.
Porta: 443 Protocolo: HTTPS	`https://products.s.kaspersky-labs.com`	Repositório dos pacotes de distribuição de aplicativos para instalação remota

Porta: 443
Protocolo: HTTPS
	`https://s00.upd.kaspersky.com`
	`https://s01.upd.kaspersky.com`
	`https://s02.upd.kaspersky.com`
	`https://s03.upd.kaspersky.com`
	`https://s04.upd.kaspersky.com`
	`https://s05.upd.kaspersky.com`
	`https://s06.upd.kaspersky.com`
	`https://s07.upd.kaspersky.com`
	`https://s08.upd.kaspersky.com`
	`https://s09.upd.kaspersky.com`
	`https://s10.upd.kaspersky.com`
	`https://s11.upd.kaspersky.com`
	`https://s12.upd.kaspersky.com`
	`https://s13.upd.kaspersky.com`
	`https://s14.upd.kaspersky.com`
	`https://s15.upd.kaspersky.com`
	`https://s16.upd.kaspersky.com`
	`https://s17.upd.kaspersky.com`
	`https://s18.upd.kaspersky.com`
	`https://s19.upd.kaspersky.com`
	`https://cm.k.kaspersky-labs.com`
		Atualização de bancos de dados, módulos de software e aplicativos da Kaspersky.

Porta: 443 Protocolo: HTTPS	`https://downloads.upd.kaspersky.com`	• Atualização de bancos de dados, módulos de software e aplicativos da Kaspersky. • Verificar se os servidores da Kaspersky estão acessíveis. Antes de baixar os bancos de dados e módulos de software da Kaspersky, o Kaspersky Security Center Linux verifica se os servidores da Kaspersky estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos.

Configurações de rede	Endereço	Descrição
Porta: 80 Protocolo: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Atualização de bancos de dados, módulos de software e aplicativos da Kaspersky.
Porta: 443 Protocolo: HTTPS	https://ds.kaspersky.com https://dc1.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com/ https://dc1-cert.ksn.kaspersky-labs.com https://dc1-cf.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-kas.ksn.kaspersky-labs.com https://dc1-ml.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com https://dc1.ksn.kaspersky-labs.com	Uso da Kaspersky Security Network.

Configurações de rede	Endereço	Descrição
Porta: 443, 1443 Protocolo: HTTPS	https://ksn-file-geo.kaspersky-labs.com https://ksn-verdict-geo.kaspersky-labs.com https://ksn-url-geo.kaspersky-labs.com https://ksn-a-p2p-geo.kaspersky-labs.com https://ksn-info-geo.kaspersky-labs.com https://ksn-cinfo-geo.kaspersky-labs.com	Uso da Kaspersky Security Network.
Porta: 443, 1443 Protocolo: KSN	ksn://ksn-a-p2p-geo.kaspersky-labs.com ksn://ksn-a-stat-geo.kaspersky-labs.com ksn://ksn-ca-geo.kaspersky-labs.com ksn://ksn-cinfo-geo.kaspersky-labs.com ksn://ksn-crypto-catm-geo.kaspersky-labs.com ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com ksn://ksn-crypto-hash-geo.kaspersky-labs.com ksn://ksn-crypto-ipm-geo.kaspersky-labs.com ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com ksn://ksn-eu-stat-kmp.kaspersky-labs.com ksn://ksn-file-geo.kaspersky-labs.com ksn://ksn-his-geo.kaspersky-labs.com ksn://ksn-info-geo.kaspersky-labs.com ksn://ksn-kas-geo.kaspersky-labs.com ksn://ksn-kddi.kaspersky-labs.com ksn://ksn-ml-geo.kaspersky-labs.com ksn://ksn-oui-geo.kaspersky-labs.com ksn://ksn-pp.kaspersky-labs.com ksn://ksn-src.kaspersky-labs.com ksn://ksn-stat-geo.kaspersky-labs.com ksn://ksn-tcert-geo.kaspersky-labs.com ksn://ksn-url-geo.kaspersky-labs.com ksn://ksn-verdict-geo.kaspersky-labs.com ksn://mdr.ksn.kaspersky-labs.com ksn://stat-eu.ksn.kaspersky-labs.com ksn://stat-hq.ksn.kaspersky-labs.com ksn://stat-ru.ksn.kaspersky-labs.com ksn://stat-sa.ksn.kaspersky-labs.com ksn://stat-sbr.ksn.kaspersky-labs.com	Uso da Kaspersky Security Network.
Porta: 443 Protocolo: HTTPS	https://click.kaspersky.com https://redirect.kaspersky.com	Como seguir os links da interface.
Porta: 80 Protocolo: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Esses servidores fazem parte da Infraestrutura de Chaves Públicas (PKI) e são necessários para verificar o status de validade dos certificados de assinatura digital da Kaspersky. A CRL é uma lista de certificados revogados. O OCSP permite solicitar o status de um certificado específico em tempo real. Esses servidores ajudam a garantir a segurança da interação com certificados digitais e protegem contra possíveis ataques.

Configurações de rede	Endereço	Descrição
Porta: 443 Protocolo: HTTPS	`https://ipm-klca.kaspersky.com`	Informativos de marketing
Porta: 443 Protocolo: HTTPS	`https://tip.kaspersky.com`	Resposta a ameaças por meio do Kaspersky Threat Intelligence Portal (ao usar a funcionalidade Kaspersky Next XDR Optimum).
Porta: 443 Protocolo: HTTPS	Para obter a lista completa de endereços, consulte o artigo Estrutura de endereços e domínios	Resposta a ameaças por meio da Kaspersky Automated Security Awareness Platform (ao usar a funcionalidade Kaspersky Next XDR Optimum).

Para a interação adequada do Kaspersky Security Center Linux com os serviços externos, considere as seguintes recomendações:
- O tráfego de rede não criptografado deve ser permitido nas portas 443 e 1443 no equipamento de rede e no servidor proxy de sua organização.
- Quando o Servidor de Administração interage com os servidores de atualização Kaspersky e os servidores da Kaspersky Security Network, é necessário evitar o sequestro do tráfego de rede com substituição de certificado (ataques MITM).

Para baixar as atualizações usando o protocolo HTTP ou HTTPS com o utilitário klscflag:

1. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Caso queira baixar as atualizações usando o protocolo HTTP, execute um dos seguintes comandos com a conta root:

   - No dispositivo com o Servidor de Administração instalado:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Em um ponto de distribuição:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Caso queira baixar as atualizações usando o protocolo HTTPS, execute um dos seguintes comandos com a conta root:

   - No dispositivo com o Servidor de Administração instalado:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - Em um ponto de distribuição:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Lista de sub-redes globais

Para cada Servidor de Administração usado, você pode configurar uma lista global de sub-redes para armazenar as informações sobre as sub-redes da sua rede. Esta lista ajuda você a combinar pares {endereço IP, máscara} e unidades físicas, como escritórios de filiais. Você pode usar sub-redes desta lista nas regras e configurações de rede.

Para adicionar sub-redes à lista global de sub-redes:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Sub-redes globais**.

3. Clique em **Adicionar**.

   A janela **Nova sub-rede** se abre.

4. Preencha os campos a seguir:

   - **Nome**
   - **Endereço de sub-rede**
   - **Máscara de sub-rede**
   - **Descrição**

5. Clique no botão **Salvar**.

A janela é fechada e a sub-rede aparece na lista de sub-redes.

Se necessário, você pode fazer o seguinte na lista de sub-redes globais:

- Excluir sub-redes da lista selecionando a sub-rede desejada e clicando no botão **Remover**.
- Modificar as propriedades das sub-redes clicando no link com o nome da sub-rede desejada e executando as ações descritas nas etapas 4 e 5.

Verificar a integridade dos módulos usando os utilitários klscmodchk e integrity_checker

O Kaspersky Security Center Linux contém vários módulos binários na forma de bibliotecas vinculadas dinamicamente, arquivos executáveis, arquivos de configuração e arquivos de interface. Um invasor pode substituir um ou mais módulos executáveis ou arquivos de aplicativo por outros arquivos que contenham código malicioso. Para evitar a falsificação de módulos e arquivos, o Kaspersky Security Center Linux implementa uma verificação de integridade dos componentes usando os utilitários klscmodchk e integrity_checker. Esses utilitários verificam módulos e arquivos em busca de alterações não autorizadas ou danos. Se um módulo ou arquivo de aplicativo tiver uma soma de verificação incorreta, ele será considerado danificado.

O utilitário klscmodchk executa verificações de integridade para os seguintes componentes do Kaspersky Security Center Linux:

- Servidor de Administração
- Agente de Rede

O utilitário integrity_checker executa verificações de integridade para os seguintes componentes do Kaspersky Security Center Linux:

- Servidor de Administração
- Agente de Rede
- Kaspersky Security Center Web Console

Ambos os utilitários verificam a integridade do módulo com base no arquivo de manifesto kl_file_integrity_manifest.xml, que faz parte da compilação do Kaspersky Security Center Linux e está localizado na pasta de instalação. O arquivo de manifesto do componente contém arquivos cuja integridade é importante para a operação correta do componente Kaspersky Security Center Linux. A integridade dos próprios arquivos de manifesto também é verificada.

Não é recomendável, de forma alguma, modificar o arquivo de manifesto kl_file_integrity_manifest.xml, pois isso invalidará a assinatura digital e fará com que a verificação de integridade falhe.

Para verificar a integridade do componente do Kaspersky Security Center Linux, execute um dos seguintes comandos:

- `klscmodchk [ parâmetros ]`

  O utilitário klscmodchk inicia o utilitário integrity_checker com o parâmetro `--verbose` e verifica a integridade dos módulos.

  Parâmetros para o utilitário klscmodchk:

  - `-logfile < caminho_do_arquivo_de_log >`. Especifique o caminho para um arquivo no disco para registrar os logs. Por padrão, as informações são enviadas para o console.
  - `-verbose`: exibir informações detalhadas durante a verificação de integridade.

- `integrity_checker [ parâmetros ] < manifest_file_path >`

  Parâmetros para o utilitário integrity_checker:

  - `--help`: exibe a ajuda do utilitário integrity_checker.
  - `--version`: exibe a versão do utilitário integrity_checker.
  - `--verbose`: exibe informações sobre a operação do utilitário. Ao executar uma verificação de integridade, é suficiente usar esse parâmetro no comando.

O resultado da verificação de cada arquivo de manifesto é exibido ao lado do nome do arquivo de manifesto no seguinte formato:

- SUCESSO: integridade do arquivo confirmada (código de retorno 0).
- FALHA: integridade do arquivo não confirmada (código de retorno diferente de zero).

Também é possível configurar as verificações de integridade para serem iniciadas automaticamente ao iniciar o aplicativo. Por padrão, a verificação de integridade automática está desativada.

Para ativar a verificação de integridade automática:

1. No dispositivo em que o Servidor de Administração está instalado, insira o seguinte comando no prompt de comando:

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Reinicie o dispositivo.

A verificação de integridade automática está ativada.

Na próxima execução do Kaspersky Security Center, o utilitário klscmodchk será executado junto com o Servidor de Administração e iniciará a verificação de integridade dos módulos. O resultado das verificações de integridade é escrito no Registro de eventos da Kaspersky.

Localizar dispositivos na rede

Esta seção descreve a pesquisa e a descoberta de dispositivos em rede.

O Kaspersky Security Center Linux permite encontrar dispositivos com base em critérios especificados. Você pode salvar os resultados da pesquisa em um arquivo de texto.

O recurso de pesquisa e localização lhe permite localizar os seguintes dispositivos:

- Os dispositivos gerenciados nos grupos de administração do Servidor de Administração do Open Single Management Platform e seus Servidores de Administração secundários.
- Dispositivos não atribuídos gerenciados pelo Servidor de Administração e por seus Servidores de Administração secundários.

Cenário: Localizar dispositivos na rede

Você deve executar a localização de dispositivos antes da instalação dos aplicativos de segurança. Quando todos os dispositivos em rede forem localizados, você pode receber informações sobre eles e gerenciá-los por meio de políticas. Sondagens de rede regulares são necessárias para saber se há algum novo dispositivo e se os dispositivos anteriormente localizados ainda estão na rede.

A localização de dispositivos na rede prossegue em estágios:

1. **Descoberta de dispositivos inicial**

   Ao concluir o assistente de início rápido, execute a descoberta de dispositivos manualmente.

2. **Configuração de sondagens futuras**

   Certifique-se de que a sondagem de conjunto de IPs esteja ativada e de que o agendamento da amostragem atenda às necessidades da sua organização. Ao configurar o agendamento da sondagem, use as recomendações para a frequência de sondagem de rede.

   Você também pode habilitar a Sondagem Zeroconf se sua rede incluir dispositivos IPv6.

   Se os dispositivos em rede estiverem incluídos em um domínio, recomenda-se usar a sondagem do controlador de domínio.

   Use pontos de distribuição baseados no Windows para sondar redes do Windows.

3. **Configuração de regras para adicionar dispositivos descobertos a grupos de administração (opcionais)**

   Novos dispositivos aparecem na rede após serem detectados durante as sondagens de rede. Esses dispositivos são automaticamente incluídos no grupo **Dispositivos não atribuídos**. Se quiser, você poderá configurar as regras para mover esses dispositivos para o grupo **Dispositivos gerenciados**. Você também pode estabelecer regras de retenção.

   Se você ignorar este estágio de configuração de regra, todos os dispositivos recentemente localizados serão movidos para o grupo **Dispositivos não atribuídos** e ficarão lá. Se quiser, você poderá mover esses dispositivos para o grupo **Dispositivos gerenciados** manualmente. Se mover os dispositivos para o grupo **Dispositivos gerenciados**, você poderá analisar informações sobre cada dispositivo e decidir se deseja movê-lo para um grupo de administração e, nesse caso, para qual grupo.

Resultados

A conclusão do cenário produz o seguinte:

- O Servidor de Administração do Kaspersky Security Center Linux descobre os dispositivos que estão na rede e fornece informações sobre eles.
- As sondagens futuras são realizadas segundo o agendamento especificado.

Os dispositivos recém-descobertos são alocados de acordo com as regras especificadas. Se nenhuma regra for configurada, os dispositivos permanecerão no grupo **Dispositivos não atribuídos**.

Sondagem da rede do Windows

Sobre a sondagem de rede do Windows

O Servidor de Administração Kaspersky Security Center Linux não é compatível com a sondagem de rede do Windows. Use pontos de distribuição baseados no Windows para sondar redes do Windows.

Durante uma sondagem rápida, os pontos de distribuição só recuperam a informação da lista dos nomes de NetBIOS dos dispositivos em todos os domínios da rede e grupos de trabalho. Durante uma sondagem completa, as seguintes informações são solicitadas de cada dispositivo cliente:

- Nome de sistema operacional
- Endereço IP
- Nome DNS
- Nome NetBIOS

As sondagens rápida e completa requerem o seguinte:

- Portas UDP 137/138, TCP 139, UDP 445, TCP 445 devem estar disponíveis na rede.
- O protocolo SMB está ativado.
- O serviço Microsoft Computer Browser deve ser usado, e o navegador principal do computador deve estar ativado no Servidor de Administração.
- O serviço Microsoft Computer Browser deve ser usado, e o navegador principal do computador deve estar ativado nos dispositivos cliente:
  - Em pelo menos um dispositivo, se o número de dispositivos em rede não exceder 32.
  - Em pelo menos um dispositivo para cada 32 dispositivos em rede.

A sondagem completa poderá ser executada apenas se a sondagem rápida tiver sido executada pelo menos uma vez.

Sondagem do conjunto de IPs

O Kaspersky Security Center Linux tenta executar a resolução de nome inversa para cada endereço IPv4 do intervalo especificado para um nome de DNS usando solicitações de DNS padrão. Se essa operação tiver sucesso, o servidor enviará uma `ICMP ECHO REQUEST` (da mesma forma que o comando ping) ao nome recebido. Se o dispositivo responder, as informações sobre ele serão adicionadas ao banco de dados do Kaspersky Security Center Linux. A resolução de nome inversa é necessária para excluir dispositivos de rede que podem ter um endereço IP, mas não são computadores, por exemplo, impressoras de rede ou roteadores.

Esse método de sondagem depende de um serviço de DNS local corretamente configurado. Ele deve ter uma zona de pesquisa inversa. Se essa zona não estiver configurada, a sondagem de sub-rede IP não produzirá nenhum resultado.

Inicialmente, o Kaspersky Security Center Linux adquire intervalos de IPs para amostragem a partir das configurações de rede do dispositivo no qual está instalado. Se o endereço de dispositivo for 192.168.0.1 e a máscara de sub-rede for 255.255.255.0, o Kaspersky Security Center Linux incluirá a rede 192.168.0.0/24 na lista do endereço de amostragem automaticamente. O Kaspersky Security Center Linux faz a amostragem de todos os endereços de 192.168.0.1 a 192.168.0.254.

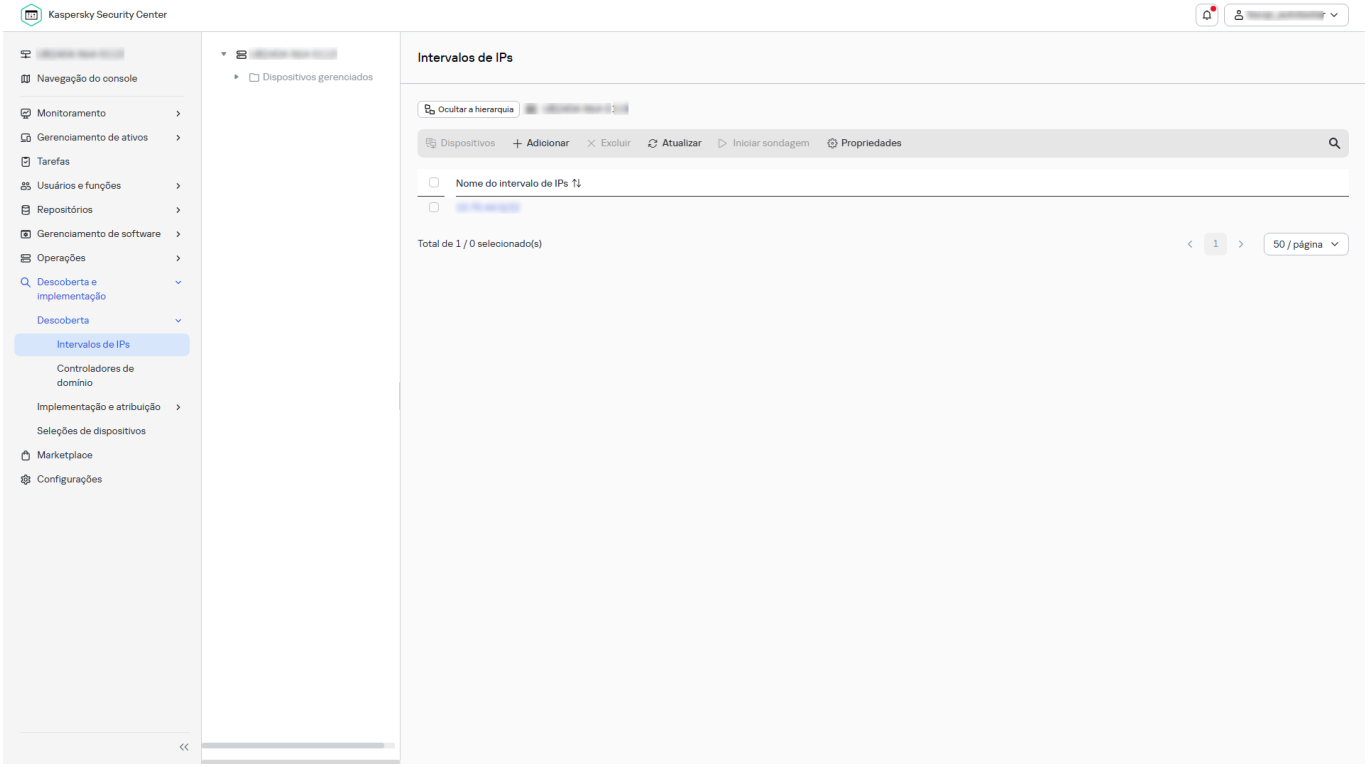
Se apenas a sondagem de conjunto de IPs estiver habilitada, o Kaspersky Security Center Linux descobrirá dispositivos apenas com endereços IPv4. Se sua rede incluir dispositivos IPv6, ative a Sondagem Zeroconf de dispositivos.

Para todos os hosts baseados em Linux dentro de um controlador de domínio Microsoft Active Directory, Samba, FreeIPA ou ALD Pro, especifique o `netbios name` e os parâmetros do `workgroup` no arquivo `/etc/samba/smb.conf`. Caso contrário, os resultados da pesquisa podem conter hosts duplicados.

Visualização e modificação de configurações para amostragem de faixas IP

Para visualizar e modificar as propriedades para amostragem de faixas IP:

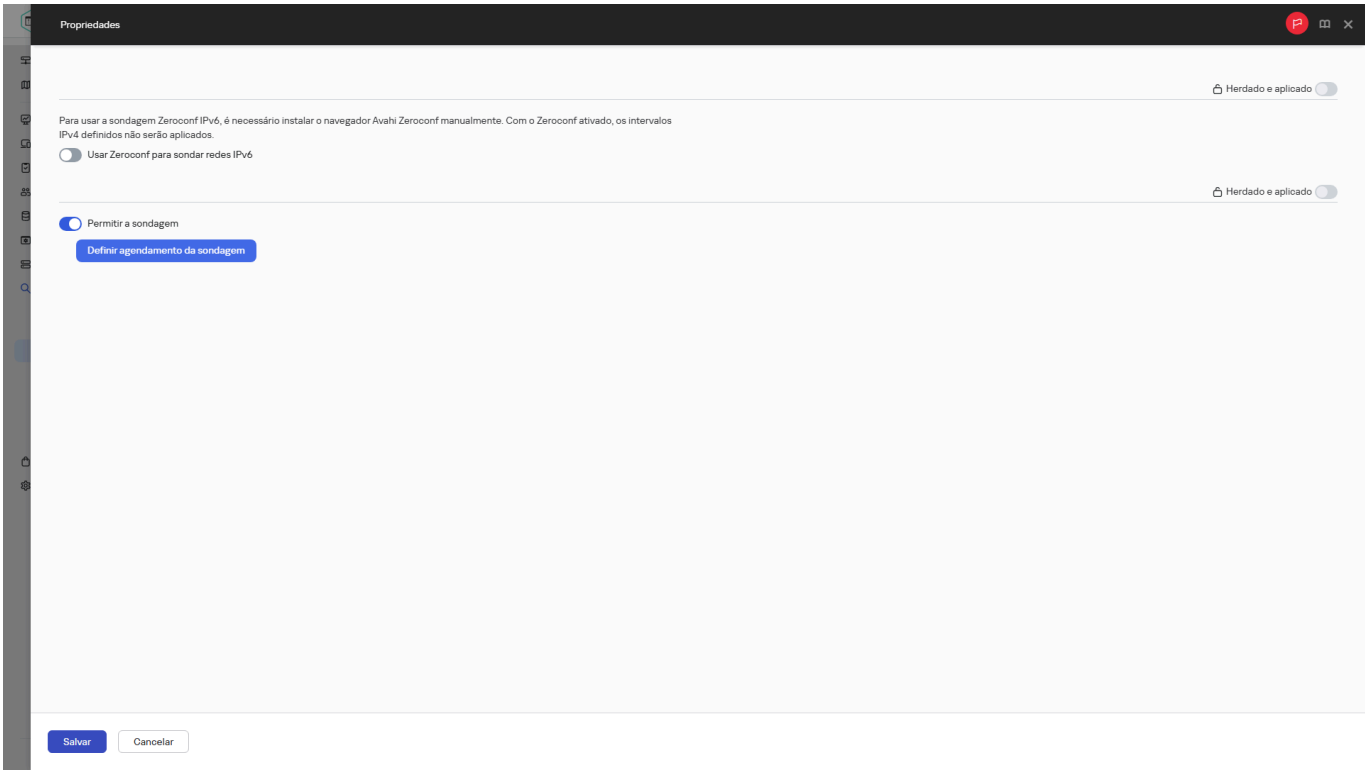
1. No menu principal, vá para **Descoberta e implementação** → **Descoberta** → **Intervalos de IPs**.



Lista de intervalos de IP

2. Clique no botão **Propriedades**.

   A janela de propriedades da Sondagem de IPs se abre.



As propriedades da sondagem de IPs

3. Ative ou desative a Sondagem de IPs usando o botão de alternar **Permitir a sondagem**.

4. Configure o agendamento da amostragem. Por padrão, a amostragem de IP é executada a cada 420 minutos (sete horas).

   Ao especificar o intervalo de amostragem, assegure-se de que essa configuração não exceda o valor do parâmetro de duração do endereço IP. Se um endereço IP não for verificado por sondagem durante a duração do endereço IP, esse endereço IP será automaticamente removido dos resultados da sondagem. Por padrão, a duração dos resultados da sondagem é de 24 horas, pois os endereços IP dinâmicos (atribuídos com o uso de Dynamic Host Configuration Protocol (DHCP)) mudam a cada 24 horas.

   Opções de agendamento da sondagem:

   - **A cada N dias**

     A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

     Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

   - **A cada N minutos**

     A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

   - **Por dias da semana**

     A sondagem é executada regularmente, nos dias da semana e na hora especificados.

   - **Mensalmente em um dia da semana selecionado**

     A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

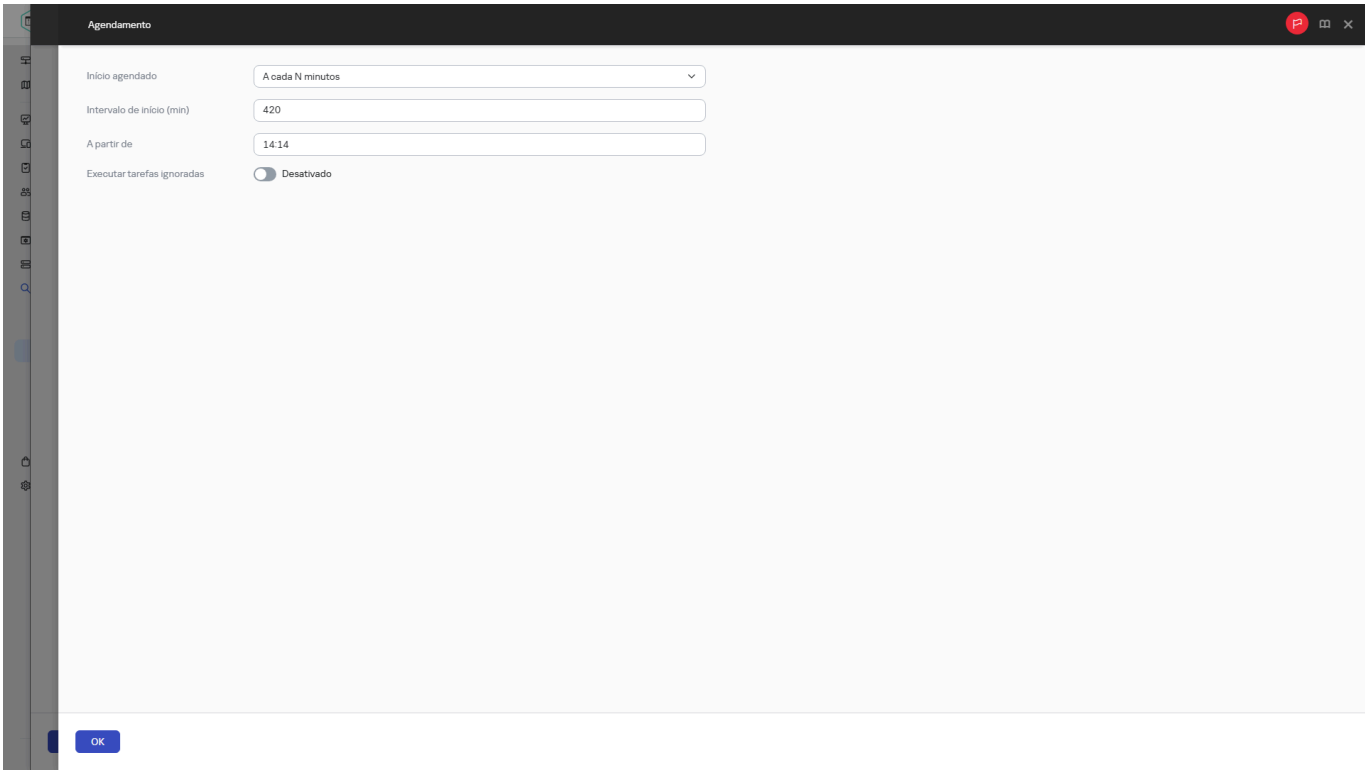
   - **Executar tarefas ignoradas**

     Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

     Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

     Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

Por padrão, esta opção está desativada.



Configurar o agendamento da sondagem

5. Clique no botão **Salvar**.

As propriedades são salvas e aplicadas a todos os conjuntos de IPs.

Execução da amostragem manualmente

Para executar a amostragem imediatamente,

Clique em **Iniciar sondagem**.

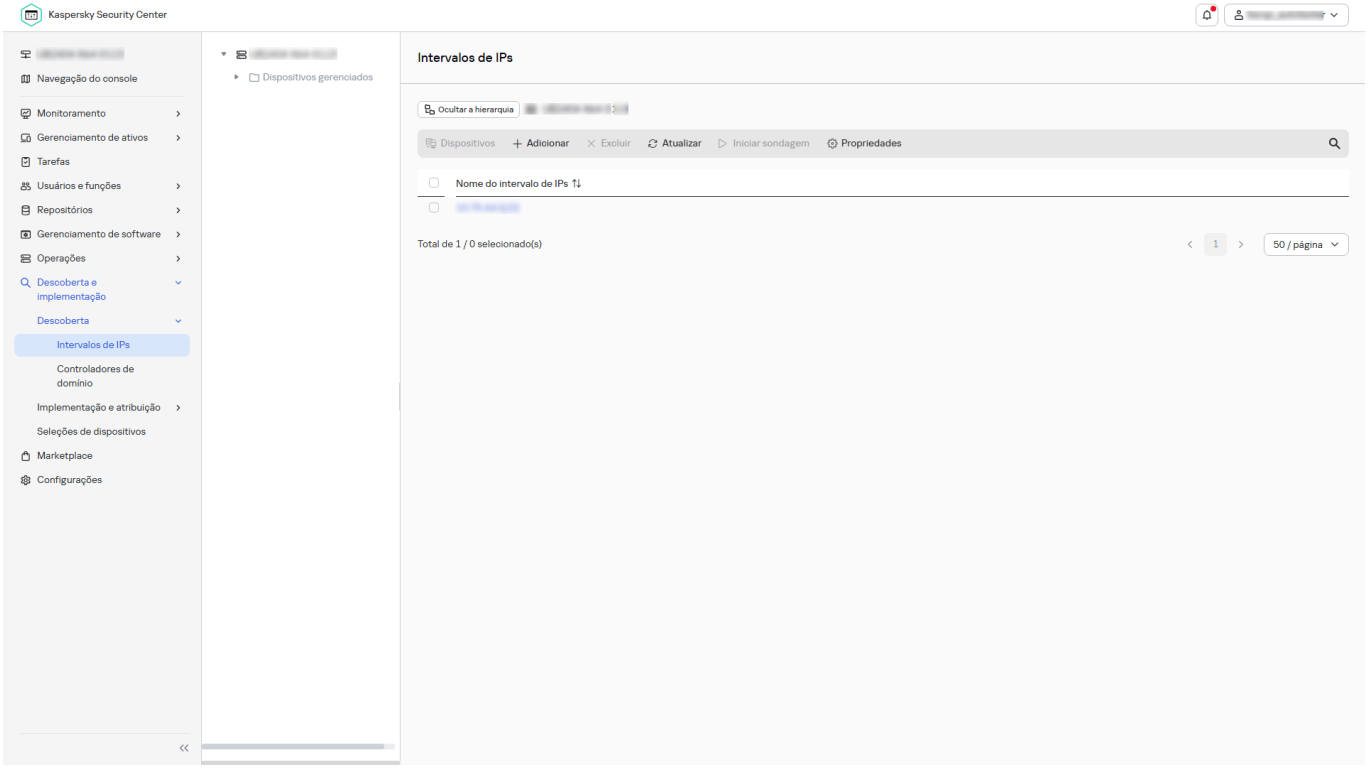
Adição e modificação de um conjunto de IPs

Inicialmente, o Kaspersky Security Center Linux adquire intervalos de IPs para amostragem a partir das configurações de rede do dispositivo no qual está instalado. Se o endereço de dispositivo for 192.168.0.1 e a máscara de sub-rede for 255.255.255.0, o Kaspersky Security Center Linux incluirá a rede 192.168.0.0/24 na lista do endereço de amostragem automaticamente. O Kaspersky Security Center Linux faz a amostragem de todos os endereços de 192.168.0.1 a 192.168.0.254. Você pode modificar os conjuntos de IPs definidos automaticamente ou adicionar conjuntos de IPs personalizados.

Você pode criar um intervalo apenas para endereços IPv4. Caso a sondagem Zeroconf seja ativada, o Kaspersky Security Center Linux sondará toda a rede.

Para adicionar um novo conjunto de IPs:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Intervalos de IPs**.



Lista de intervalos de IP

2. Para adicionar um novo conjunto de IPs, clique no botão **Adicionar**.

3. Na janela que for aberta, especifique as seguintes configurações:

   Nome do intervalo de IPs

   Um nome do conjunto de IPs. Você pode especificar o próprio conjunto de IPs como o nome, por exemplo, "192.168.0.0/24".

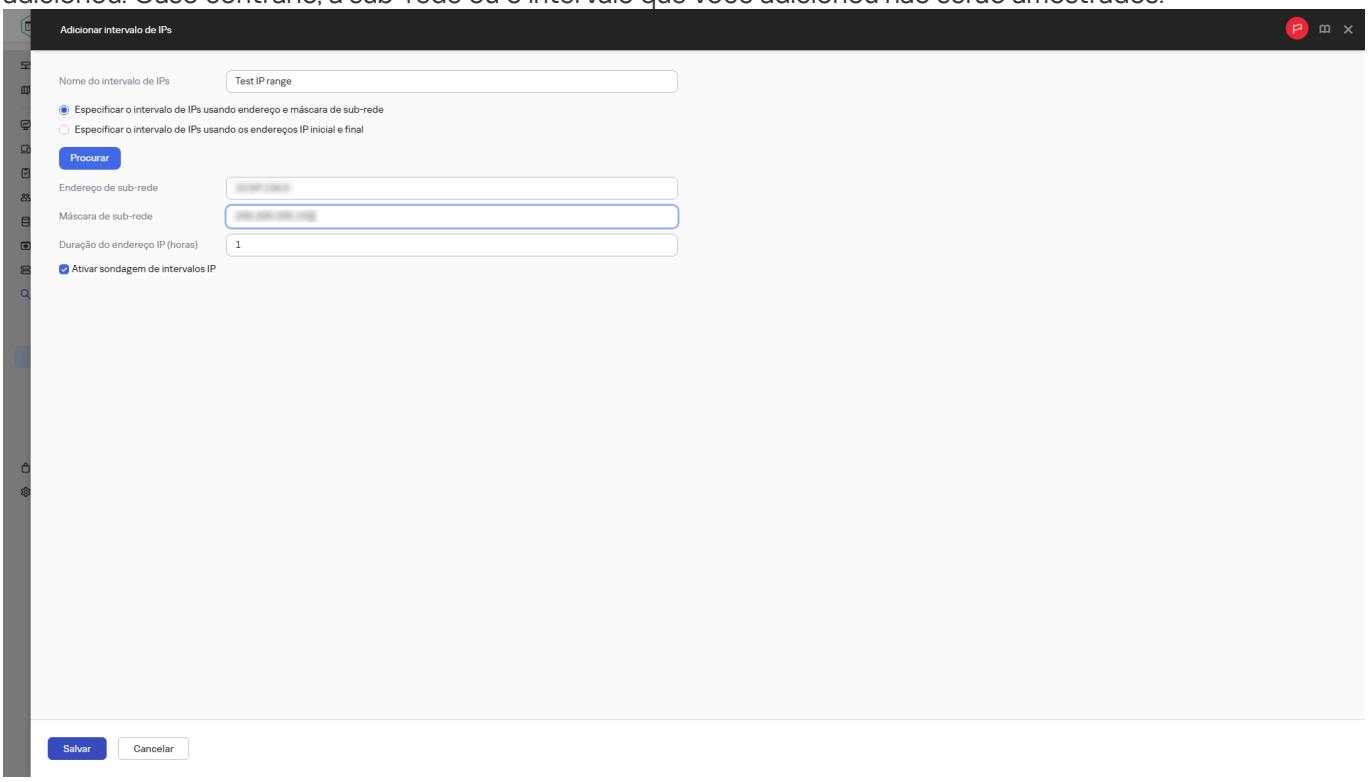
   Intervalo de IP ou endereço e máscara de sub-rede

   Defina o conjunto de IPs especificando os endereços IP inicial e final ou o endereço de sub-rede e a máscara de sub-rede. Você também pode selecionar um dos conjuntos de IPs já existentes clicando no botão **Procurar**.

   Duração do endereço IP (horas)

   Ao especificar esse parâmetro, verifique se ele excede o conjunto de intervalos de sondagem no agendamento de sondagem. Se um endereço IP não for verificado por sondagem durante a duração do endereço IP, esse endereço IP será automaticamente removido dos resultados da sondagem. Por padrão, a duração dos resultados da sondagem é de 24 horas, pois os endereços IP dinâmicos (atribuídos com o uso de Dynamic Host Configuration Protocol (DHCP)) mudam a cada 24 horas.

4. Selecione **Ativar sondagem de intervalos IP** se quiser fazer a amostragem da sub-rede ou do intervalo que adicionou. Caso contrário, a sub-rede ou o intervalo que você adicionou não serão amostrados.



Especificação de configurações de intervalo de IP

5. Clique no botão **Salvar**.

   O novo conjunto de IPs é adicionado à lista de conjuntos de IPs.

Você pode executar a amostragem de cada conjunto de IPs separadamente usando o botão **Iniciar sondagem**. Por padrão, a duração dos resultados da sondagem é de 24 horas e é igual à configuração de duração do endereço IP.

Para adicionar uma sub-rede a um conjunto de IPs existente:

1. No menu principal, vá para **Descoberta e implementação** → **Descoberta** → **Intervalos de IPs**.

2. Clique no nome do conjunto de IPs ao qual deseja adicionar uma sub-rede.

3. Na janela que se abre, clique no botão **Adicionar**.

4. Especifique uma sub-rede usando o seu endereço e máscara ou usando o primeiro e o último endereço IP no conjunto de IPs. Ou adicione uma sub-rede existente clicando no botão **Procurar**.

5. Clique no botão **Salvar**.

   A nova sub-rede é adicionada ao conjunto de IPs.

6. Clique no botão **Salvar**.

   As novas configurações do conjunto de IPs são salvas.

Você pode adicionar quantas sub-redes precisar. Não é permitido que os conjuntos de IPs se sobreponham, mas as sub-redes não nomeadas dentro de um conjunto de IPs não têm tais restrições. Você pode ativar e desativar a amostragem independentemente para cada conjunto de IPs.

Sondagem Zeroconf

Este tipo de pesquisa é compatível apenas com pontos de distribuição baseados em Linux.

O Kaspersky Security Center Linux pode sondar as redes que possuem dispositivos com endereços IPv6. Nesse caso, os intervalos IP não são especificados e o Kaspersky Security Center Linux sonda toda a rede usando a rede zero configuração (também chamada de *Zeroconf*). Para começar a usar o Zeroconf, você deve instalar os componentes do avahi (avahi-utils) no dispositivo Linux que sonda as redes, ou seja, o Servidor de Administração ou um ponto de distribuição.

Ao usar o Zeroconf, o Servidor de Administração ou o ponto de distribuição verifica a rede para descobrir dispositivos compatíveis com o protocolo Zeroconf e os adiciona temporariamente à lista. Em seguida, é realizado um ping ICMPv6 para cada dispositivo para verificar sua disponibilidade, e o serviço avahi faz uma pesquisa DNS reversa para obter os nomes DNS correspondentes aos endereços IPv6. As informações sobre o sistema host (nome DNS e tipo de sistema operacional) são registradas no banco de dados do Kaspersky Security Center Linux.

O escopo da sondagem Zeroconf é determinado pelas configurações do serviço avahi. Por padrão, é realizada uma sondagem por difusão em uma sub-rede. Se várias interfaces de rede estiverem configuradas no dispositivo que hospeda o Servidor de Administração ou o ponto de distribuição, o serviço avahi sonda as sub-redes associadas a todas as interfaces ativas.

Recomendações para a conclusão bem-sucedida de uma sondagem Zeroconf

- Verifique se as seguintes configurações foram definidas no arquivo /etc/avahi/avahi-daemon.conf:
  - No Servidor de Administração ou no ponto de distribuição:
    ```
    [server]
    use-ipv6=yes
    ```
  - Nos dispositivos:
    ```
    [server]
    use-ipv6=yes
    [publish]
    publish-addresses=yes
    publish-workstation=yes
    ```
- Certifique-se de que a seguinte linha esteja presente no arquivo /etc/nsswitch.conf:
  - No Servidor de Administração ou no ponto de distribuição:
    ```
    mdns_minimal [NOTFOUND=return] dns
    ```

Para habilitar a sondagem do Zeroconf:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Intervalos de IPs**.
2. Clique no botão **Propriedades**.
3. Na janela aberta, ative o botão **Usar Zeroconf para sondar redes IPv6**.

Em seguida, o Kaspersky Security Center Linux começa a sondar a rede. Nesse caso, os intervalos IP especificados são ignorados.

Sondagem do controlador de domínio

O Kaspersky Security Center Linux é compatível com a sondagem dos seguintes tipos de controlador de domínio:

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

Para um controlador de domínio Samba, o Samba 4 é usado como um controlador de domínio do Active Directory.

Ao fazer a sondagem de um controlador de domínio, o Servidor de Administração ou um ponto de distribuição recupera as informações sobre a estrutura do domínio, contas de usuário, grupos de segurança e nomes DNS dos dispositivos incluídos no domínio.

Recomendamos usar a sondagem do controlador de domínio se todos os dispositivos em rede forem membros de um domínio. Caso alguns dos dispositivos em rede não estejam incluídos no domínio, esses dispositivos não poderão ser descobertos pela sondagem do controlador de domínio.

Pré-requisitos

Antes de fazer a sondagem de um controlador de domínio, é necessário permitir as conexões com o controlador de domínio por meio de um firewall ou de um servidor proxy. Também é necessário que os seguintes protocolos estejam ativados no controlador de domínio:

- Lightweight Directory Access Protocol (LDAP)
- Simple Authentication and Security Layer (SASL)

  Esse protocolo é usado caso a conexão com o controlador de domínio seja estabelecida com o uso da autenticação SASL. O Servidor de Administração e os pontos de distribuição são compatíveis apenas com o mecanismo DIGEST-MD5.

- Lightweight Directory Access Protocol sobre Secure Sockets Layer (LDAPS)

  Esse protocolo é usado caso seja necessário se conectar ao controlador de domínio por meio de uma conexão criptografada.

Certifique-se de que as seguintes portas estão disponíveis no dispositivo controlador de domínio:

- 389 para o protocolo LDAP e autenticação simples (inclusive SASL)
- 636 para o protocolo LDAPS

No FreeIPA e no ALD Pro, os protocolos LDAP e LDAPS são usados apenas para a sondagem de domínio. O Kaspersky Security Center Linux não é compatível com a autenticação de contas do FreeIPA por meio do LDAP(S). Para permitir que os usuários do FreeIPA e do ALD Pro façam login no Web Console, você deve configurar a autenticação Kerberos por meio do serviço IAM.

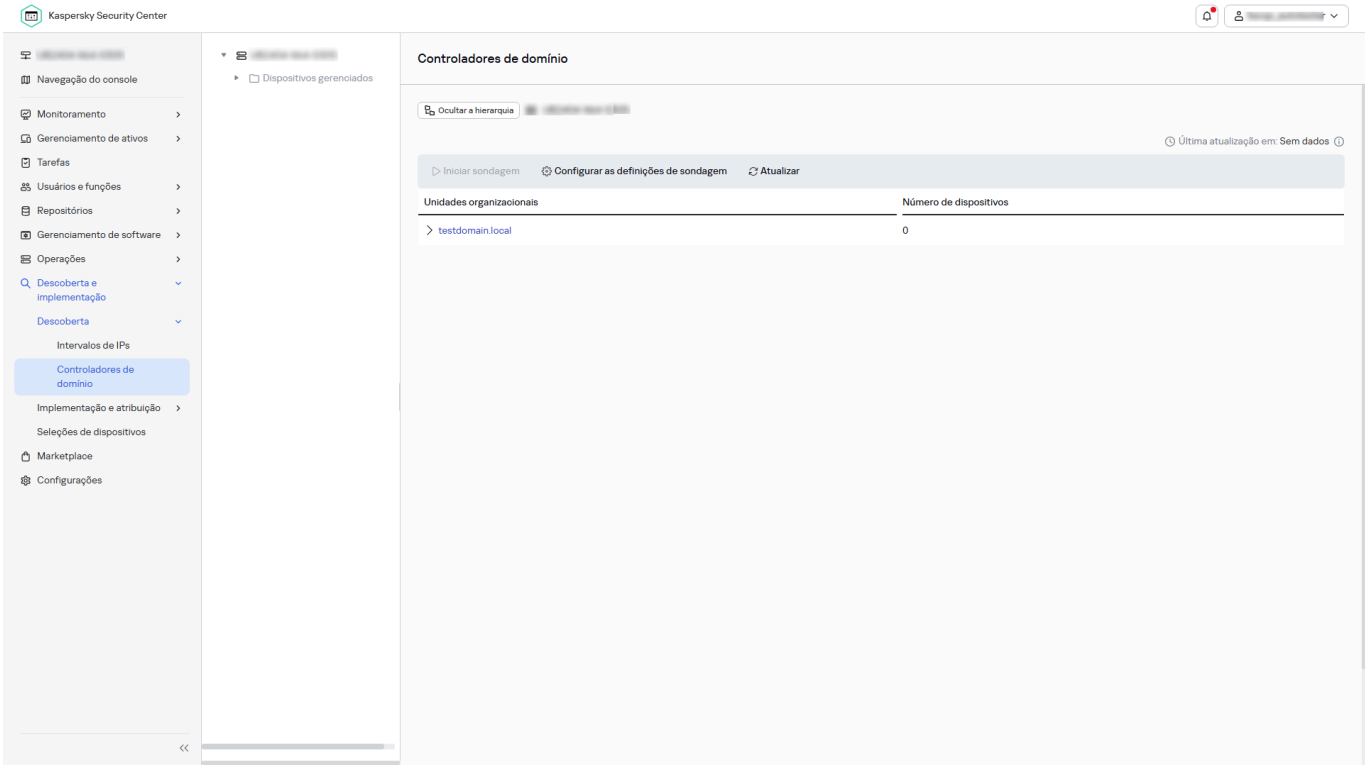
Para todos os hosts baseados em Linux dentro de um controlador de domínio Microsoft Active Directory, Samba, FreeIPA ou ALD Pro, será necessário especificar o `netbios name` e os parâmetros do `workgroup` no arquivo `/etc/samba/smb.conf`. Caso contrário, os resultados da pesquisa podem conter hosts duplicados.

Se um domínio do Microsoft Active Directory contiver vários controladores de domínio, a seleção de um controlador específico durante a sondagem de domínio não será compatível. A conexão é estabelecida com o primeiro controlador de domínio detectado. Para garantir a autenticação adequada com o domínio do Microsoft Active Directory, o campo Nome alternativo da entidade (SAN) do certificado deve incluir todos os endereços dos controladores de domínio incluídos nesse domínio, bem como o nome NetBIOS do domínio do Microsoft Active Directory.

A sondagem do controlador de domínio com o uso do Servidor de Administração

Para sondar um controlador de domínio com o uso do Servidor de Administração:

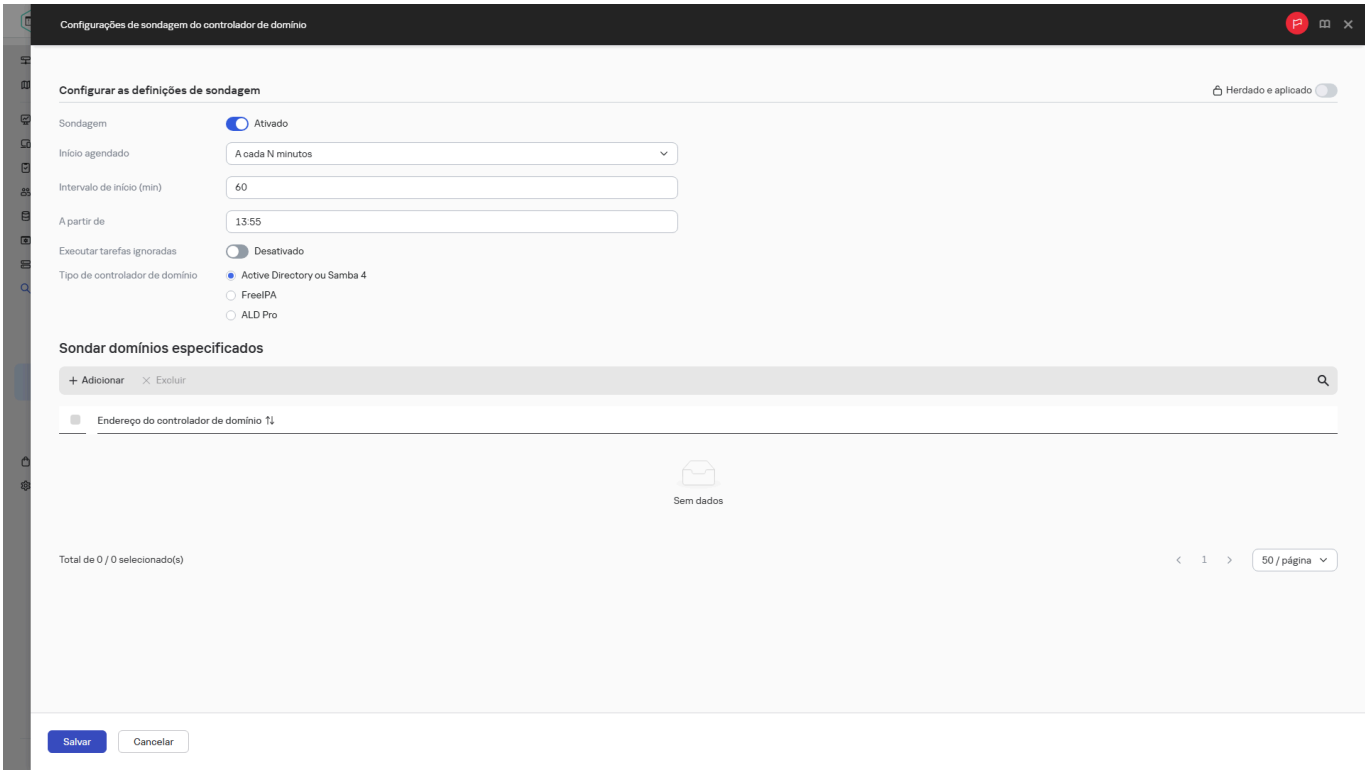
1. No menu principal, vá para **Descoberta e implementação → Descoberta → Controladores de domínio**.



Janela de sondagem do controlador de domínio

2. Clique em **Configurar as definições de sondagem**.

   A janela **Configurações de sondagem do controlador de domínio** é exibida.



Configurações de sondagem do controlador de domínio

3. No campo **Sondagem**, mude a posição do botão de alternância para **Ativado**.

4. Em **Sondar domínios especificados**, clique em **Adicionar** e especifique o endereço e as credenciais de usuário do controlador de domínio.

5. Na janela **Configurações de sondagem do controlador de domínio**, faça o seguinte:

   - Selecione o tipo de controlador de domínio a ser sondado: **Active Directory ou Samba 4**, **FreeIPA**, **ALD Pro**.

   - Caso necessário, defina o agendamento da sondagem. O período padrão é de uma hora. Os dados recebidos na próxima sondagem substituem completamente os dados antigos.

     As seguintes opções de agendamento da sondagem estão disponíveis:

     A cada N dias

     A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

     Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

     A cada N minutos

     A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

     Por dias da semana

     A sondagem é executada regularmente, nos dias da semana e na hora especificados.

     Mensalmente em um dia da semana selecionado

     A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

Executar tarefas ignoradas

Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

Por padrão, esta opção está desativada.

Caso as contas de usuário sejam alteradas em um grupo de segurança do domínio, essas alterações serão exibidas no Kaspersky Security Center Linux uma hora após a sondagem do controlador de domínio.

6. Clique em **Salvar** para aplicar as alterações.

7. Caso queira executar a sondagem imediatamente, clique no botão **Iniciar sondagem**.

A sondagem do controlador de domínio com o uso de um ponto de distribuição

Também é possível sondar um controlador de domínio com o uso de um ponto de distribuição. Um dispositivo gerenciado baseado em Windows ou Linux pode atuar como um ponto de distribuição.

Para um ponto de distribuição baseado em Linux, há suporte para a sondagem de todos os tipos de controlador de domínio.
Para um ponto de distribuição baseado em Windows, há suporte apenas para a sondagem de um controlador de domínio do Microsoft Active Directory.
Não há suporte para a sondagem com um ponto de distribuição do Mac.

Para configurar a sondagem do controlador de domínio com o uso do ponto de distribuição:

1. Abra as propriedades do ponto de distribuição.

2. Selecione a seção **Sondagem do controlador de domínio**.

3. No campo **Sondagem**, mude a posição do botão de alternância para **Ativado**.

4. Se você usar um ponto de distribuição do Linux, selecione o tipo de controlador de domínio a ser sondado: **Active Directory ou Samba 4**, **FreeIPA**, **ALD Pro**.

   Não é necessário especificar o mesmo tipo de controlador de domínio ao configurar a sondagem usando um ponto de distribuição e o Servidor de Administração.

5. Selecione o controlador de domínio que deseja sondar.

   Caso queira usar um ponto de distribuição do Linux, na seção **Sondar domínios especificados**, clique em **Adicionar** e especifique o endereço e as credenciais de usuário do controlador de domínio.

Se você usar um ponto de distribuição do Windows, poderá selecionar uma das seguintes opções:

- **Sondar domínio atual**
- **Sondar toda a floresta de domínios**
- **Sondar domínios especificados**

6. Clique no botão **Definir agendamento da sondagem** para especificar as opções de agendamento de sondagem, caso seja necessário.

   A sondagem é iniciada de acordo com o agendamento especificado apenas. O início manual da sondagem não está disponível.

Após a conclusão da sondagem, a estrutura do domínio será exibida na seção **Controladores de domínio**.

Se você tiver configurado e ativado as regras para migrar dispositivos, os dispositivos recentemente descobertos estarão automaticamente incluídos no grupo **Dispositivos gerenciados**. Se nenhuma regra de movimento tiver sido ativada, os dispositivos recentemente descobertos serão automaticamente incluídos no grupo **Dispositivos não atribuídos**.

As contas de usuário descobertas podem ser usadas para autenticação de domínio no Kaspersky Security Center Web Console.

Autenticação e conexão com um controlador de domínio

Autenticação e conexão com um controlador de domínio ao efetuar a sondagem de um domínio

Ao efetuar a sondagem de um controlador de domínio, o Servidor de Administração ou um ponto de distribuição identifica o protocolo de conexão para estabelecer a conexão inicial com o controlador de domínio. Esse protocolo é usado para todas as conexões futuras com o controlador de domínio. Ao estabelecer a conexão inicial com o controlador de domínio, você pode alterar as opções de conexão usando os sinalizadores do Agente de Rede (`KLNAG_LDAP_TLS_REQCERT` e `KLNAG_LDAP_SSL_CACERT`). Você pode configurar os sinalizadores do Agente de Rede usando o comando klscflag, conforme descrito neste artigo.

A conexão inicial com um controlador de domínio prossegue da seguinte forma:

1. O Servidor de Administração ou um ponto de distribuição tenta se conectar ao controlador de domínio através do LDAPS.

   Por padrão, a verificação do certificado não é necessária. Defina o sinalizador `KLNAG_LDAP_TLS_REQCERT` como 1 para impor a verificação do certificado.

   Valores possíveis do sinalizador `KLNAG_LDAP_TLS_REQCERT`:

   - `0` — O certificado é solicitado, mas se não for fornecido ou se a verificação do certificado falhar, a conexão TLS ainda será considerada criada com êxito (valor padrão).
   - `1` — É necessária a verificação estrita do certificado do servidor LDAP.

Por padrão, se o sinalizador `KLNAG_LDAP_SSL_CACERT` não estiver especificado, o caminho dependente do SO usará o caminho padrão para acessar a autoridade de certificação (CA) e a cadeia de certificados. Use o sinalizador `KLNAG_LDAP_SSL_CACERT` para especificar um caminho personalizado.

2. Se a conexão LDAPS falhar, o Servidor de Administração ou um ponto de distribuição tentará se conectar ao controlador de domínio através de uma conexão TCP não criptografada usando SASL (DIGEST-MD5).

Autenticação e conexão a um controlador de domínio ao autenticar um usuário de domínio no Servidor de Administração

Quando um usuário de domínio se autentica no Servidor de Administração, o Servidor de Administração identifica o protocolo para estabelecer a conexão com o controlador de domínio.

No FreeIPA e no ALD Pro, os protocolos LDAP e LDAPS são usados apenas para a sondagem de domínio. O Kaspersky Security Center Linux não é compatível com a autenticação de contas do FreeIPA por meio do LDAP(S). Para permitir que os usuários do FreeIPA e do ALD Pro façam login no Web Console, você deve configurar a autenticação Kerberos por meio do serviço IAM.

A conexão com um controlador de domínio prossegue da seguinte forma:

1. O Servidor de Administração tenta se conectar ao controlador de domínio via LDAPS.

   A verificação rigorosa do certificado do servidor LDAP é obrigatória.

   Por padrão, se o sinalizador `KLNAG_LDAP_SSL_CACERT` não estiver especificado, o caminho dependente do SO usará o caminho padrão para acessar a autoridade de certificação (CA) e a cadeia de certificados. Use o sinalizador `KLNAG_LDAP_SSL_CACERT` para especificar um caminho personalizado.

2. Se a conexão LDAPS falhar, ocorrerá um erro ao conectar-se ao controlador de domínio e outros protocolos de conexão não serão usados.

Configurar sinalizadores

É possível usar o utilitário klscflag para configurar sinalizadores.

Execute a linha de comando e, em seguida, altere o diretório atual para o diretório com o utilitário klscflag. No dispositivo do Servidor de Administração, o utilitário klscflag está localizado no diretório de instalação. O caminho de instalação padrão é /opt/kaspersky/ksc64/sbin.

Por exemplo, o seguinte comando impõe a verificação do certificado:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Configuração de um controlador de domínio Samba

O Kaspersky Security Center Linux é compatível apenas com um controlador de domínio Linux executado no Samba 4.

Um controlador de domínio Samba é compatível com as mesmas extensões de esquema que um controlador de domínio Microsoft Active Directory. É possível ativar a compatibilidade total de um controlador de domínio Samba com um controlador de domínio Microsoft Active Directory usando a extensão de esquema Samba 4. Essa é uma ação opcional.

Recomendamos ativar a compatibilidade total de um controlador de domínio Samba com um controlador de domínio Microsoft Active Directory. Isso garantirá a interação correta entre o Kaspersky Security Center Linux e o controlador de domínio Samba.

Para ativar a compatibilidade total de um controlador de domínio Samba com um controlador de domínio Microsoft Active Directory:

1. Execute o seguinte comando para usar a extensão de esquema RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Ative a atualização do esquema em um controlador de domínio Samba. Para fazer isso, adicione as seguintes linhas ao arquivo `/etc/samba/smb.conf`:

   ```
   dsdb:schema update allowed = true
   ```

   Caso a atualização do esquema seja concluída com um erro, será necessário executar uma restauração completa do controlador de domínio que atua como controlador principal do esquema.

Para todos os hosts baseados em Linux dentro de um controlador de domínio Samba, especifique o `netbios name` e os parâmetros do `workgroup` no arquivo `/etc/samba/smb.conf`. Caso contrário, os resultados da pesquisa podem conter hosts duplicados.

Inventário de equipamentos

A lista de hardware (**Gerenciamento de ativos** → **Hardware**) usada para inventariar equipamentos é preenchida de duas formas: automática e manual. Após cada sondagem de rede, todos os dispositivos detectados serão automaticamente adicionados na lista. No entanto, você também pode adicionar dispositivos manualmente se não quiser fazer a sondagem da rede. Você pode adicionar outros dispositivos na lista manualmente, por exemplo, roteadores, impressoras ou hardware de dispositivos.

Nas propriedades de um dispositivo, é possível ver e editar informações detalhadas sobre esse dispositivo.

A lista de hardware pode conter os seguintes tipos de dispositivos:

- Computadores
- Dispositivos móveis
- Dispositivos de rede
- Dispositivos virtuais
- Componentes OEM
- Periféricos do computador

- Dispositivos conectados
- Telefones VoIP
- Repositórios da rede

O administrador pode atribuir o atributo *Equipamento corporativo* aos dispositivos detectados. Este atributo pode ser atribuído manualmente nas propriedades de um dispositivo, ou o administrador pode especificar critérios para o atributo a atribuir automaticamente. Neste caso, o atributo *Equipamento corporativo* é atribuído pelo tipo de dispositivo.

O Kaspersky Security Center Linux permite a baixa de equipamentos. Para isso, selecione a opção **Baixa efetuada** nas propriedades do dispositivo. O dispositivo não é exibido na lista de equipamentos.

Um administrador pode gerenciar a lista de controladores lógicos programáveis (PLC) na pasta **Hardware**. As informações detalhadas sobre como gerenciar a lista PLC são fornecidas no *Guia do Usuário do Kaspersky Industrial CyberSecurity for Nodes*.

Adição de informações dobre novos dispositivos

Para adicionar informações sobre novos dispositivos na rede:

1. No menu principal, vá para **Gerenciamento de ativos** → **Hardware**.
2. Clique no botão **Adicionar** para abrir a janela **Novo dispositivo**.
3. Na janela **Novo dispositivo**, na lista suspensa **Tipo de dispositivo**, selecione um tipo de dispositivo que pretende adicionar.
4. Clique em **OK**.

   A janela Propriedades do dispositivo é aberta na seção **Geral**.
5. Na seção **Geral**, preencha os campos de entrada com os dados do dispositivo. A seção **Geral** lista as seguintes configurações:

   - **Dispositivo corporativo**. Selecione a caixa de seleção se você quiser atribuir o atributo *Corporativo* ao dispositivo. Usando este atributo, você poderá procurar por dispositivos na pasta **Hardware**.
   - **Baixa efetuada**. Selecione a caixa de seleção se você não quiser que o dispositivo seja exibido na lista de dispositivos na pasta **Hardware**.
6. Clique em **Aplicar**.

O novo dispositivo será exibido no espaço de trabalho da seção **Hardware**.

Configuração de critérios usados para definir dispositivos corporativos

Para configurar os critérios de detecção para dispositivos corporativos:

1. No menu principal, vá para **Gerenciamento de ativos** → **Hardware**.
2. Na parte superior da página **Hardware**, clique no link **Configurar as regras para dispositivos corporativos**.

   Um painel **Configurar as regras para dispositivos corporativos** será exibido.
3. No painel **Configurar as regras para dispositivos corporativos**, ative a opção **Configurar o atributo Dispositivo corporativo automaticamente para o dispositivo**. Especifique os tipos de dispositivos aos quais o atributo *Enterprise* será atribuído automaticamente.

   Essa opção afeta apenas os dispositivos adicionados por meio de sondagem de rede. Para os dispositivos adicionados manualmente, defina o atributo *Corporativo* manualmente.
4. Clique em **OK**.

Os critérios de detecção para dispositivos corporativos são configurados.

Usar o modo dinâmico VDI nos dispositivos cliente

Uma infraestrutura virtual pode ser implementada em uma rede corporativa usando máquinas virtuais temporárias. O Kaspersky Security Center Linux detecta máquinas virtuais temporárias e adiciona as informações sobre elas no banco de dados do Servidor de Administração. Após um usuário terminar de usar uma máquina virtual temporária, a máquina é removida da infraestrutura virtual. No entanto, um registro sobre a máquina virtual removida poderá ser salvo no banco de dados do Servidor de Administração. Além disso, máquinas virtuais inexistentes podem ser exibidas no Kaspersky Security Center Web Console.

Para impedir que informações sobre máquinas virtuais não existentes sejam salvas, o Kaspersky Security Center Linux oferece suporte ao modo dinâmico para a Virtual Desktop Infrastructure (VDI). O administrador pode ativar o suporte do modo dinâmico para VDI nas propriedades do pacote de instalação do Agente de Rede para que seja instalado na máquina virtual temporária.

Quando uma máquina virtual temporária é desativada, o Agente de Rede notifica o Servidor de Administração de que a máquina foi desativada. Após uma máquina virtual ter sido desativada com êxito, ela é removida da lista de dispositivos conectados com o Servidor de Administração. Se a máquina virtual for desativada com erros e o Agente de Rede não enviar uma notificação sobre a máquina virtual desativada para o Servidor de Administração, é usado um cenário de backup. Sob esse cenário, a máquina virtual é removida da lista de dispositivos conectados com o Servidor de Administração após três tentativas sem êxito de sincronização com o Servidor de Administração.

Ativar o modo dinâmico VDI nas propriedades de um pacote de instalação para o Agente de Rede

Para ativar o modo dinâmico VDI:

1. No menu principal, vá para **Gerenciamento de software → Pacotes de instalação**.
2. No menu de contexto do pacote de instalação do Agente de Rede, selecione **Propriedades**.
   A janela **Properties** é aberta.
3. Na janela **Properties**, selecione a seção **Avançado**.
4. Na seção **Avançado**, selecione a opção **Ativar modo dinâmico para VDI**.

O dispositivo no qual o Agente de Rede será instalado fará parte da VDI.

Mover os dispositivos da VDI para um grupo de administração

Para migrar dispositivos que fazem parte da VDI para um grupo de administração:

1. Vá para **Gerenciamento de ativos → Regras de migração**.
2. Clique em **Adicionar**.
3. Na guia **Condições da regra**, selecione a guia **Máquinas virtuais**.
4. Defina a regra **Esta é uma máquina virtual** como **Sim** e **Parte da Virtual Desktop Infrastructure** como **Sim.**
5. Clique em **Salvar**.

Gerenciamento de dispositivos cliente

O Kaspersky Security Center Linux permite gerenciar dispositivos clientes:

- Visualize as configurações e o status dos dispositivos gerenciados, incluindo clusters e matrizes de servidores.
- Configurar os pontos de distribuição.
- Gerenciar tarefas.

É possível usar grupos de administração para combinar dispositivos clientes em um conjunto que pode ser gerenciado como uma unidade única. Um dispositivo cliente pode ser incluído em apenas um grupo de administração. Os dispositivos podem ser alocados a um grupo automaticamente com base nas **Condições da regra**:

- Criar regras para mover dispositivos.
- Copiar regras para mover dispositivos.
- Condições de uma regra de migração de dispositivos.

É possível usar seleções de dispositivos para filtrar dispositivos com base em uma condição. Também é possível marcar dispositivos para criar seleções, localizar dispositivos e distribuir dispositivos entre grupos de administração.

Configurações de um dispositivo gerenciado

Para exibir as configurações de um dispositivo gerenciado:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo necessário.

A janela Propriedades do dispositivo selecionado é exibida.

As seguintes guias são exibidas na parte superior da janela de propriedades; elas representam os principais grupos de configurações:

Geral

Esta guia compreende as seguintes seções:

- A seção **Geral** exibe as informações gerais sobre o dispositivo cliente. As informações são fornecidas com base nos dados recebidos durante a última sincronização do dispositivo cliente com o Servidor de Administração:
  - **Nome**

    Neste campo, você poderá visualizar e modificar o nome de um dispositivo cliente no grupo de administração.

- **Descrição**

  Nesse campo, você poderá inserir uma descrição adicional de um dispositivo cliente.

- **Status do dispositivo**

  Status do dispositivo cliente atribuído com base nos critérios definidos pelo administrador para o status de proteção antivírus no dispositivo e na atividade do dispositivo na rede.

- **Nome completo do grupo**

  Grupo de administração que inclui o dispositivo cliente.

- **Última atualização dos bancos de dados de antivírus**

  Data em que os bancos de dados de antivírus ou os aplicativos foram atualizados pela última vez no dispositivo.

- **Conectado ao Servidor de Administração**

  Data e hora da última vez que o Agente de Rede instalado no dispositivo cliente foi conectado ao Servidor de Administração.

- **Última visualização**

  Data e hora de quando o dispositivo esteve por último visível na rede.

- **Versão do Agente de Rede**

  Versão do Agente de Rede instalado.

- **Criação**

  Data de criação do dispositivo no Kaspersky Security Center Linux.

- **Proprietário do dispositivo**

  Nome do proprietário do dispositivo. É possível atribuir ou remover um usuário como proprietário de um dispositivo ao clicar no link **Gerenciar proprietário do dispositivo**.

- **Não desconectar do Servidor de Administração**

  Caso a opção seja ativada, será mantida uma conectividade contínua entre o dispositivo gerenciado e o Servidor de Administração. Convém utilizar essa opção caso os servidores push, que fornecem essa conectividade, não estejam sendo usados.

  Caso essa opção esteja desativada e os servidores push não estejam sendo utilizados, o dispositivo gerenciado somente se conectará ao Servidor de Administração para sincronizar dados ou transmitir informações.

  O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

  A opção é desativada por padrão em dispositivos gerenciados. A opção é ativada por padrão no dispositivo onde o Servidor de Administração está instalado e permanece ativada mesmo se você tentar desativá-la.

- A seção **Rede** exibe as seguintes informações sobre as propriedades da rede do dispositivo cliente:

  - **Endereço IP**

Endereço IP do dispositivo.

- **Domínio do Windows**

  Grupo de trabalho que contém o dispositivo.

- **Nome DNS**

  O nome do domínio DNS do dispositivo cliente.

- **Nome do NetBIOS**

  Nome do dispositivo cliente.

- **Endereço IPv6**

- A seção **Sistema** fornece informações sobre o sistema operacional instalado no dispositivo cliente:

  - **SO**

  - **Arquitetura da CPU**

  - **Nome do dispositivo**

  - **Tipo de máquina virtual**

    O fabricante da máquina virtual.

  - **Máquina virtual dinâmica como parte da VDI**

    Esta seta exibe se o dispositivo cliente é uma máquina virtual dinâmica como parte da VDI.

- A seção **Proteção** fornece as seguintes informações sobre o status atual da proteção antivírus no dispositivo cliente:

  - **Visível**

    O status da visibilidade do dispositivo cliente.

  - **Status do dispositivo**

    Status do dispositivo cliente atribuído com base nos critérios definidos pelo administrador para o status de proteção antivírus no dispositivo e na atividade do dispositivo na rede.

  - **Descrição de status**

    Status da proteção do dispositivo cliente e conexão com o Servidor de Administração.

  - **Status da proteção**

    Esse campo exibe o status atual da proteção em tempo real do dispositivo cliente.

    Quando o status é alterado no dispositivo, o novo status é exibido na janela de propriedades do dispositivo só depois que o dispositivo cliente é sincronizado com o Servidor de Administração.

  - **Última verificação completa**

    Data e hora em que a verificação de malwares foi executada por último no dispositivo cliente.

- **Vírus detectado**

  Número total de ameaças detectadas no dispositivo cliente desde a instalação do aplicativo de segurança (primeira verificação) ou desde a última redefinição do contador de ameaças.

- **Objetos com desinfecção mal-sucedida**

  Número de arquivos não processados no dispositivo cliente.

  Este campo ignora o número de arquivos não processados nos dispositivos móveis.

- **Status de criptografia do disco**

  O status atual da criptografia do arquivo nas unidades locais do dispositivo. Para obter uma descrição dos status, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

  Os arquivos podem ser criptografados apenas nos dispositivos gerenciados nos quais o Kaspersky Endpoint Security for Windows está instalado.

- A seção **Status do dispositivo definido pelo aplicativo** fornece informações sobre o status do dispositivo definido pelo aplicativo gerenciado e instalado no dispositivo. O status do dispositivo pode ser diferente do definido pelo Kaspersky Security Center Linux.

Aplicativos

Esta guia lista todos os aplicativos da Kaspersky instalados no dispositivo cliente. Esta guia contém os botões **Iniciar** e **Parar**, que iniciam e interrompem o aplicativo da Kaspersky selecionado (exceto o Agente de Rede). Você pode usar esses botões se a porta 15000 UDP estiver disponível no dispositivo gerenciado para notificações push do Servidor de Administração. Se o dispositivo gerenciado não estiver disponível para notificações push, mas o modo estiver configurado para manter uma conexão contínua com o Servidor de Administração (a opção **Não desconectar do Servidor de Administração** na seção **Geral** estiver ativada), os botões **Iniciar** e **Parar** ainda estarão disponíveis. Caso contrário, ao tentar iniciar ou interromper o aplicativo, uma mensagem de erro será exibida. É possível clicar no nome do aplicativo para visualizar informações gerais sobre ele, uma lista de eventos que ocorreram no dispositivo e as configurações do aplicativo.

Políticas e perfis de política ativos

Esta guia lista as políticas e perfis de políticas atualmente ativos no dispositivo gerenciado.

Tarefas

Na guia **Tarefas**, é possível gerenciar as tarefas do dispositivo cliente: visualizar a lista de tarefas existentes, criar novas, remover, iniciar e interromper tarefas, modificar as suas configurações e visualizar os resultados da execução. A lista de tarefas é fornecida com base nos dados recebidos durante a última sessão de sincronização do cliente com o Servidor de Administração. O Servidor de Administração solicita os detalhes do status de tarefa do dispositivo cliente. Se a porta 15000 UDP estiver disponível no dispositivo gerenciado para receber notificações push do Servidor de Administração, o status da tarefa será exibido e os botões para gerenciar a tarefa serão ativados. Se um servidor push não conseguir se comunicar com o dispositivo gerenciado, mas o modo de conexão contínua com o Servidor de Administração estiver ativado (a opção **Não desconectar do Servidor de Administração** na seção **Geral** está ativada), as ações com tarefas também estarão disponíveis.

Se a conexão não é estabelecida, o status não é exibido e os botões são desabilitados.

Eventos

A guia **Eventos** exibe os eventos registrados no Servidor de Administração para o dispositivo cliente selecionado.

Você pode exportar, copiar e excluir os eventos do dispositivo.

Problemas de segurança

Na guia **Problemas de segurança**, é possível visualizar, editar e criar problemas de segurança para o dispositivo cliente. Os problemas de segurança podem ser criados automaticamente pelos aplicativos da Kaspersky gerenciados e instalados no dispositivo cliente ou manualmente pelo administrador. Por exemplo, caso alguns usuários movam regularmente malwares de suas unidades removíveis para os dispositivos, o administrador poderá criar um problema de segurança. No texto do problema de segurança, o administrador pode fornecer uma breve descrição do caso e as ações recomendadas (como ações disciplinares a serem tomadas contra um usuário) e pode adicionar um link para o usuário ou usuários.

Um problema de segurança para o qual todas as ações necessárias foram tomadas é chamado de *processado*. A presença de problemas de segurança não processados pode ser escolhida como a condição para uma alteração do status do dispositivo para *Crítico* ou *Advertência*.

Esta seção contém uma lista de problemas de segurança que foram criados para o dispositivo. Os problemas de segurança são classificados por nível de gravidade e tipo. O tipo de problema de segurança é definido pelo aplicativo da Kaspersky, que cria o problema de segurança. É possível destacar os problemas de segurança processados na lista ao marcar a caixa de seleção na coluna **Processed**.

Tags

Na guia **Tags**, é possível gerenciar a lista de palavras-chave que são usadas para localizar os dispositivos cliente: visualizar a lista de tags existentes, atribuir tags a partir da lista, configurar regras de identificação automática, adicionar novas tags, renomear as antigas e excluir tags.

Avançado

Esta guia compreende as seguintes seções:

- **Registro de aplicativos**. Nesta seção, é possível exibir o registro de aplicativos instalados no dispositivo clientes e suas atualizações, assim como configurar a exibição do registro de aplicativos.

  Informações sobre os aplicativos instalados são fornecidas se o Agente de Rede instalado no dispositivo cliente enviar as informações necessárias ao Servidor de Administração. Você pode configurar o envio de informações para o Servidor de Administração na janela Propriedades do Agente de Rede ou sua política, na seção **Repositórios**.

  Clicar no nome de um aplicativo abre uma janela que contém os detalhes do aplicativo e uma lista dos pacotes de atualização instalados para o aplicativo.

- **Arquivos executáveis**. Esta seção exibe os arquivos executáveis encontrados no dispositivo cliente.

- **Pontos de distribuição**. Esta seção fornece uma lista de pontos de distribuição com os quais o dispositivo interage.

  - **Exportar para arquivo**

    Clique no botão **Exportar para arquivo** para salvar a um arquivo de uma lista de pontos de distribuição com os quais o dispositivo interage. Por padrão, o aplicativo exporta a lista de dispositivos para um arquivo CSV.

  - **Propriedades**

    Clique no botão **Propriedades** para exibir e configurar o ponto de distribuição com o qual o dispositivo interage.

- **Registro de hardware**. Nesta seção, é possível visualizar as informações sobre o hardware instalado no dispositivo cliente.

Se o Agente de Rede estiver instalado em um dispositivo com Windows, ele enviará ao Servidor de Administração as seguintes informações sobre o hardware:

- RAM
- Dispositivos de armazenamento em massa
- Placa-mãe
- CPU
- Adaptadores de rede
- Monitores
- Adaptador de vídeo
- Placa de som

Se o Agente de Rede estiver instalado em um dispositivo com Linux ou macOS, ele enviará ao Servidor de Administração as seguintes informações sobre o hardware, caso o sistema operacional as forneça:

- Volume total de RAM
- Volume total de dispositivos de armazenamento em massa
- Placa-mãe
- CPU
- Adaptadores de rede

- **Atualizações disponíveis**. Esta seção exibe uma lista de atualizações de software encontradas neste dispositivo, mas ainda não instaladas.

- **Vulnerabilidades de software**. Esta seção fornece informações sobre as vulnerabilidades de aplicativos de terceiros instalados nos dispositivos cliente.

  Para salvar as vulnerabilidades em um arquivo, marque as caixas de seleção ao lado das vulnerabilidades que deseja salvar e clique no botão **Exportar para CSV** ou no botão **Exportar para TXT**.

  Esta seção contém as seguintes configurações:

  - **Mostrar somente vulnerabilidades que podem ser corrigidas**

    Se esta opção estiver ativada, a seção exibe vulnerabilidades que podem ser corrigidas usando um patch.

    Se essa opção estiver desativada, a seção exibe ambas as vulnerabilidades que podem ser corrigidas usando um patch, bem como as vulnerabilidades para as quais não foi lançado nenhum patch.

    Por padrão, esta opção está ativada.

  - **Propriedades de vulnerabilidade**

Clique no nome de uma vulnerabilidade de software na lista para visualizar as propriedades da vulnerabilidade de software selecionada em uma janela separada. Na janela, você pode fazer o seguinte:

- Ignore a vulnerabilidade de software neste dispositivo gerenciado (no Kaspersky Security Center Web Console).
- Consulte a lista de correções recomendadas para a vulnerabilidade.
- Especifique manualmente as atualizações de software para corrigir a vulnerabilidade (no Kaspersky Security Center Web Console).
- Exibir as instâncias de vulnerabilidade.
- Consulte a lista de tarefas existentes para corrigir a vulnerabilidade e crie novas tarefas para corrigir a vulnerabilidade.

- **Diagnóstico remoto**. Nesta seção, é possível executar o diagnóstico remoto de dispositivos clientes.

Caso um DBMS PostgreSQL, MariaDB ou MySQL seja usado, a guia **Eventos** poderá exibir uma lista incompleta de eventos para o dispositivo cliente selecionado. Isso ocorre quando o DBMS armazena uma quantidade muito grande de eventos. É possível aumentar o número de eventos exibidos com a execução de um dos seguintes procedimentos:

- Remoção de eventos desnecessários.
- Redução do prazo de armazenamento para eventos desnecessários.

Para ver uma lista completa de eventos registrados no Servidor de Administração para o dispositivo, use Relatórios.

Verificar a conexão entre um dispositivo cliente e o Servidor de Administração. Utilitário klnagchk

Você pode verificar a conexão e obter informações detalhadas sobre as configurações da conexão entre um dispositivo cliente e o Servidor de Administração usando o utilitário klnagchk. O utilitário klnagchk está localizado na pasta Instalação do Agente de Rede.

Quando iniciado a partir da linha de comando, o utilitário klnagchk pode executar as seguintes ações (dependendo das chaves que estiverem em uso):

- Exibe na tela ou registra em log os valores das configurações usadas para conectar o Agente de Rede instalado no dispositivo ao Servidor de Administração.
- Grava em um arquivo de log de eventos as estatísticas do Agente de Rede (desde a última inicialização) e os resultados de operação do utilitário ou exibe as informações na tela.
- Tenta estabelecer uma conexão entre o Agente de Rede e o Servidor de Administração.

  Se a tentativa de conexão falhar, o utilitário envia um pacote ICMP para verificar o status do dispositivo no qual o Servidor de Administração está instalado.

Para verificar a conexão entre um dispositivo cliente e o Servidor de Administração usando o utilitário klnagchk.

No dispositivo com o Agente de Rede instalado, inicie o utilitário klnagchk por meio da linha de comando em uma conta de administrador local.

A sintaxe da linha de comando do utilitário:

```
klnagchk [-logfile <nome do arquivo>] [-sp] [-savecert <caminho para o arquivo de certificado>] [-restart][-sendhb]
```

Descrições das chaves:

- `-logfile <nome do arquivo>` – Registra os valores das configurações de conexão entre o Agente de Rede e o Servidor de Administração, assim como os resultados da operação do utilitário em um arquivo de log.

  Por predefinição, as informações são salvas na transmissão de saída predefinido (stdout). Se a chave não estiver sendo usada, as configurações, os resultados e as mensagens de erro são exibidos na tela.

- `-sp` – Mostra a senha para a autenticação do usuário no servidor proxy.

  A chave está em uso se a conexão ao Servidor de Administração for estabelecida por meio de um servidor proxy.

- `-savecert <nome do arquivo>` – Salva o certificado usado para acessar o Servidor de Administração em um arquivo especificado.

- `-restart` – Inicia o Agente de Rede após a conclusão do utilitário.

- `-sendhb` – Inicia a sincronização do Agente de Rede com o Servidor de Administração.

Após a inicialização, o utilitário klnagchk acessa os arquivos de configuração do Agente de Rede e exibe os parâmetros de conexão. Esses parâmetros são especificados durante a instalação do Agente de Rede e nas configurações da política do Agente de Rede:

- `Current device` – Nome de rede Windows do dispositivo cliente.

- `Network Agent version` – Número completo da versão do Agente de Rede (com patches) instalado no dispositivo.

- `Server address` – O endereço do Servidor de Administração.

- `Use SSL` – Parâmetro que indica se uma conexão segura é usada ao conectar-se ao Servidor de Administração.

  Valores possíveis:

  - 0 – A conexão segura não é usada.

  - 1 – A conexão segura é usada.

- `Compress traffic` – Parâmetro que indica se o tráfego entre o dispositivo cliente e o Servidor de Administração é compactado.

- `Server SSL ports` – Números de portas válidas para comunicação com o Servidor de Administração ao usar uma conexão segura.

- `Server ports` – Números das portas válidas para comunicação com o Servidor de Administração ao usar uma conexão comum.
- `Use proxy server` – Parâmetro que indica se um servidor proxy é usado.

  Valores possíveis:

  - 0 – O servidor proxy não é usado.
  - 1 – O servidor proxy é usado.
- `Address` – Endereço e porta do servidor proxy separados por dois pontos. Esse parâmetro é exibido somente se um servidor proxy for usado.
- `User name` – Nome de usuário para acessar o servidor proxy. Esse parâmetro é exibido somente se um servidor proxy for usado.
- `Password` – Senha para acessar o servidor proxy. Esse parâmetro é exibido somente se um servidor proxy for usado. Para mostrar a senha do servidor proxy, é necessário usar a chave `sp` no comando.
- `Certificate` – Parâmetro que indica se o dispositivo cliente tem um certificado do Servidor de Administração. Um certificado pode não existir, por exemplo, se o Agente de Rede nunca tiver se conectado com êxito ao Servidor de Administração.

  Valores possíveis:

  - `not installed` – O dispositivo cliente não tem um certificado do Servidor de Administração.
  - `present` – O dispositivo cliente tem um certificado do Servidor de Administração.
- `Open UDP port` – Parâmetro que indica se o Agente de Rede usa a porta UDP para receber solicitações de sincronização do Servidor de Administração.

  Valores possíveis:

  - 0 – A porta UDP está fechada para receber as solicitações de sincronização do Servidor de Administração.
  - 1 – A porta UDP está aberta para receber as solicitações de sincronização do Servidor de Administração.
- `UDP ports` – Números das portas UDP que podem ser usadas pelo Agente de Rede.
- `Location name` – Localização da rede do dispositivo.
- `State of network location` – Parâmetro que indica se o dispositivo cliente pode ser alternado de um perfil de conexão do Servidor de Administração para outro.

  Valores possíveis:

  - `Enabled` – O perfil de conexão do Servidor de Administração pode ser trocado para o dispositivo cliente.
  - `Disabled` – O perfil de conexão do Servidor de Administração não pode ser trocado para o dispositivo cliente.
- `Profile to use` – Perfil de conexão para o Servidor de Administração.
- `Condition` – Endereço IP e máscara de sub-rede da rede à qual o dispositivo cliente está conectado.
- `Ping period, minutes` – Intervalo padrão entre sincronizações.

- `Conn timeout, s` – Tempo limite da conexão.
- `RW timeout, s` – Tempo limite da conexão das operações de leitura/gravação.
- `Host ID` – ID do dispositivo na rede. O `Device ID` é exclusivo entre os dispositivos clientes gerenciados pelo mesmo Servidor de Administração.
- `Locations of connection gateways` – Parâmetros para conectar o dispositivo cliente ao Servidor de Administração por meio do gateway de conexão.
- `Location of distribution points` – Parâmetros para conectar o dispositivo cliente ao Servidor de Administração por meio do ponto de distribuição.
- `Connection with server` – Parâmetro que indica se o gateway de conexão tem uma conexão contínua com o Servidor de Administração. O parâmetro é exibido somente se o dispositivo cliente atuar como um gateway de conexão.

  Valores possíveis:

  - `active` – O gateway de conexão tem uma conexão contínua com o Servidor de Administração.
  - `inactive` – O gateway de conexão não tem uma conexão contínua com o Servidor de Administração.
- `Connection with server through connection gateway` – Parâmetro que indica se a conexão ao Servidor de Administração por meio de um gateway de conexão foi estabelecida corretamente. O parâmetro é exibido somente se o dispositivo cliente atuar como um gateway de conexão.

  Valores possíveis:

  - `active` – A conexão com o Servidor de Administração por meio de um gateway de conexão foi estabelecida corretamente.
  - `inactive` – A conexão com o Servidor de Administração por meio de um gateway de conexão foi estabelecida incorretamente.

Além disso, a saída do utilitário klnagchk pode conter uma das seguintes linhas:

- `Administration Server is installed on this device` – O utilitário klnagchk é executado no dispositivo do Servidor de Administração.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server`. O utilitário klnagchk é executado no dispositivo no qual o Agente de Rede está instalado, no modo de gateway de conexão. O gateway de conexão configurado está aguardando uma conexão do Servidor de Administração, mas o Servidor de Administração não lista o dispositivo entre os dispositivos gerenciados. Você precisa garantir que o Servidor de Administração inicie uma conexão com o gateway de conexão.
- `This device is a connection gateway` – O utilitário klnagchk é executado no dispositivo que atua como um gateway de conexão.
- `Acts as a distribution point`. O utilitário klnagchk é executado no dispositivo que atua como um ponto de distribuição.

O utilitário klnagchk verifica o status do serviço do Agente de Rede. Se o serviço não estiver em execução, o utilitário será interrompido. Se o serviço estiver em execução, o utilitário exibirá as seguintes estatísticas de conexão:

- `Ping count` – Número de tentativas para conectar o dispositivo cliente ao Servidor de Administração.
- `Succ. pings` – Número de tentativas bem-sucedidas de conectar o dispositivo cliente ao Servidor de Administração.
- `Sync count` – Número de tentativas para sincronizar as configurações do dispositivo cliente com as configurações do Servidor de Administração.
- `Succ. syncs` – Número de tentativas bem-sucedidas de sincronizar as configurações do dispositivo cliente ao Servidor de Administração.
- `Last ping` – Data e hora da última conexão.

Você precisa usar os parâmetros `Ping count` e `Succ. pings` ao analisar a conexão entre o Servidor de Administração e o Agente de Rede. As configurações do dispositivo cliente só serão sincronizadas com as configurações do Servidor de Administração se as configurações do Servidor de Administração forem alteradas (por exemplo, se novas tarefas forem adicionadas ou as configurações de política forem modificadas). Caso contrário, os valores dos parâmetros `Ping count` e `Succ. pings` permanecerão inalterados.

Para obter mais informações sobre como solucionar problemas de conexão do Agente de Rede ao Servidor de Administração, consulte as perguntas frequentes do Kaspersky Security Center Linux.

Regras de migração de dispositivos

Recomendamos definir a alocação automática de dispositivos em grupos de administração através das *regras de migração de dispositivos*. Uma regra para migrar dispositivo compõe-se de três partes principais: um nome, uma condição de execução (expressão lógica com os atributos de dispositivo) e um grupo de administração alvo. Uma regra move um dispositivo para o grupo de administração alvo se os atributos do dispositivo atendam a condição de execução da regra.

Todas as regras para migrar dispositivo têm prioridades. O Servidor de Administração verifica os atributos do dispositivo quanto a se eles atendem a condição de execução de cada regra, na ordem ascendente da prioridade. Se os atributos do dispositivo atenderem a condição de execução de uma regra, o dispositivo é movido para o grupo alvo, portanto o processamento de regra é completo para este dispositivo. Se os atributos do dispositivo atenderem as condições de múltiplas regras, o dispositivo é movido para o grupo alvo da regra com a prioridade mais alta (ou seja, ele tem a classificação mais alta na lista de regras).

As regras para migrar dispositivo podem ser criadas implicitamente. Por exemplo, nas propriedades de um pacote de instalação ou de uma tarefa de instalação remota, você pode especificar o grupo de administração para o qual o dispositivo deve ser movido após que Agente de Rede seja instalado nele. Além disso, as regras para migrar dispositivos podem ser criadas explicitamente pelo administrador do Kaspersky Security Center Linux na seção **Gerenciamento de ativos → Regras de migração**.

Por padrão, uma regra para mover dispositivo é destinada para a alocação inicial de uma só vez de dispositivos aos grupos de administração. A regra move os dispositivos do grupo dispositivos não atribuídos somente uma vez. Se um dispositivo foi movido uma vez por esta regra, a regra nunca mais o moverá novamente, mesmo se você devolver o dispositivo ao grupo dispositivos não atribuídos manualmente. Esta é a forma recomendada de aplicar regras para mover.

Você pode migrar dispositivos que já foram alocados à alguns dos grupos de administração. Para fazer isso, nas propriedades de uma regra, desmarque a caixa de seleção **Somente mover os dispositivos que não pertencem a um grupo de administração**.

Aplicar regras para mover aos dispositivos que já foram alocados à alguns dos grupos de administração, aumenta significativamente a carga do Servidor de Administração.

A caixa de seleção **Somente mover os dispositivos que não pertencem a um grupo de administração** é bloqueada nas propriedades das regras de movimentação criadas automaticamente. As regras são criadas ao adicionar a tarefa *Instalar aplicativo remotamente* ou ao criar um pacote de instalação independente.

Você pode criar uma regra para mover que iria afetar um único dispositivo repetidamente.

Nós recomendamos com ênfase que você evite mover um dispositivo único de um grupo para outro repetidamente (por exemplo, para poder aplicar uma política especial àquele dispositivo, executar uma tarefa de grupo especial, ou atualizar o dispositivos através de um ponto de distribuição específico).

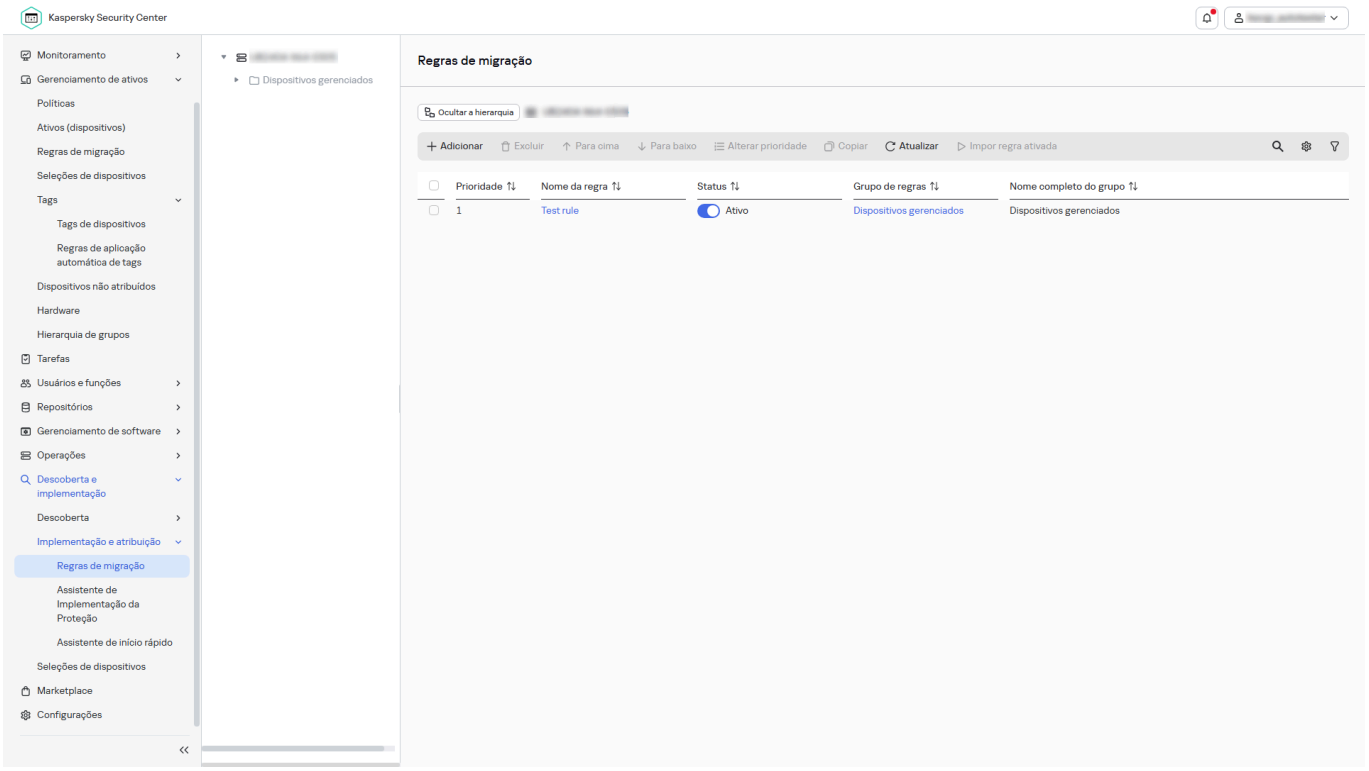
Tais cenários não são compatíveis, porque eles aumentam a carga no Servidor de Administração e o tráfego da rede para um grau extremo. Estes cenários também estão em conflito com os princípios operacionais do Kaspersky Security Center Linux (em particular na área de direitos de acesso, eventos e relatórios). Outra solução deve ser encontrada, por exemplo, por meio do uso de perfis de política, tarefas para seleções de dispositivo e atribuição de Agentes de Rede de acordo com o cenário padrão.

Criar regras para mover dispositivos

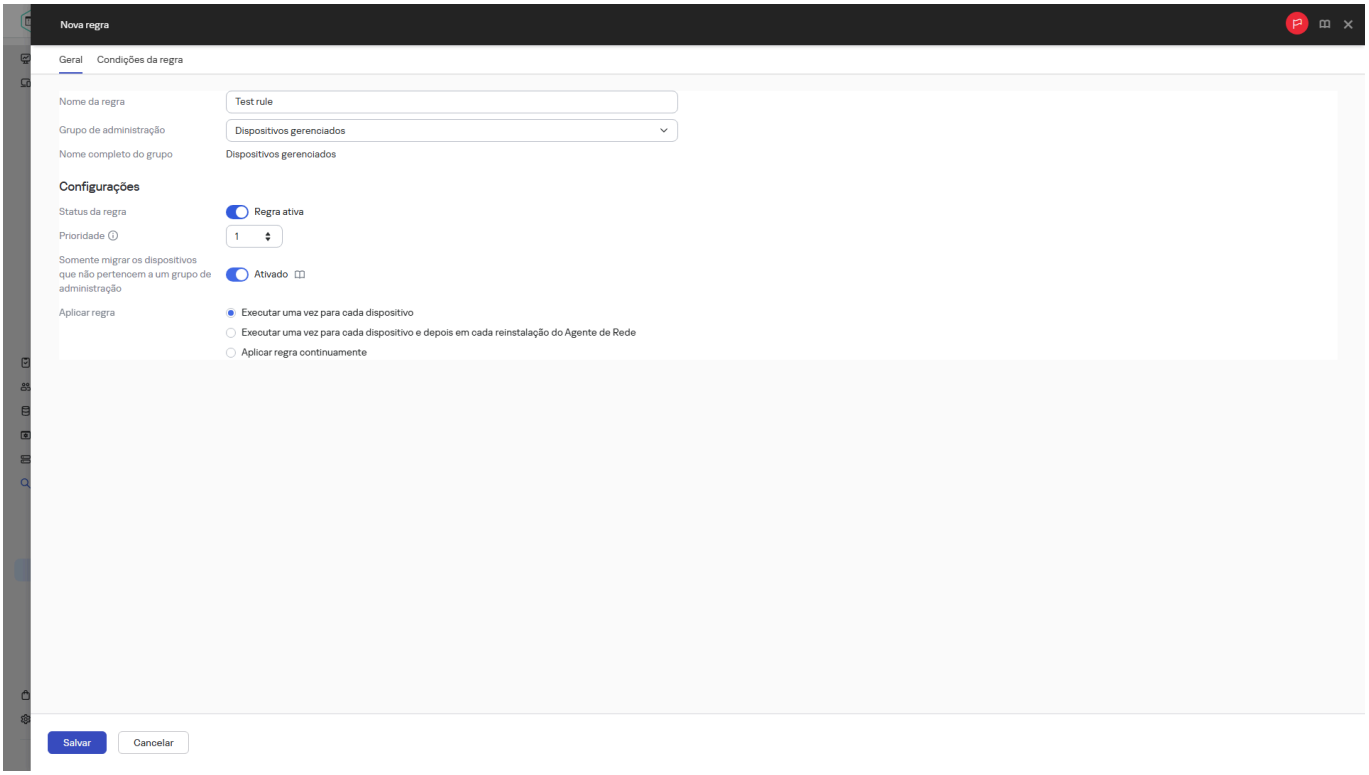
É possível configurar as regras de migração de dispositivos, ou seja, as regras que alocam automaticamente os dispositivos para grupos de administração.

Para criar uma regra para mover dispositivos:

1. No menu principal, vá para **Gerenciamento de ativos** → **Regras de migração**.



2. Clique em **Adicionar**. A janela **Nova regra** se abre.



3. Na janela exibida, especifique as seguintes informações na guia **Geral**:

   Nome da regra

   Digite um nome para a nova regra.

   Se estiver copiando uma regra, a nova regra adquirirá o mesmo nome da regra de origem, mas um índice no formato () será adicionado ao nome, por exemplo: (1).

   Grupo de administração

Selecione o grupo de administração para o qual os dispositivos devem ser movidos automaticamente.

Status da regra

Se esta opção estiver ativada, a regra será ativada e começará a funcionar após ser salva.

Se esta opção estiver desativada, a regra será criada, mas não ativada. Ela não funcionará até que você ative esta opção.

Prioridade

É possível especificar a prioridade da regra de movimentação. A prioridade mais alta é 1. Quanto maior o valor de **Prioridade**, menor a prioridade da regra e sua posição na lista.

Se nenhuma prioridade for atribuída, a regra receberá a prioridade mais baixa.

Ao copiar uma regra, sua cópia recebe a prioridade da regra original. A prioridade da regra original é, então, aumentada em 1.

Somente migrar os dispositivos que não pertencem a um grupo de administração

Se esta opção estiver ativada, somente os dispositivos não atribuídos serão movidos para o grupo selecionado.

Se esta opção estiver desativada, os dispositivos que já pertencem a outros grupos de administração, bem como os dispositivos não atribuídos, serão movidos para o grupo selecionado.

Aplicar regra

Você pode selecionar uma das seguintes opções:

- **Executar uma vez para cada dispositivo**

  A regra é aplicada uma vez para cada dispositivo que atenda aos critérios.

- **Executar uma vez para cada dispositivo e depois em cada reinstalação do Agente de Rede**

  A regra é aplicada uma vez para cada dispositivo que atende aos critérios e apenas quando o Agente de Rede é reinstalado nesses dispositivos.

- **Aplicar regra continuamente**

  A regra é aplicada de acordo com o agendamento que o Servidor de Administração configura automaticamente (normalmente a cada várias horas).

4. Na guia **Condições da regra**, especifique pelo menos um critério pelo qual os dispositivos são movidos para um grupo de administração.

5. Clique em **Salvar**.

A regra de movimentação é criada. Ela é exibida na lista de regras de movimento.

Quanto mais elevada a posição na lista, maior a prioridade da regra.

Para alterar a prioridade:

1. Marque a caixa de seleção de uma regra em movimento.
2. Execute uma das seguintes ações:
   - Clique no botão **Alterar prioridade** e especifique a nova prioridade.
   - Mova a regra para cima ou para baixo na lista clicando nos botões **Para cima** ou **Para baixo**.
3. Clique no botão **Salvar**.

> Se a opção **Aplicar regra continuamente** estiver selecionada, a regra de migração será aplicada independentemente das configurações de prioridade. Essas regras são aplicadas de acordo com o agendamento que o Servidor de Administração configura automaticamente.

Se os atributos do dispositivo atenderem as condições de múltiplas regras, o dispositivo é movido para o grupo alvo da regra com a prioridade mais alta (ou seja, ele tem a classificação mais alta na lista de regras).

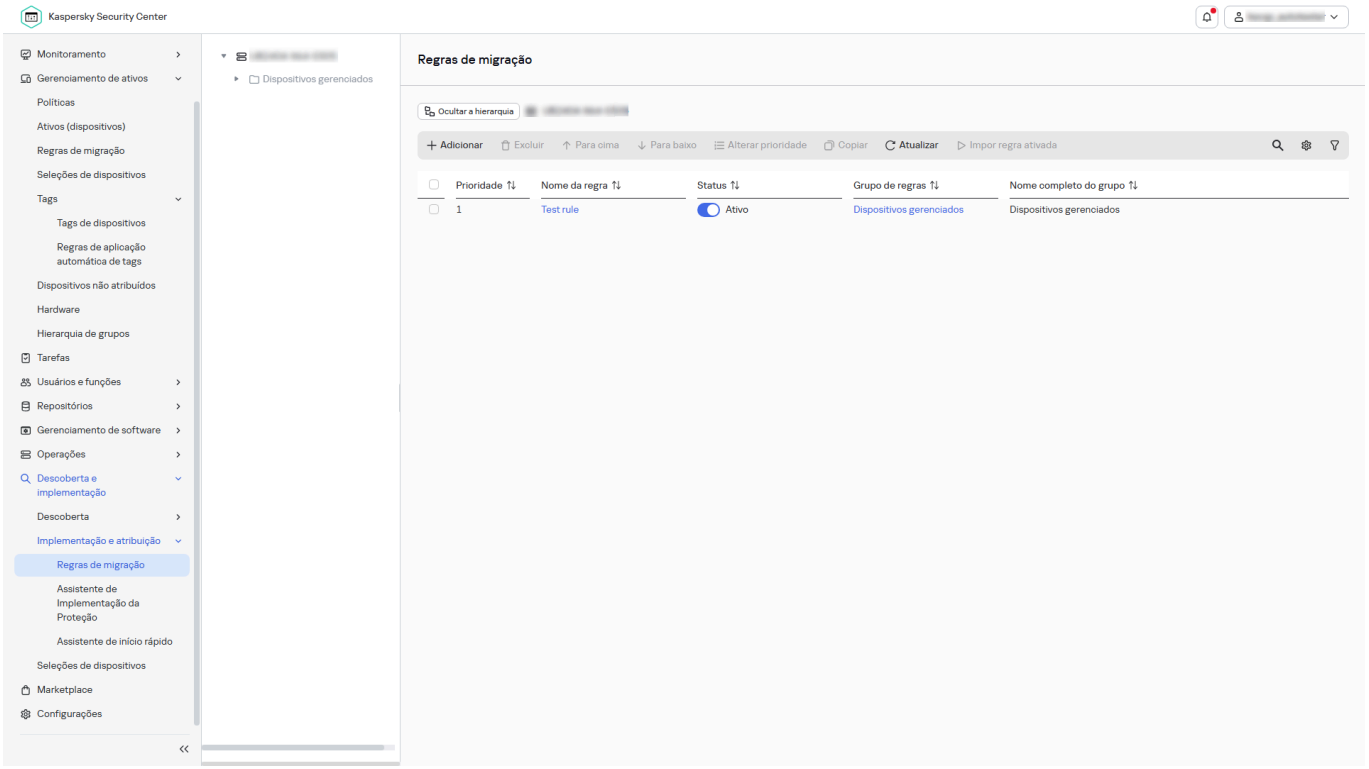
Copiar as regras para mover dispositivos

Você poderá copiar regras de movimento, por exemplo, se quiser ter várias regras idênticas para grupos de administração de destino diferentes.

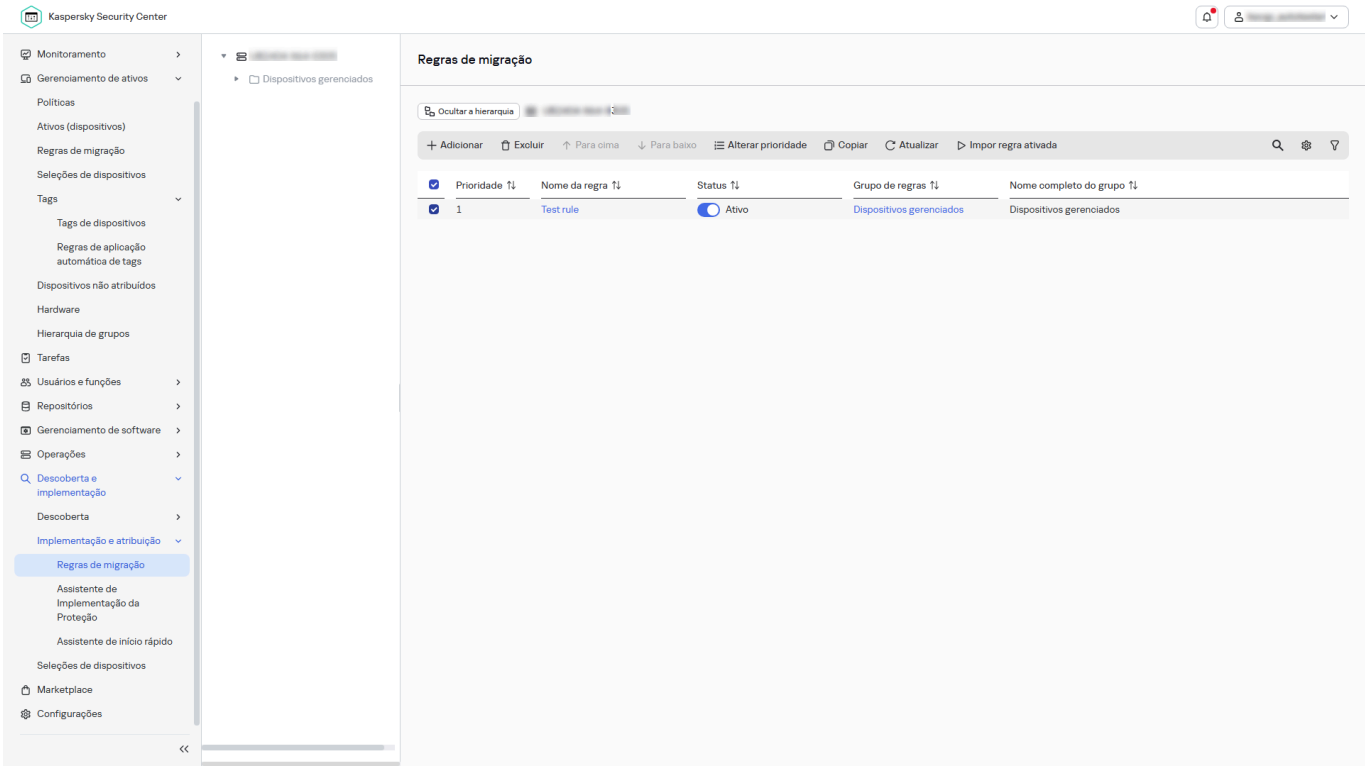
Para copiar uma regra de movimentação existente:

1. Execute uma das seguintes ações:
   - No menu principal, vá para **Gerenciamento de ativos → Regras de migração**.
   - No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Regras de migração**.

A lista de regras de movimento é exibida.



2. Marque a caixa de seleção ao lado da regra que deseja copiar.



3. Clique em **Copiar**.

4. Na janela que se abre, modifique as seguintes informações na guia **Geral** ou não faça nenhuma modificação se você só quiser copiar a regra sem modificar as suas configurações:

   Nome da regra

   Digite um nome para a nova regra.

   Se estiver copiando uma regra, a nova regra adquirirá o mesmo nome da regra de origem, mas um índice no formato () será adicionado ao nome, por exemplo: (1).

   Grupo de administração

Selecione o grupo de administração para o qual os dispositivos devem ser movidos automaticamente.

Status da regra

Se esta opção estiver ativada, a regra será ativada e começará a funcionar após ser salva.

Se esta opção estiver desativada, a regra será criada, mas não ativada. Ela não funcionará até que você ative esta opção.

Prioridade

É possível especificar a prioridade da regra de movimentação. A prioridade mais alta é 1. Quanto maior o valor de **Prioridade**, menor a prioridade da regra e sua posição na lista.

Se nenhuma prioridade for atribuída, a regra receberá a prioridade mais baixa.

Ao copiar uma regra, sua cópia recebe a prioridade da regra original. A prioridade da regra original é, então, aumentada em 1.

Somente migrar os dispositivos que não pertencem a um grupo de administração

Se esta opção estiver ativada, somente os dispositivos não atribuídos serão movidos para o grupo selecionado.

Se esta opção estiver desativada, os dispositivos que já pertencem a outros grupos de administração, bem como os dispositivos não atribuídos, serão movidos para o grupo selecionado.

Aplicar regra

Você pode selecionar uma das seguintes opções:

- **Executar uma vez para cada dispositivo**

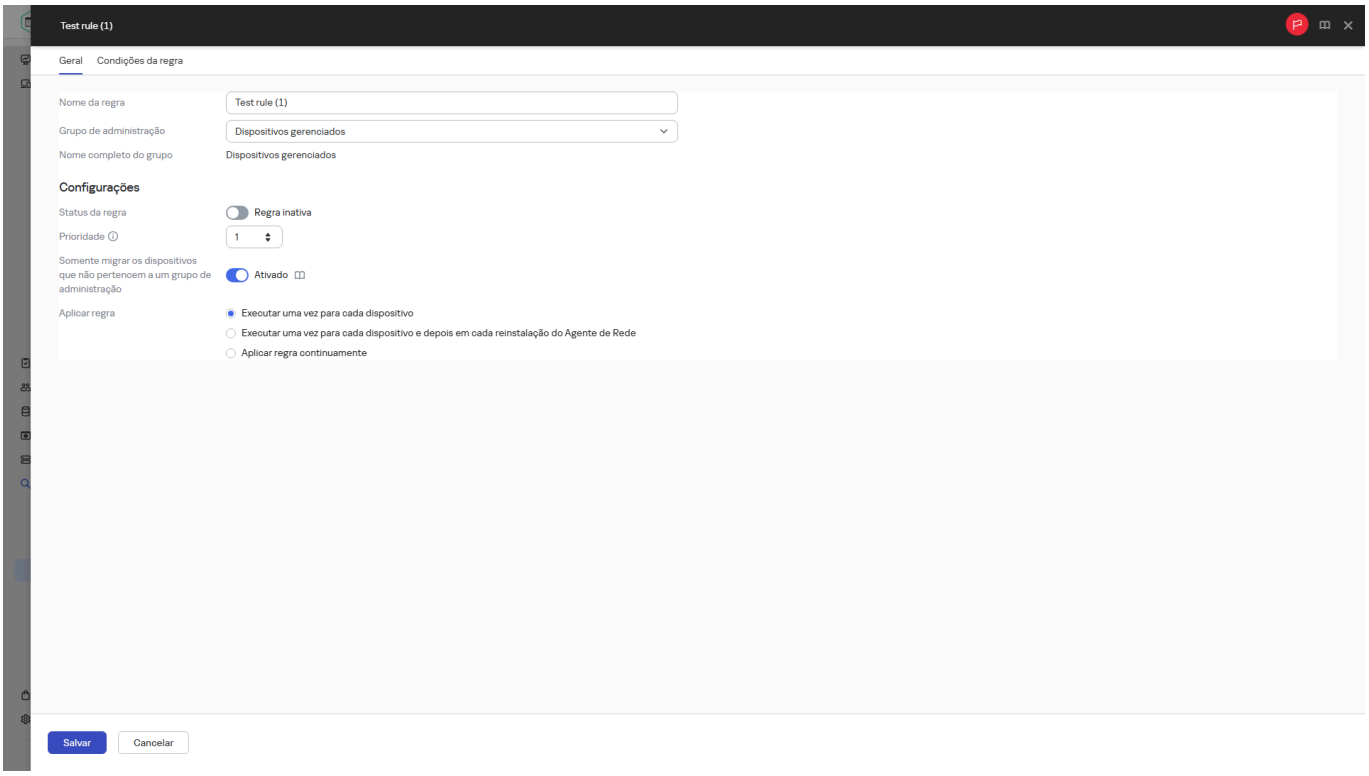
  A regra é aplicada uma vez para cada dispositivo que atenda aos critérios.

- **Executar uma vez para cada dispositivo e depois em cada reinstalação do Agente de Rede**

  A regra é aplicada uma vez para cada dispositivo que atende aos critérios e apenas quando o Agente de Rede é reinstalado nesses dispositivos.

- **Aplicar regra continuamente**

  A regra é aplicada de acordo com o agendamento que o Servidor de Administração configura automaticamente (normalmente a cada várias horas).



5. Na guia **Condições da regra**, especifique pelo menos um critério para os dispositivos que deseja serem movidos automaticamente.

6. Clique em **Salvar**.

A nova regra de movimentação é criada. Ela é exibida na lista de regras de movimento.

Condições para migrar uma regra de um dispositivo

Ao criar ou copiar uma regra para migrar dispositivos cliente para grupos de administração, na guia **Condições da regra**, as condições para migrar os dispositivos serão definidas. Para determinar quais dispositivos migrar, será necessário usar os seguintes critérios:

- Tags atribuídas a dispositivos clientes.
- Parâmetros de rede. Por exemplo, é possível migrar os dispositivos com os endereços IP a partir de um intervalo especificado.
- Proprietário do dispositivo, sua função e associação ao grupo de segurança.
- Aplicativos gerenciados e instalados em dispositivos clientes, por exemplo, o Agente de Rede ou o Servidor de Administração.
- Máquinas virtuais, que são os dispositivos clientes.
- Unidades organizacionais do controlador de domínio.
- Segmentos da nuvem.

Abaixo, é possível encontrar a descrição sobre a especificação dessas informações em uma regra de movimentação de dispositivos.

Caso especifique várias condições na regra, o operador lógico AND funcionará e todas as condições serão aplicadas ao mesmo tempo. Caso não selecione nenhuma opção ou alguns campos sejam deixados em branco, essas condições não serão aplicadas.

Guia Tags

Nesta guia, é possível configurar uma regra de migração de dispositivo de acordo com as tags de dispositivo adicionadas anteriormente nas descrições dos dispositivos clientes. Para fazer isso, selecione as tags necessárias. Além disso, é possível ativar as seguintes opções:

Aplicar aos dispositivos sem tags especificadas

Caso esta opção esteja habilitada, todos os dispositivos com as tags especificadas serão excluídos de uma regra de migração de dispositivos. Caso esta opção esteja desabilitada, a regra de migração de dispositivo será aplicável aos dispositivos com todas as tags selecionadas.

Por padrão, esta opção está desativada.

Aplicar se pelo menos uma tag especificada corresponder

Caso esta opção esteja habilitada, uma regra de migração de dispositivo será aplicável aos dispositivos clientes com pelo menos uma das tags selecionadas. Caso esta opção esteja desabilitada, a regra de migração de dispositivo será aplicável aos dispositivos com todas as tags selecionadas.

Por padrão, esta opção está desativada.

Guia Rede

Nesta guia, é possível especificar os dados de rede dos dispositivos que uma regra de migração de dispositivo considera:

Nome do dispositivo na rede Windows

Nome da rede Windows (nome NetBIOS) do dispositivo ou o endereço IPv4 ou IPv6.

Domínio do Windows

Uma regra de migração de dispositivo será aplicável a todos os dispositivos incluídos no domínio do Windows especificado.

Nome DNS do dispositivo

Nome do domínio DNS do dispositivo cliente que deseja migrar. Preencha este campo se sua rede incluir um servidor DNS.

Caso o agrupamento com distinção entre maiúsculas e minúsculas seja definido para o banco de dados usado para o Kaspersky Security Center Linux, mantenha maiúsculas e minúsculas ao especificar um nome DNS de dispositivo. Caso contrário, a regra de movimentação do dispositivo não funcionará.

Domínio DNS

Uma regra de migração de dispositivo será aplicável a todos os dispositivos incluídos no sufixo DNS principal especificado. Preencha este campo se sua rede incluir um servidor DNS.

Intervalo de IPs

Se esta opção estiver ativada, você poderá inserir os endereços IP inicial e final do conjunto de IPs no qual os dispositivos relevantes devem ser incluídos.

Por padrão, esta opção está desativada.

Endereço IP para conexão com o Servidor de Administração

Caso esta opção esteja habilitada, será possível definir os endereços IP pelos quais os dispositivos clientes serão conectados ao Servidor de Administração. Para fazer isso, especifique o intervalo de IP que inclui todos os endereços IP necessários.

Por padrão, esta opção está desativada.

O dispositivo está localizado em um subgrupo do grupo de Domínios

Se esta opção estiver ativada, você poderá selecionar um subgrupo do grupo Domínios. Os dispositivos relevantes devem estar localizados no subgrupo selecionado.

Por padrão, esta opção está desativada.

O dispositivo está no intervalo de IPs

Se esta opção estiver habilitada, você poderá selecionar um intervalo de IP que você adicionou anteriormente na seção **Intervalos de IPs**. Os dispositivos relevantes devem ser incluídos no intervalo de IPS selecionado.

Por padrão, esta opção está desativada.

Perfil de conexão alterado

Selecione um dos seguintes valores:

- **Sim**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente com um perfil de conexão alterado.
- **Não**. A regra de movimentação de dispositivos se aplica apenas aos dispositivos clientes cujo perfil de conexão não foi alterado.
- **Nenhum valor está selecionado**. A condição não se aplica.

Gerenciado por outro Servidor de Administração

Selecione um dos seguintes valores:

- **Sim**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente gerenciados por outros Servidores de Administração. Esses servidores são diferentes do servidor no qual a regra de migração de dispositivo é configurada.
- **Não**. A regra de movimentação de dispositivos aplica-se apenas a dispositivos clientes gerenciados pelo Servidor de Administração atual.
- **Nenhum valor está selecionado**. A condição não se aplica.

Guia Proprietário do dispositivo

Nesta guia, você pode configurar uma regra de movimentação de dispositivos com base no proprietário do dispositivo, na associação ao grupo de segurança e na função:

Proprietário do dispositivo

Selecione o nome de usuário do proprietário do dispositivo em um grupo de segurança interno. Saiba mais sobre usuários e funções de usuário nesta seção.

> Somente um usuário pode ser registrado como proprietário do dispositivo.

Associação do proprietário do dispositivo no grupo de segurança do Active Directory

Selecione um grupo de segurança externo do Active Directory ao qual o proprietário do dispositivo pertence.

> O usuário pode fazer parte de um grupo de segurança do Active Directory ou de um grupo incluído nesse grupo de segurança do Active Directory.

Função do proprietário do dispositivo

Selecione a função atribuída ao proprietário do dispositivo. Saiba mais sobre as funções do usuário neste artigo.

Associação do proprietário do dispositivo em um grupo de segurança interno

Selecione um grupo de segurança interno ao qual o proprietário do dispositivo pertence.

Guia Aplicativos

Nesta guia, é possível configurar uma regra de migração de dispositivo de acordo com os aplicativos gerenciados e sistemas operacionais instalados nos dispositivos cliente:

Agente de Rede instalado

Selecione um dos seguintes valores:

- **Sim**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente com o Agente de Rede instalado.
- **Não**. A regra de movimentação de dispositivos se aplica apenas a dispositivos clientes nos quais o Agente de Rede não está instalado.
- **Nenhum valor está selecionado**. A condição não se aplica.

Aplicativos

Especifique quais aplicativos gerenciados devem ser instalados em dispositivos cliente para que uma regra de migração de dispositivo seja aplicável a esses dispositivos. Por exemplo, é possível selecionar **Agente de Rede do Kaspersky Security Center 17** ou **Servidor de Administração do Kaspersky Security Center 17**.

Caso nenhum aplicativo gerenciado seja selecionado, a condição não será aplicável.

Versão do SO

É possível selecionar os dispositivos cliente de acordo com a versão do sistema operacional. Para isso, especifique os sistemas operacionais que devem ser instalados nos dispositivos cliente. Assim, uma regra de migração de dispositivo será aplicável aos dispositivos cliente com os sistemas operacionais selecionados.

Caso esta opção não seja habilitada, a condição não será aplicável. Por padrão, esta opção está desativada.

Arquitetura do SO

É possível selecionar os dispositivos cliente pelos tamanhos de bits do sistema operacional. No campo **Arquitetura do sistema operacional**, será possível selecionar um dos seguintes valores:

- **Desconhecido**
- **x86**
- **AMD64**
- **IA64**

Para verificar a arquitetura do sistema operacional dos dispositivos cliente:

1. No menu principal, acesse a seção **Gerenciamento de ativos** → **Dispositivos gerenciados**.
2. Clique no botão **Configurações de colunas** (⚙) à direita.
3. Selecione a opção **Arquitetura do SO** e clique no botão **Salvar**.

   Depois disso, a arquitetura do sistema operacional será exibida para cada dispositivo gerenciado.

Gerenciador de pacotes do SO

É possível remover os dispositivos clientes usando o gerenciador de pacotes do sistema operacional. No campo **Gerenciador de pacotes do SO**, será possível selecionar um dos seguintes valores:

- rpm: para dispositivos que executam os sistemas operacionais Red Hat Enterprise Linux, CentOS, Fedora, SUSE e Oracle Linux
- apt (dpkg): para dispositivos que executam os sistemas operacionais Debian, Ubuntu e Kali
- pkg: para dispositivos que executam os sistemas operacionais FreeBSD e OpenBSD

Para verificar o gerenciador de pacotes do sistema operacional dos dispositivos cliente:

1. No menu principal, acesse a seção **Gerenciamento de ativos** → **Dispositivos gerenciados**.
2. Clique no botão **Configurações de colunas** (⚙) à direita.
3. Selecione a opção **Gerenciador de pacotes do SO** e clique no botão **Salvar**.

O gerenciador de pacotes do sistema operacional é exibido para cada dispositivo gerenciado.

Versão do pacote de serviço do SO

Neste campo, você pode especificar a versão do pacote do sistema operacional (no formato *X.Y*), o que determinará como a regra de migração será aplicada ao dispositivo. Por padrão, nenhum valor de versão é especificado.

Certificado do usuário

Selecione um dos seguintes valores:

- **Instalado**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos móveis com um certificado móvel.
- **Não instalado**. A regra de migração de dispositivo se aplicável apenas aos dispositivos móveis sem um certificado móvel.
- **Nenhum valor está selecionado**. A condição não se aplica.

Compilação do SO

Esta configuração é aplicável somente aos sistemas operacionais Windows.

É possível especificar se o sistema operacional selecionado ter um número de versão igual, anterior ou posterior. Também é possível configurar a regra de migração de dispositivo para todos os números de compilação, exceto o especificado.

Número da versão do SO

Esta configuração é aplicável somente aos sistemas operacionais Windows.

É possível especificar se o sistema operacional selecionado ter um número de versão igual, anterior ou posterior. Também é possível configurar a regra de migração de dispositivo para todos os números de compilação, exceto o especificado.

Guia Máquinas virtuais

Na guia, é possível configurar a migração de dispositivo de acordo com o fato de que os dispositivos cliente sejam máquinas virtuais ou parte da Virtual Desktop Infrastructure (VDI):

Esta é uma máquina virtual

Na lista suspensa, é possível selecionar os seguintes itens:

- **N/A**. A condição não se aplica.
- **Não**. Mover dispositivos que não sejam máquinas virtuais.
- **Sim**. Migrar dispositivos que sejam máquinas virtuais.

Tipo de máquina virtual

Parte da Virtual Desktop Infrastructure

Na lista suspensa, é possível selecionar os seguintes itens:

- **N/A**. A condição não se aplica.
- **Não**. Mover dispositivos que não fazem parte do VDI.
- **Sim**. Migre os dispositivos que fazem parte da VDI.

Guia Controlador de domínio

Nesta guia, é possível especificar se é necessário mover os dispositivos incluídos no domínio da unidade organizacional. Também é possível mover os dispositivos de todas as unidades organizacionais secundárias do domínio da unidade organizacional especificado:

O dispositivo está incluído na seguinte unidade organizacional

Caso esta opção esteja ativada, uma regra de migração de dispositivos será aplicada aos dispositivos da unidade organizacional do controlador de domínio especificada na lista da opção.

Por padrão, esta opção está desativada.

Incluir unidades organizacionais secundárias

Caso esta opção esteja ativada, a seleção incluirá os dispositivos das unidades organizacionais secundárias da unidade organizacional do controlador de domínio especificado.

Por padrão, esta opção está desativada.

Migrar dispositivos de unidades secundárias para os subgrupos correspondentes

Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente

Excluir subgrupos não presentes no domínio

O dispositivo está incluído no seguinte grupo de segurança do domínio

Caso esta opção esteja ativada, uma regra de movimentação de dispositivos se aplica aos dispositivos do grupo de segurança do domínio especificado na lista da opção.

Por padrão, esta opção está desativada.

Guia Segmentos da nuvem

Nesta guia, você pode especificar que é necessário mover os dispositivos incluídos no segmento da nuvem. Também é possível mover os dispositivos de todas as unidades organizacionais secundárias do domínio da unidade organizacional especificado:

O dispositivo está no segmento da nuvem

Se você selecionar esta opção, a regra de migração de dispositivos será aplicada aos dispositivos clientes que pertencem a um segmento da nuvem. Você pode selecionar o segmento da nuvem necessário até uma sub-rede na lista sob a opção.

Por padrão, esta opção está desativada.

Incluir objetos secundários

Caso esta opção esteja ativada, a seleção incluirá os dispositivos de todas as unidades organizacionais secundárias do segmento da nuvem especificado.

Por padrão, esta opção está desativada.

Migrar dispositivos de objetos aninhados para os subgrupos correspondentes

Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente

Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem

Dispositivo detectado usando a API

Na lista suspensa, é possível selecionar os seguintes itens:

- Nenhum valor está selecionado. A condição não se aplica.
- **Não**. Mover dispositivos que não foram descobertos usando a API.
- **AWS**. Mover dispositivos descobertos pela API da AWS.
- **Azure**. Mover dispositivos descobertos pela API do Azure.
- **Google Cloud**. Mover dispositivos descobertos pela API do Google Cloud.

Depois disso, dependendo do valor selecionado, você pode preencher os seguintes campos:

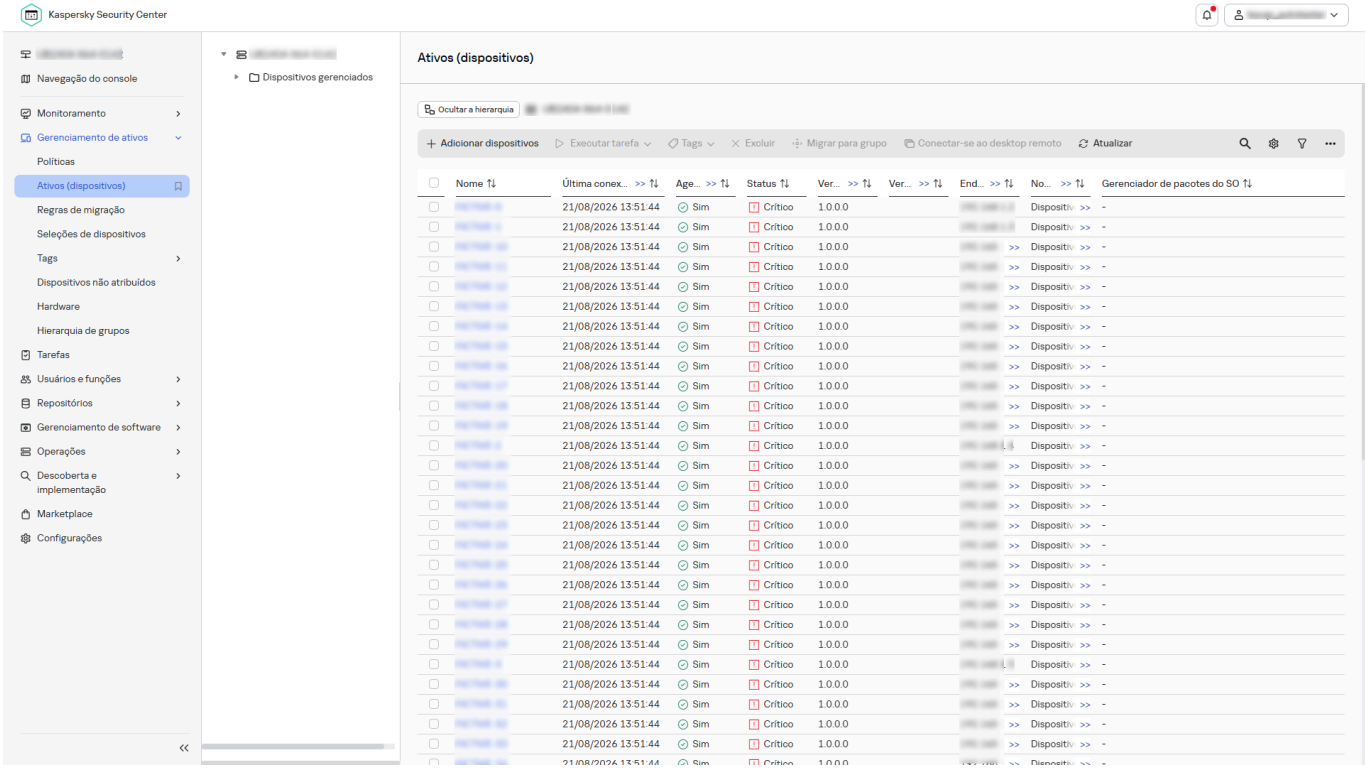
- **Sub-rede do dispositivo na nuvem**.
- **Zona de disponibilidade do dispositivo na nuvem**.
- **Grupo de posicionamento de dispositivos na nuvem**.

Adicionar dispositivos manualmente a um grupo de administração

É possível mover dispositivos para grupos de administração automaticamente, criando regras de movimentação de dispositivos, ou manualmente, movendo dispositivos de um grupo de administração para outro, ou adicionando dispositivos a um grupo de administração selecionado. Esta seção descreve como adicionar dispositivos a um grupo de administração manualmente.

Para adicionar manualmente um ou mais dispositivos a um grupo de administração selecionado:

1. No menu principal, vá para **Gerenciamento de ativos → Dispositivos gerenciados**.



A lista de dispositivos gerenciados

2. Selecione o grupo de administração para o qual deseja adicionar os dispositivos:

   - Para o grupo raiz:

     Neste caso, é necessário prosseguir para a próxima etapa.

   - Para um subgrupo:

     a. Clique no botão **Mostrar a hierarquia** na parte superior da página.

     O nome do botão mudará para **Ocultar a hierarquia**.

     b. Na janela aberta, clicar no nome do subgrupo.

   O caminho para o grupo selecionado é exibido na parte superior da página. Caso necessário, é possível clicar em um link com o nome do grupo de administração para ir até o grupo. Por padrão, o último link no caminho fica inativo. Além disso, é possível fechar a janela de hierarquia clicando no botão **Ocultar a hierarquia**.

3. Clique no botão **Adicionar dispositivos**.

   O Assistente para Mover Dispositivos é iniciado.

4. Faça uma lista dos dispositivos que deseja adicionar ao grupo de administração.

> Só é possível adicionar dispositivos para os quais informações já tenham sido adicionadas ao banco de dados do Servidor de Administração ao conectar o dispositivo ou após a descoberta de dispositivos.

Selecione como deseja adicionar dispositivos à lista:

- Clique no botão **Adicionar dispositivos** e especifique os dispositivos de uma das seguintes maneiras:
  - Selecione dispositivos na lista de dispositivos detectados pelo Servidor de Administração.
  - Especifique o endereço IP de um dispositivo ou um conjunto de IPs.

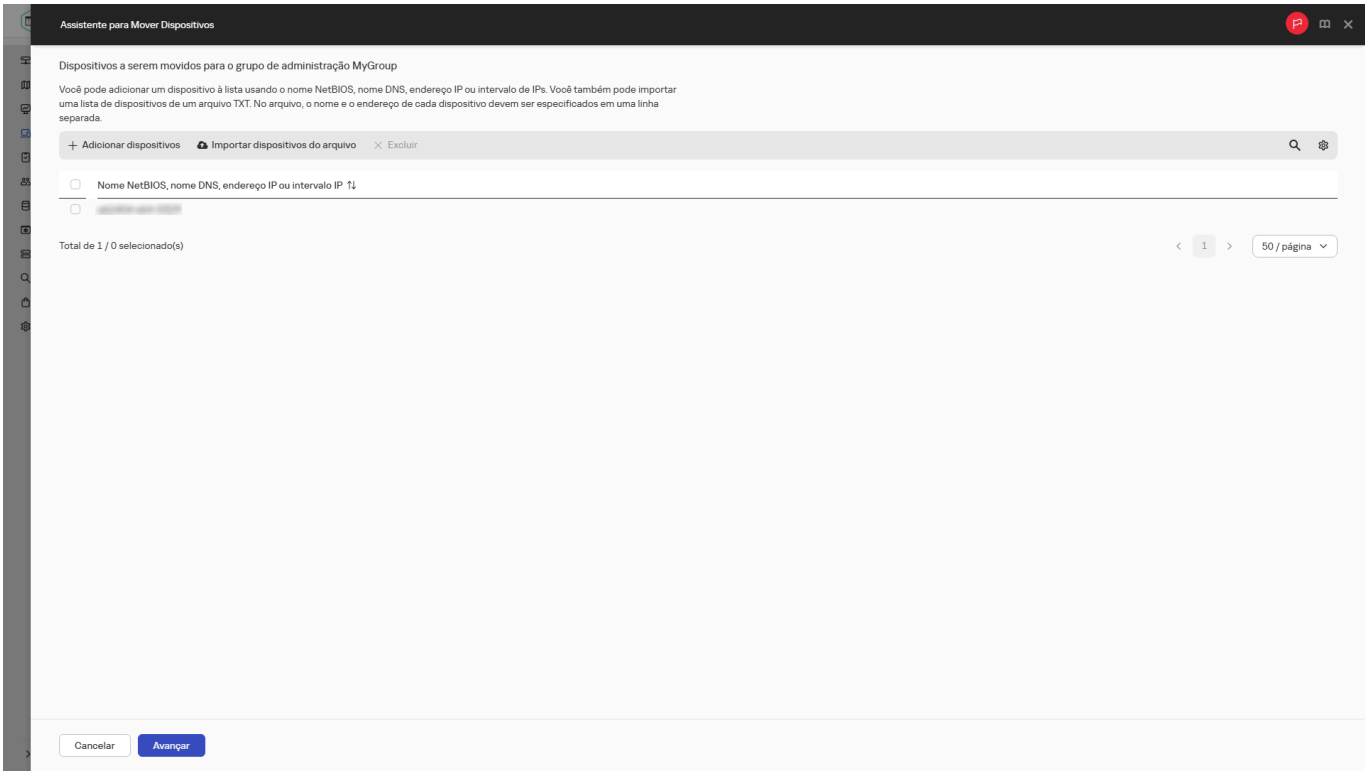
    O intervalo de IPs não deve conter mais de 1.048.576 endereços.

  - Especifique um nome DNS do dispositivo.

    O campo do nome do dispositivo não deve caracteres de espaço, retorno nem os seguintes caracteres proibidos: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Clique no botão **Importar dispositivos do arquivo** para importar uma lista de dispositivos a partir de um arquivo .txt. Cada endereço ou nome de dispositivo deve ser especificado em uma linha separada.

  O arquivo não deve conter caracteres de espaços, retrocessos nem os seguintes caracteres proibidos: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %



Seleção de dispositivos para mover para o grupo de administração

5. Veja a lista de dispositivos a serem adicionados ao grupo de administração. É possível editar a lista adicionando ou removendo dispositivos.

6. Depois de garantir que a lista esteja correta, clique no botão **Avançar**.

O assistente processa a lista de dispositivos e exibe o resultado. Os dispositivos processados com sucesso são adicionados ao grupo de administração e exibidos na lista de dispositivos sob nomes gerados pelo Servidor de

Migrando dispositivos ou clusters manualmente para um grupo de administração

Você pode mover dispositivos de um grupo de administração para outro ou do grupo de dispositivos não atribuídos para um grupo de administração.

É possível também mover clusters ou matrizes de servidor de um grupo de administração para outro. Ao mover um cluster ou matriz de servidores para outro grupo, todos os seus nós são movidos com ele, porque um cluster e qualquer um de seus nós sempre pertencem ao mesmo grupo de administração. Quando um único nó de cluster é selecionado na guia **Dispositivos**, o botão **Migrar para grupo** fica indisponível.

Para migrar um ou diversos dispositivos ou clusters em um grupo de administração selecionado:

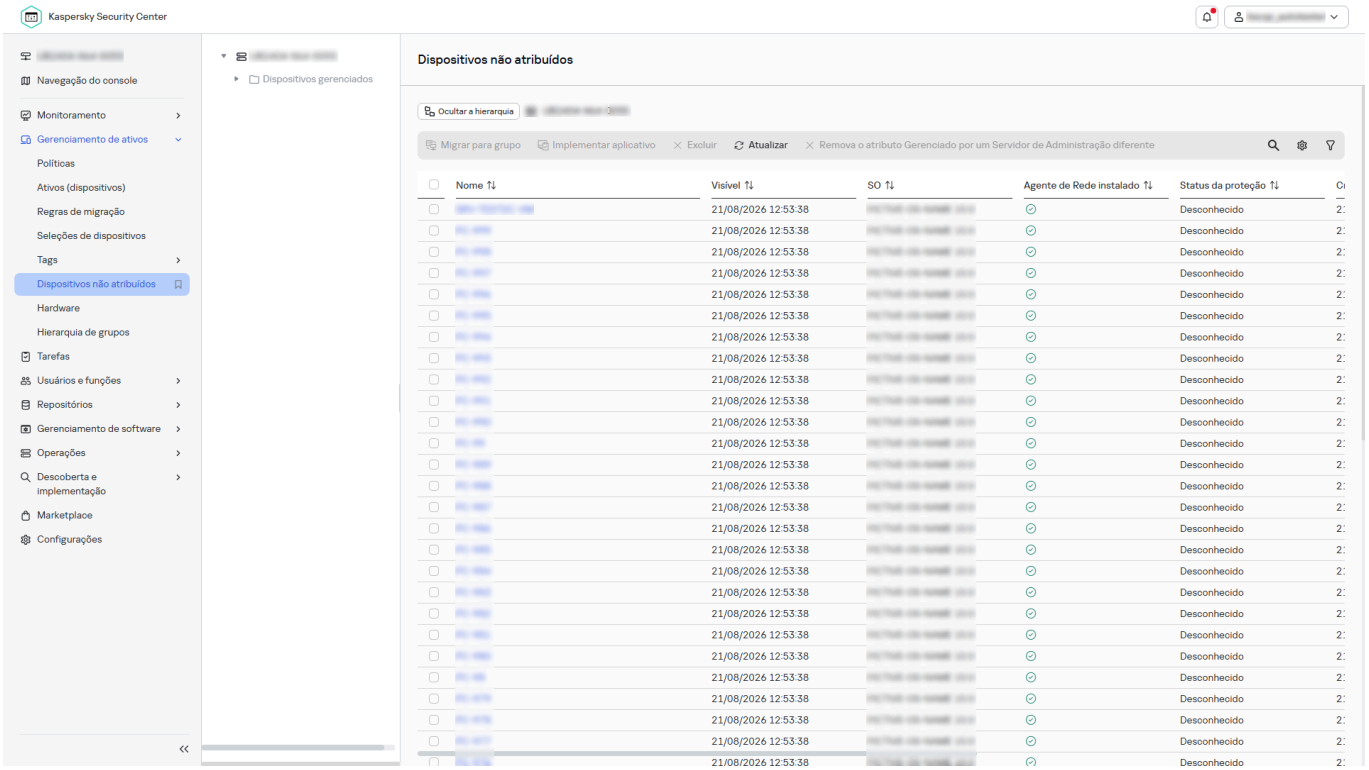
1. Abra o grupo de administração do qual você deseja migrar os dispositivos. Para fazer isso, siga uma destas etapas:

   - Para abrir um grupo de administração, no menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados** e selecione o grupo de administração desejado.

     - Para o grupo raiz, é possível prosseguir para a próxima etapa.

     - Para um subgrupo, clique no botão **Mostrar a hierarquia** na parte superior da página e, na janela que é exibida, selecione o grupo de administração desejado.

   - Para abrir o grupo **Dispositivos não atribuídos**, no menu principal, vá para **Gerenciamento de ativos** → **Dispositivos não atribuídos**.



A lista de dispositivos não atribuídos

2. Caso o grupo de administração contenha clusters ou matrizes de servidores, a seção **Dispositivos gerenciados** será dividida em duas guias – a guia **Dispositivos** e a guia **Grupamentos e matrizes de servidores**. Abra a guia do objeto que deseja mover.

3. Marque a caixa de seleção ao lado dos dispositivos ou clusters que deseja migrar para um grupo diferente.

4. Clique no botão **Migrar para grupo**.

5. Na hierarquia de grupos de administração, marque a caixa de seleção ao lado do grupo de administração para o qual deseja migrar os dispositivos ou clusters selecionados.

6. Clique no botão **Migrar**.

Os dispositivos ou clusters selecionados são movidos para o grupo de administração selecionado.

Sobre clusters e matrizes de servidores

O Kaspersky Security Center Linux é compatível com a tecnologia de cluster. Se o Agente de Rede enviar uma informação ao Servidor de Administração confirmando que o aplicativo instalado no dispositivo cliente faz parte de uma matriz de servidor, este dispositivo cliente torna-se um nó de cluster.

Caso um grupo de administração contenha clusters ou matrizes de servidor, a página **Dispositivos gerenciados** exibe duas guias – uma para dispositivos individuais e outra para clusters e matrizes de servidor. Depois que os dispositivos gerenciados são detectados como nós de cluster, o cluster é adicionado como um objeto individual à guia **Grupamentos e matrizes de servidores**.

Os nós da matriz de cluster ou servidor são listados na guia **Dispositivos**, juntamente com outros dispositivos gerenciados. É possível ver propriedades dos nós como dispositivos individuais e executar outras operações, mas não é possível excluir um nó de cluster ou movê-lo para outro grupo de administração separadamente de seu cluster. Só é possível excluir ou mover um cluster inteiro.

É possível executar as seguintes operações com clusters ou matrizes de servidor:

- Ver propriedades
- Mover o cluster ou matriz de servidores para outro grupo de administração

  Ao mover um cluster ou matriz de servidores para outro grupo, todos os seus nós são movidos com ele, porque um cluster e qualquer um de seus nós sempre pertencem ao mesmo grupo de administração.

- Excluir

  É razoável excluir um cluster ou matriz de servidor somente quando o cluster ou matriz de servidor não existir mais na rede da organização. Caso um cluster ainda esteja visível em sua rede, e caso o Agente de Rede e o aplicativo de segurança da Kaspersky ainda estejam instalados nos nós de cluster, a Kaspersky Security Center Linux retornará automaticamente o cluster excluído e seus nós para a lista de dispositivos gerenciados.

Propriedades de um cluster ou matriz de servidores

Para visualizar as configurações de um cluster ou matriz de servidores:

1. No menu principal, vá para **Gerenciamento de ativos → Dispositivos gerenciados → Grupamentos e matrizes de servidores**.

   A lista de clusters e matrizes de servidores é exibida.

2. Clique no nome do cluster ou matriz de servidor necessária.

A janela de propriedades do cluster ou matriz de servidor selecionada é exibida.

Geral

A seção **Geral** exibe informações gerais sobre o cluster ou a matriz de servidores. As informações são fornecidas com base nos dados recebidos durante a última sincronização dos nós de cluster com o Servidor de Administração:

Nome

Descrição

Domínio do Windows

Domínio ou grupo de trabalho do Windows, que contém o cluster ou a matriz do servidor.

Nome do NetBIOS

Nome da rede Windows do cluster ou matriz de servidor.

Nome DNS

Nome do domínio DNS do cluster ou matriz de servidor.

Tarefas

Na guia **Tarefas**, é possível gerenciar as tarefas atribuídas ao cluster ou matriz de servidores: visualizar a lista de tarefas existentes; criar novas tarefas; remover, iniciar e interromper tarefas; modificar as suas configurações; e visualizar os resultados da execução. As tarefas listadas estão relacionadas ao aplicativo de segurança Kaspersky instalado nos nós de cluster. A Kaspersky Security Center Linux recebe a lista de tarefas e os detalhes do status da tarefa dos nós de cluster. Se uma conexão não for estabelecida, o status não será exibido.

Nós

Essa guia exibe uma lista de nós incluídos no cluster ou na matriz do servidor. É possível clicar em um nome de nó para visualizar a janela de propriedades do dispositivo.

Aplicativo Kaspersky

A janela de propriedades também pode conter guias adicionais com informações e configurações relacionadas ao aplicativo de segurança Kaspersky instalado nos nós de cluster.

Ajuste de pontos de distribuição e gateways de conexão

Uma estrutura de grupos de administração no Kaspersky Security Center Linux executa as seguintes funções:

- Define o escopo das políticas

  Há um modo alternativo para aplicar configurações relevantes nos dispositivos, usando *perfis de política*.

- Define o escopo da tarefas de grupo

  Há uma abordagem para definir o escopo da tarefas de grupo que não tem base em uma hierarquia de grupos de administração: uso de tarefas para seleções de dispositivos e tarefas para dispositivos específicos.

- Define os direitos de acesso aos dispositivos, Servidores de Administração virtuais e Servidores de Administração secundários

- Atribui os pontos de distribuição

Ao criar a estrutura de grupos de administração, você deve levar em conta a topologia da rede da organização para a atribuição ótima de pontos de distribuição. A distribuição ótima dos pontos de distribuição permite poupar tráfego na rede da organização.

Dependendo do esquema da organização e da topologia da rede, as seguintes configurações padrão podem ser aplicadas à estrutura de grupos de administração:

- Escritório único

- Múltiplos pequenos escritórios remotos

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Sobre os pontos de distribuição

Um dispositivo com o Agente de Rede instalado pode ser usado como um ponto de distribuição. Nesse modo, o Agente de Rede pode distribuir as atualizações que podem ser recuperadas do Servidor de Administração ou dos servidores da Kaspersky. Nesse último caso, configure o download da atualização para um ponto de distribuição.

A implementação de pontos de distribuição em uma rede da organização tem os seguintes objetivos:

- Reduzir a carga no Servidor de Administração.
- Otimizar o tráfego.
- Fornecer ao Servidor de Administração o acesso aos dispositivos em pontos de difícil acesso de uma rede da organização. A disponibilidade de um ponto de distribuição na rede além da NAT (em relação ao Servidor de Administração) permite ao Servidor de Administração executar as seguintes ações:
  - Enviar notificações para dispositivos por UDP na rede IPv4 ou IPv6
  - Sondar a rede IPv4 ou IPv6
  - Executar a implementação inicial
  - Atuar como um servidor push

Um ponto de distribuição é atribuído para um grupo de administração. Neste caso, o escopo do ponto de distribuição inclui todos os dispositivos dentro do grupo de administração e todos dos seus subgrupos. No entanto, o dispositivo que atua como o ponto de distribuição não pode estar incluído no grupo de administração ao qual foi atribuído.

Você pode criar uma função de ponto de distribuição como um gateway de conexão. Neste caso, os dispositivos no escopo do ponto de distribuição serão conectados ao Servidor de Administração por meio do gateway, não diretamente. Este modo pode ser útil em cenários que não permitem o estabelecimento de uma conexão direta entre o Servidor de Administração e os dispositivos gerenciados.

Se você usar um dispositivo baseado em Linux como um ponto de distribuição, é altamente recomendável aumentar o limite de descritores de arquivo para o serviço klnagent, porque se o escopo do ponto de distribuição incluir muitos dispositivos, o número máximo padrão de arquivos que podem ser abertos pode não ser suficiente.

Configuração padrão de pontos de distribuição: escritório único

Em uma configuração de "escritório único" padrão, todos os dispositivos estão dentro da rede da organização, portanto eles podem se "ver" mutuamente. A rede da organização pode consistir em algumas partes separadas (redes ou segmentos de rede) vinculadas por canais estreitos.

Os seguintes métodos de criar a estrutura de grupos de administração são possíveis:

- Criar uma estrutura de grupos de administração levando em consideração a topologia da rede. A estrutura de grupos de administração pode não refletir a topologia da rede com uma precisão absoluta. Uma coincidência entre as partes separadas da rede e determinados grupos de administração seria suficiente. Você pode usar a atribuição automática de pontos de distribuição ou atribui-los manualmente.

- Criar uma estrutura de grupos de administração não levando em consideração a topologia da rede. Nesse caso, é necessário desativar a atribuição automática de pontos de distribuição e, a seguir, atribuir um ou diversos dispositivos para atuar como pontos de distribuição de um grupo de administração raiz em cada uma das partes separadas da rede, por exemplo, para o grupo **Dispositivos gerenciados**. Todos os pontos de distribuição estarão no mesmo nível e apresentarão a mesma expansão de escopo para todos os dispositivos na rede da organização. Nesse caso, cada Agente de Rede se conectará ao ponto de distribuição que tenha a rota mais curta. A rota para um ponto de distribuição pode ser traçada com o utilitário tracert.

Configuração padrão de pontos de distribuição: múltiplos pequenos escritórios remotos

Esta configuração padrão proporciona uma série de pequenos escritórios remotos, que podem se comunicar com a sede através da Internet. Cada escritório remoto é localizado além da NAT, ou seja, a conexão de um escritório remoto ao outro não é possível porque os escritórios estão isolados entre si.

A configuração deve ser refletida na estrutura de grupos de administração: um grupo de administração separado deve ser criado para cada escritório remoto (grupos **Escritório 1** e **Escritório 2** na figura abaixo).



Os escritórios remotos estão incluídos na estrutura do grupo de administração

Um ou vários pontos de distribuição devem ser atribuídos à cada grupo de administração que corresponda a um escritório. Os pontos de distribuição devem ser dispositivos nos escritórios remotos que têm espaço livre suficiente em disco. Os dispositivos implementados no grupo **Escritório 1**, por exemplo, acessarão os pontos de distribuição atribuídos ao grupo de administração **Escritório 1**.

Se alguns usuários se moverem entre escritórios fisicamente, com os seus computadores portáteis, você deve selecionar dois ou mais dispositivos (além dos pontos de distribuição existentes) em cada escritório remoto e atribui-los para atuar como pontos de distribuição para um grupo de administração de nível superior (**Grupo de raiz para escritórios** na figura acima).

Exemplo: Um computador portátil é implementado no grupo de administração **Escritório 1** e então é movido fisicamente para o escritório que corresponde ao grupo de administração **Escritório 2**. Após o computador portátil ter sido movido, o Agente de Rede tenta acessar os pontos de distribuição atribuídos ao grupo **Escritório 1**, mas aqueles pontos de distribuição estão indisponíveis. Então, O Agente de Rede começa a tentar acessar os pontos de distribuição que foram atribuídos ao **Grupo de raiz para escritórios**. Como os escritórios remotos estão isolados entre si, as tentativas de acessar os pontos de distribuição atribuídos ao grupo de administração **Grupo raiz para escritórios** somente terão êxito quando o Agente de Rede tentar acessar os pontos de distribuição no grupo **Escritório 2**. Ou seja, o computador portátil permanecerá no grupo de administração que corresponde ao escritório inicial, mas o computador portátil usará o ponto de distribuição do escritório onde estiver fisicamente localizado no momento.

Calcular o número e a configuração de pontos de distribuição

Quanto mais dispositivos clientes uma rede contiver, mais pontos de distribuição ela exigirá. Recomendamos que você não desative a atribuição automática de pontos de distribuição. Quando a atribuição automática de pontos de distribuição estiver ativada, o Servidor de Administração atribui pontos de distribuição se o número de dispositivos clientes for bastante grande e define a sua configuração.

Usar pontos de distribuição exclusivamente atribuídos

Se você planejar usar determinados dispositivos específicos como pontos de distribuição (ou seja, servidores exclusivamente atribuídos), você pode optar por não utilizar a atribuição automática de pontos de distribuição. Neste caso, assegure-se de que os dispositivos aos quais você pretende tornar pontos de distribuição tenham volume suficiente de espaço livre em disco, não sejam desligados regularmente e estejam com o modo Suspenso desativado.

Número de pontos de distribuição dedicados em uma rede com um segmento de rede, dependendo do número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Número de pontos de distribuição dedicados em uma rede com vários segmentos de rede, dependendo do número de dispositivos na rede

Número de dispositivos cliente em cada segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10–100	1
Mais de 100	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Usar dispositivos clientes padrão (estações de trabalho) como pontos de distribuição

Se você planejar usar dispositivos clientes padrão (isto é, estações de trabalho) como pontos de distribuição, recomendamos atribuir pontos de distribuição, como mostrado nas tabelas abaixo, para evitar a carga excessiva dos canais de comunicação e do Servidor de Administração:

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém um segmento de rede único, com base no número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém vários segmentos de rede, com base no número de dispositivos na rede

Número de dispositivos cliente em cada segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10–30	1
31–300	2
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

Se um ponto de distribuição estiver desativado (ou não disponível por algum outro motivo), os dispositivos gerenciados no escopo poderão acessar o Servidor de Administração para as atualizações.

Atribuir os pontos de distribuição automaticamente

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center Linux selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos.

Os dispositivos que executam o Microsoft Windows on Arm não podem atuar como pontos de distribuição.

Para atribuir os pontos de distribuição automaticamente:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Selecione a opção **Atribuir automaticamente os pontos de distribuição**.

   Se a atribuição automática dos dispositivos para agirem como pontos de distribuição estiver ativada, você não pode configurar manualmente os pontos de distribuição nem editar a lista de pontos de distribuição.

4. Clique no botão **Salvar**.

O Servidor de Administração atribui e configura automaticamente os pontos de distribuição.

Atribuir os pontos de distribuição manualmente

O Kaspersky Security Center Linux permite que você atribua dispositivos manualmente para agirem como pontos de distribuição.

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center Linux selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos. No entanto, se por algum motivo você precisar desativar a atribuição automática de pontos de distribuição (por exemplo, se quiser usar servidores atribuídos exclusivamente), poderá atribuir os pontos de distribuição manualmente após Calcular o número e a configuração dos pontos de distribuição.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Os dispositivos que executam o Microsoft Windows on Arm não podem atuar como pontos de distribuição.

Para atribuir manualmente os dispositivos para agir como ponto de distribuição:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Selecione a opção **Atribuir manualmente os pontos de distribuição**.

4. Clique no botão **Atribuir**.

5. Selecione o dispositivo que você quer atribuir como ponto de distribuição.

   Ao selecionar um dispositivo, tenha em mente os recursos da operação de pontos de distribuição e os requisitos definidos para o dispositivo que age como ponto de distribuição.

6. Selecione o grupo de administração que você quer incluir no escopo do ponto de distribuição selecionado.

7. Clique em **OK**.

   O pontos de distribuição que você adicionou será exibido na lista de pontos de distribuição na seção **Pontos de distribuição**.

8. Clique no ponto de distribuição recém-adicionado na lista para abrir sua janela de propriedades.

9. Configure o ponto de distribuição na janela de propriedades:

   - A seção **Geral** contém as configurações de interação entre o ponto de distribuição e os dispositivos clientes.

     Porta SSL

     O número da porta SSL para a conexão criptografada entre dispositivos clientes e o ponto de distribuição usando SSL.

     O número da porta padrão é 13000.

     Ativado

     Se esta opção estiver ativada, o IP multicasting será usado para distribuição automática de pacotes de instalação para dispositivos clientes dentro do grupo.

     O multicast de IP diminui o tempo necessário para instalar um aplicativo de um pacote de instalação em um grupo de dispositivos clientes, mas aumenta o tempo de instalação quando você instala um aplicativo em um único dispositivo cliente.

Endereço IP multicast

O endereço IP que será usado para multicasting. Você pode definir um endereço IP no conjunto de 224.0.0.0 – 239.255.255.255

Por padrão, o Kaspersky Security Center Linux atribui automaticamente um endereço IP multicast exclusivo dentro do intervalo especificado.

Número da porta de IP multicast

Número da porta para multicasting de IP.

Por padrão, o número de porta é 15001. Se o dispositivo com o Servidor de Administração instalado for especificado como o ponto de distribuição, por padrão a porta 13001 é usada para conexão SSL.

Endereço do ponto de distribuição para dispositivos remotos

O endereço de rede por meio do qual os dispositivos remotos se conectam ao ponto de distribuição.

Ativado

As atualizações são distribuídas para dispositivos gerenciados a partir das seguintes fontes:

- Este ponto de distribuição, caso esta opção esteja ativada.
- Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

Caso utilize os pontos de distribuição para implantar atualizações, será possível economizar tráfego, pois o número de downloads será reduzido. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. Você pode calcular o número e a configuração dos pontos de distribuição da sua rede para otimizar o tráfego e a carga.

Caso essa opção seja desativada, o número de downloads de atualização e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

Ativado

Os pacotes de instalação são distribuídos para dispositivos gerenciados a partir das seguintes fontes:

- Este ponto de distribuição, caso esta opção esteja ativada.
- Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

Se você usar pontos de distribuição para implementar pacotes de instalação, poderá economizar tráfego porque reduz o número de downloads. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. Você pode calcular o número e a configuração dos pontos de distribuição da sua rede para otimizar o tráfego e a carga.

Caso essa opção seja desativada, o número de downloads de pacotes de instalação e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

Ativado

No Kaspersky Security Center Linux, um ponto de distribuição pode funcionar como um servidor push para os dispositivos gerenciados por meio do protocolo móvel e para os dispositivos gerenciados pelo Agente de Rede. Por exemplo, um servidor push deve ser ativado se você quiser forçar a sincronização dos dispositivos KasperskyOS com o Servidor de Administração. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Se você tiver vários pontos de distribuição atribuídos ao mesmo grupo de administração, poderá ativar o servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

Porta do servidor push

O número da porta para o servidor push. Você pode especificar o número de qualquer porta livre.

- Na seção **Escopo**, especifique os grupos de administração para os quais o ponto de distribuição distribuirá atualizações.

- Na seção **Fonte de atualizações**, você pode selecionar uma fonte de atualizações para o ponto de distribuição:

  Fonte de atualizações

  Selecione uma origem de atualização para o ponto de distribuição:

  - Para permitir que o ponto de distribuição receba atualizações do Servidor de Administração, selecione **Obter do Servidor de Administração**.

  - Para permitir que o ponto de distribuição receba atualizações usando uma tarefa, selecione **Usar tarefa de download de atualizações** e, em seguida, especifique a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*:

    - Se essa tarefa já existir no dispositivo, selecione a tarefa na lista.

    - Se ainda não existir tal tarefa no dispositivo, clique no link **Criar tarefa** para criar uma tarefa. O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

  Baixar arquivos diff

  Esta opção ativa o recurso de download dos arquivos diff.

  Por padrão, esta opção está ativada.

- Caso seus pontos de distribuição usem o servidor proxy para se conectar à internet, na subseção **Configurações de conexão com a internet**, você poderá especificar as seguintes configurações:

  Usar o servidor proxy

  Se esta caixa de seleção estiver marcada, um servidor proxy da Internet será usado para conectar os pontos de distribuição aos servidores de atualização Kaspersky. Nos campos de entrada, você pode configurar a conexão com o servidor proxy.

  Por padrão, esta caixa de seleção está desmarcada.

  Endereço do servidor proxy

  Endereço do servidor proxy.

  Número da porta

  O número da porta que é usada para conexão.

  Ignorar servidor proxy para endereços locais

  Se esta opção estiver ativada, nenhum servidor proxy será usado para se conectar aos dispositivos na rede local.

  Por padrão, esta opção está desativada.

  Autenticação do servidor proxy

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

  Por padrão, esta caixa de seleção está desmarcada.

  Nome do usuário

Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida.

Senha

Senha da conta sob a qual a tarefa será executada.

- Na seção **Proxy da KSN**, você pode configurar o aplicativo para usar o ponto de distribuição para encaminhar solicitações do KSN a partir dos dispositivos gerenciados:

  Ativar o proxy da KSN no lado do ponto de distribuição

  O serviço Proxy da KSN é executado no dispositivo que é usado como um ponto de distribuição. Use este recurso para redistribuir e otimizar o tráfego na rede.

  O ponto de distribuição envia as estatísticas da KSN, que estão listadas na Declaração da Kaspersky Security Network, à Kaspersky.

  Por padrão, esta opção está desativada. A ativação desta opção somente terá efeito caso as opções **Usar Servidor de Administração como um servidor proxy** e **Concordo em usar a Kaspersky Security Network** estejam ativadas na janela de propriedades do Servidor de Administração.

  É possível atribuir um nó de um cluster ativo-passivo a um ponto de distribuição e habilitar o servidor proxy da KSN nesse nó.

  Encaminhar solicitações da KSN para o Servidor de Administração

  O ponto de distribuição encaminha solicitações do KSN dos dispositivos gerenciados para o Servidor de Administração.

  Por padrão, esta opção está ativada.

  Acessar a KSN Cloud/KPSN diretamente pela Internet

  O ponto de distribuição encaminha solicitações da KSN de dispositivos gerenciados para a KSN Cloud ou KPSN. As solicitações da KSN geradas no próprio ponto de distribuição também são enviadas diretamente para a KSN Cloud ou para a KPSN.

  Ignorar as configurações do servidor proxy ao se conectar com a KPSN

  Ative esta opção, caso tenha as configurações do servidor proxy definidas nas propriedades do ponto de distribuição ou na política do Agente de Rede, mas a sua arquitetura de rede requer que você use KPSN diretamente. Caso contrário, as solicitações dos aplicativos gerenciados não chegarão à KPSN.

  Esta alternativa estará disponível caso a opção **Acessar a KSN Cloud/KPSN diretamente pela Internet** seja selecionada.

  Porta

  O número da porta TCP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. O número da porta padrão é 13111.

  Usar porta UDP

  Se você desejar que os dispositivos gerenciados sejam conectados ao proxy da KSN através de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de Porta UDP. Por padrão, esta opção está ativada.

  Porta UDP

  O número da porta UDP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. A porta UDP padrão para se conectar ao servidor proxy KSN é 15111.

  Usar HTTPS

Se você precisar que os dispositivos gerenciados se conectem ao servidor proxy da KSN por meio de uma porta HTTPS, ative a opção **Usar HTTPS** e especifique um número em **HTTPS através da porta**. A porta HTTPS padrão para se conectar ao servidor proxy KSN é 17111.

Porta HTTPS

O número da porta HTTPS que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. A porta HTTPS padrão para se conectar ao servidor proxy KSN é 17111.

- Na seção **Gateway de conexão**, é possível configurar o ponto de distribuição para atuar como um gateway para conexão entre as instâncias do Agente de Rede e o Servidor de Administração:

  Gateway de conexão

  Caso uma conexão direta entre o Servidor de Administração e os Agentes de Rede não possa ser estabelecida em função da organização de sua rede, será possível usar o ponto de distribuição para atuar como o gateway de conexão entre o Servidor de Administração e os Agentes de Rede.

  Ative essa opção caso você precise que o ponto de distribuição atue como um gateway de conexão entre os Agentes de Rede e o Servidor de Administração. Por padrão, esta opção está desativada.

  Estabelecer conexão com o gateway a partir do Servidor de Administração (se o gateway estiver na DMZ)

  Caso o Servidor de Administração esteja localizado fora da zona desmilitarizada (DMZ), na rede local, os Agentes de Rede instalados em dispositivos remotos não poderão se conectar com o Servidor de Administração. É possível usar um ponto de distribuição como o gateway de conexão com conectividade reversa (o Servidor de Administração estabelece uma conexão com o ponto de distribuição).

  Ative essa opção caso seja necessário conectar o Servidor de Administração ao gateway de conexão na DMZ.

  Abra a porta local do Kaspersky Security Center Web Console

  Ative essa opção caso seja necessário que o gateway de conexão na DMZ abra uma porta para o Web Console que esteja na DMZ ou na Internet. Especifique o número da porta que será usada para conexão do Web Console com o ponto de distribuição. O número da porta padrão é 13299.

  Essa opção estará disponível caso a opção **Estabelecer conexão com o gateway a partir do Servidor de Administração (se o gateway estiver na DMZ)** seja ativada.

  Ao conectar os dispositivos móveis com o Servidor de Administração por meio do ponto de distribuição que atua como gateway de conexão, é possível ativar as seguintes opções:

  Abrir porta para dispositivos móveis (apenas autenticação SSL do Servidor de Administração)

  Ative essa opção caso seja necessário que o gateway de conexão abra uma porta para dispositivos móveis e especifique o número da porta que os dispositivos móveis usarão para estabelecer conexão com o ponto de distribuição. O número da porta padrão é 13292. O dispositivo móvel verificará o certificado do Servidor de Administração. Ao estabelecer a conexão, somente o Servidor de Administração será autenticado.

  Abrir porta para dispositivos móveis (autenticação SSL bidirecional)

Ative essa opção caso seja necessário que o gateway de conexão abra uma porta que será usada para autenticação bidirecional do Servidor de Administração e dispositivos móveis. O dispositivo móvel verificará o certificado do Servidor de Administração e o Servidor de Administração verificará o certificado de dispositivos móveis. Especificar as seguintes configurações:

- Número da porta que os dispositivos móveis usarão para conexão com o ponto de distribuição. O número da porta padrão é 13293.

- Nomes de domínio DNS do gateway de conexão que serão usados por dispositivos móveis. Separe os nomes de domínio com vírgulas. Os nomes de domínio especificados serão incluídos no certificado do ponto de distribuição. Caso os nomes de domínio usados pelos dispositivos móveis não correspondam ao nome comum no certificado do ponto de distribuição, os dispositivos móveis não se conectarão com ponto de distribuição.

  O nome de domínio DNS padrão é o nome FQDN do gateway de conexão.

Em ambos os casos, os certificados serão verificados durante o estabelecimento da sessão TLS somente no ponto de distribuição. Os certificados não são encaminhados para serem verificados pelo Servidor de Administração. Depois que uma sessão TLS é estabelecida com o dispositivo móvel, o ponto de distribuição usa o certificado do Servidor de Administração para criar um túnel para sincronização entre o dispositivo móvel e o Servidor de Administração. Caso a porta para autenticação SSL bidirecional seja aberta, a única maneira de distribuir o certificado de dispositivos móveis é por meio de um pacote de instalação.

- Configure a sondagem de rede do Windows usando o ponto de distribuição baseado no Windows.

  Domínios do Windows

  Você pode ativar a descoberta de dispositivos para domínios do Windows e definir o agendamento para a localização.

- Configure a sondagem do controlador de domínio pelo ponto de distribuição.

  Sondagem do controlador de domínio

  É possível ativar a descoberta de dispositivos para controladores de domínio.

  No campo **Sondagem**, depois de mudar a posição do botão de alternância para **Ativado**, é possível selecionar controladores de domínio para sondagem e também especificar o agendamento de sondagem para eles.

  Caso queira usar um ponto de distribuição do Linux, na seção **Sondar domínios especificados**, clique em **Adicionar** e especifique o endereço e as credenciais de usuário do controlador de domínio. Além disso, é possível especificar o tipo de domínio a ser sondado: Active Directory ou Samba, FreeIPA, ALD Pro.

  Se você usar um ponto de distribuição do Windows, poderá selecionar uma das seguintes opções:

  - **Sondar domínio atual**

  - **Sondar toda a floresta de domínios**

  - **Sondar domínios especificados**

- Configure a pesquisa de intervalos de IP por ponto de distribuição.

  Sondagem de intervalos de IP

  Você pode ativar a descoberta de dispositivos para conjuntos IPv4 e redes IPv6.

  Ao ativar a opção **Ativar sondagem de conjuntos**, você poderá adicionar conjuntos verificados e definir seu agendamento. Você pode adicionar conjuntos de IPs à lista de conjuntos verificados.

Ao ativar a opção **Usar Zeroconf para sondar redes IPv6**, o ponto de distribuição sonda automaticamente a rede IPv6 usando rede zero configuração (também referida como *Zeroconf*). Nesse caso, os conjuntos IP especificados são ignorados, pois o ponto de distribuição sonda toda a rede. A opção **Usar Zeroconf para sondar redes IPv6** estará disponível caso o ponto de distribuição execute Linux. Para usar a sondagem do Zeroconf IPv6, é necessário instalar o utilitário avahi-browse no ponto de distribuição.

- Na seção **Avançado**, especifique a pasta que o ponto de distribuição deve usar para armazenar os dados distribuídos.

  Usar pasta padrão

  Se você selecionar esta opção, o aplicativo usa a pasta de Instalação do Agente de Rede no ponto de distribuição.

  Usar pasta especificada

  Se selecionar esta opção, você pode, no campo abaixo, especificar o caminho até a pasta. Pode ser uma pasta local no ponto de distribuição ou pode ser uma pasta em qualquer dispositivo na rede corporativa.

  A conta do usuário usada no ponto de distribuição para executar o Agente de Rede deve ter acesso de leitura/gravação à pasta especificada.

10. Clique em **OK**.

Os dispositivos selecionados agirão como pontos de distribuição.

Adicionando um gateway de conexão na DMZ como um ponto de distribuição

Se o Servidor de Administração estiver fora da zona desmilitarizada (DMZ), os Agentes de Rede instalados em dispositivos externos não poderão se conectar ao Servidor de Administração. Nesse caso, você pode usar um ponto de distribuição como o gateway de conexão. O ponto de distribuição abre uma porta para o Servidor de Administração criar a conexão. Quando o Servidor de Administração for iniciado, ele se conecta com um ponto de distribuição e mantém essa conexão durante toda a sessão.

Se você precisar estabelecer uma conexão entre o Servidor de Administração e seus dispositivos gerenciados fora do período de sincronização entre o Agente de Rede e o Servidor de Administração, você deve ativar um servidor push e abrir a porta 13295 no lado do Ponto de distribuição.

Recomendamos que você use um dispositivo especialmente atribuído como o gateway de conexão. Para obter informações sobre o número máximo de dispositivos cliente (incluindo dispositivos móveis), consulte o guia de dimensionamento.

Um gateway de conexão aguarda por conexões do Servidor de Administração, em vez de estabelecer conexões com o Servidor de Administração. Isso significa que logo após um gateway de conexão ser instalado em um dispositivo na DMZ, o Servidor de Administração não lista o dispositivo entre os dispositivos gerenciados. Portanto, você precisa de um procedimento especial para garantir que o Servidor de Administração inicie uma conexão com o gateway de conexão.

Para adicionar um dispositivo com um gateway de conexão como ponto de distribuição:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Selecione a opção **Atribuir manualmente os pontos de distribuição**.

4. Na barra de ferramentas, clique no botão **Atribuir**.

5. No painel esquerdo que é exibido, execute uma das seguintes ações:

   a. Selecione a opção **Usar o gateway de conexão DMZ por endereço**.

   b. No campo **Endereço do gateway de conexão**, especifique o endereço IP ou o nome DNS do dispositivo.

   c. Clique no botão **Atribuir**.

   d. O painel é fechado e o ponto de distribuição é exibido com o nome **Entrada temporária para gateway de conexão**.

6. Clique no botão **Salvar**.

   O Servidor de Administração tenta se conectar ao gateway de conexão no endereço especificado. Se for bem-sucedido, o nome da entrada muda para o nome do dispositivo de gateway de conexão. Esse processo leva até cinco minutos.

Se você abrir as propriedades do ponto de distribuição clicando no nome **Entrada temporária para gateway de conexão**, todas as opções ficarão esmaecidas. Você só pode visualizar a guia Geral que exibe o nome do ponto de distribuição. Por padrão, a porta (13000) é usada. Você só pode configurar o ponto de distribuição após o Servidor de Administração se conectar a ele. Enquanto a entrada temporária do gateway de conexão está sendo convertida em uma entrada nomeada, o gateway de conexão também aparece no grupo Dispositivos não atribuídos.

Para adicionar um gateway de conexão a uma rede configurada anteriormente:

1. Instale o Agente de Rede na função de gateway de conexão.

2. Reinstale o Agente de Rede em dispositivos que deseja conectar ao gateway de conexão recém-adicionado.

Modificar a lista de pontos de distribuição para um grupo de administração

Você pode visualizar a lista de pontos de distribuição atribuídos a um grupo de administração específico e modificá-la adicionando ou removendo pontos de distribuição.

Para visualizar e modificar a lista de pontos de distribuição atribuídos a um grupo de administração:

1. No menu principal, vá para **Gerenciamento de ativos → Dispositivos gerenciados**.

2. Selecione um grupo de administração para o qual você deseja visualizar os pontos de distribuição atribuídos clicando no botão **Mostrar a hierarquia** na parte superior da página e, na janela que é exibida, clique no nome do grupo desejado.

   Isso ativa o item de menu **Pontos de distribuição**.

   O caminho para o grupo selecionado é exibido na parte superior da página. Caso seja necessário, neste caminho é possível clicar em um link com o nome do grupo de administração para ir até ele. Por padrão, o último link no caminho fica inativo.

3. No menu principal, vá para **Gerenciamento de ativos → Pontos de distribuição**.

4. Para adicionar novos pontos de distribuição para o grupo de administração, clique no botão **Atribuir**.

5. Para remover os pontos de distribuição atribuídos, selecione os dispositivos na lista e clique no botão **Desatribuir**.

Dependendo das suas modificações, os novos pontos de distribuição serão adicionados à lista ou os pontos de distribuição existentes serão removidos da lista.

Ativando um servidor push

No Kaspersky Security Center Linux, um ponto de distribuição pode funcionar como um servidor push para os dispositivos gerenciados por meio do protocolo móvel e para os dispositivos gerenciados pelo Agente de Rede. Por exemplo, um servidor push deve ser ativado se você quiser forçar a sincronização dos dispositivos KasperskyOS com o Servidor de Administração. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Se você tiver vários pontos de distribuição atribuídos ao mesmo grupo de administração, poderá ativar o servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

É possível querer usar pontos de distribuição como servidores push para garantir que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração. A conectividade contínua é necessária para algumas operações, como executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado ou criar um túnel. Caso um ponto de distribuição seja usado como servidor push, não será necessário usar a opção **Não desconectar do Servidor de Administração** nos dispositivos gerenciados nem enviar pacotes para a porta UDP do Agente de Rede.

Um servidor push suporta a carga de até 50.000 conexões simultâneas.

Para ativar o servidor push em um ponto de distribuição:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Clique no nome do ponto de distribuição no qual deseja ativar o servidor push.

   A janela Propriedades do ponto de distribuição é aberta.

4. Na seção **Geral**, selecione a opção **Ativado**.

5. No campo **Porta do servidor push**, digite o número da porta. Você pode especificar o número de qualquer porta livre.

6. No campo **Endereço para hosts remotos**, especifique o endereço IP ou o nome do dispositivo do ponto de distribuição.

7. Clique em **OK**.

O servidor push é ativado no ponto de distribuição selecionado.

Aumento do limite de descritores de arquivo para o serviço klnagent

Caso o escopo de um ponto de distribuição baseado em Linux inclua muitos dispositivos, o limite padrão de arquivos que podem ser abertos (descritores de arquivo) pode não ser suficiente. Para evitar isso, é possível aumentar o limite de descritores de arquivo para o serviço klnagent.

Para aumentar o limite de descritores de arquivo para o serviço klnagent:

1. No dispositivo baseado em Linux que atua como um ponto de distribuição, execute o seguinte comando:

   `systemctl edit klnagent64.service`

2. Especifique os limites rígidos e flexíveis dos descritores de arquivo no parâmetro `LimitNOFILE` da seção `[Service]`:

   `LimitNOFILE=<limite flexível de recurso>:<limite rígido de recurso>`

   Por exemplo, `LimitNOFILE=32768:131072`. Observe que o limite flexível dos descritores de arquivo deve ser menor ou igual ao limite absoluto.

3. Execute o seguinte comando para garantir que os parâmetros sejam especificados corretamente:

   `systemd-analyze verify klnagent64.service`

   Caso os parâmetros sejam especificados incorretamente, esse comando poderá gerar um dos seguintes erros:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Caso ocorra esse erro, os símbolos na linha `LimitNOFILE` foram especificados incorretamente. É necessário verificar e corrigir a linha inserida.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Se esse erro ocorrer, o limite flexível dos descritores de arquivo inseridos será maior que o limite absoluto. É necessário verificar a linha inserida e garantir que o limite flexível dos descritores de arquivo seja menor ou igual ao limite absoluto.

4. Execute o seguinte comando para recarregar o processo do systemd:

   `systemctl daemon-reload`

5. Execute o seguinte comando para reiniciar o serviço do Agente de Rede:

   `systemctl restart klnagent`

6. Execute o seguinte comando para garantir que os parâmetros especificados sejam aplicados corretamente:

   `less /proc/<ID do processo nagent>/limits`

   em que o parâmetro `<ID do processo nagent>` é o identificador do processo do Agente de Rede. É possível executar o seguinte comando para obter o identificador:

   `ps -ax | grep klnagent`

Para o ponto de distribuição baseado em Linux, o limite de arquivos que podem ser abertos é aumentado.

Sobre os status do dispositivo

O Kaspersky Security Center Linux atribui um status a cada dispositivo gerenciado. O status específico depende se as condições definidas pelo usuário são atendidas. Em alguns casos, ao atribuir um status a um dispositivo, o Kaspersky Security Center Linux leva em consideração o sinalizador de visibilidade do dispositivo na rede (consulte a tabela abaixo). Por exemplo, se um dispositivo gerenciado recebeu o status *Crítico* porque a condição *Os bancos de dados estão desatualizados* foi atendida e, posteriormente, o sinalizador de visibilidade foi definido para esse dispositivo, ele passa a receber o status *OK*. Se o Kaspersky Security Center Linux não encontrar um dispositivo na rede dentro de duas horas, o sinalizador de visibilidade do dispositivo será definido como *Não visível*.

Os status são os seguintes:

- *Crítico* ou *Crítico/Visível*
- *Advertência* ou *Advertência/Visível*
- *OK* ou *OK/Visível*

A tabela abaixo lista as condições padrão que devem ser atendidas para atribuir o status *Crítico* ou *Advertência* a um dispositivo, com todos os valores possíveis.

Condições para atribuir um status a um dispositivo

Condição	Descrição da condição	Valores disponíveis
O aplicativo de segurança não está instalado	O Agente de Rede é instalado no dispositivo, mas um aplicativo de segurança não é instalado.	• O botão de alternar é ativado. • O botão de alternar é desativado.
Excesso de vírus detectados	Alguns vírus foram encontrados no dispositivo por uma tarefa de detecção de vírus, por exemplo, a tarefa de verificação de malware, e o número de vírus encontrados excede o valor especificado.	Mais de 0.
O nível da proteção em tempo real é diferente do nível definido pelo administrador	O dispositivo está visível na rede, mas o nível de proteção em tempo real difere do nível definido (na condição) pelo administrador para o status do dispositivo.	• Parado. • Suspenso. • Executando.
A verificação de malware não é executada há muito tempo	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas nem a tarefa de *verificação de malware* nem a verificação local foram executadas dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 7 dias ou antes.	Mais de 1 dia.
Os bancos de dados estão desatualizados	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas os bancos de dados antivírus não foram atualizados neste dispositivo dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 1 dia ou antes.	Mais de 1 dia.
Não conectado há muito tempo	O Agente de Rede está instalado no dispositivo, mas o dispositivo não se conectou a um Servidor de Administração dentro do intervalo de tempo especificado, porque o dispositivo estava desativado.	Mais de 1 dia.
Foram detectadas ameaças ativas	O número de objetos não processados na pasta **Ameaças ativas** excede o valor especificado.	Mais de 0 itens.

Condição	Descrição da condição	Valores disponíveis
Tempo desde o reinício necessário	O dispositivo está visível na rede, mas um aplicativo está aguardando uma reinicialização por mais tempo do que o intervalo de tempo especificado.	Mais de 0 minuto.
Motivo do reinício	O dispositivo está visível na rede, mas um aplicativo requer a reinicialização do dispositivo por um dos motivos selecionados.	• Motivo desconhecido • O aplicativo não funcionará até a reinicialização • É necessário reiniciar para concluir a atualização; o aplicativo está em execução • É necessário reiniciar para iniciar a atualização • É necessário reiniciar para concluir a verificação ou a desinfecção • A reinicialização é necessária para concluir a instalação/desinstalação remota • Concluindo a criptografia de dados no disco
Aplicativos incompatíveis estão instalados	O dispositivo está visível na rede, mas o inventário de software executado pelo Agente de Rede detectou aplicativos incompatíveis instalados no dispositivo.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Foram detectadas vulnerabilidades de software	O dispositivo está visível na rede, e o Agente de Rede está instalado no dispositivo, mas a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* detectou vulnerabilidades com o nível de gravidade especificado nos aplicativos instalados no dispositivo.	• Crítico. • Alto. • Médio. • Ignorar se a vulnerabilidade não puder ser corrigida. • Ignorar se uma atualização for atribuída para instalação.
A licença expirou	O dispositivo está visível na rede, mas a licença expirou.	• O botão de alternar é desativado. • O botão de alternar é ativado.
A licença expira em breve	O dispositivo está visível na rede, mas a licença expirará no dispositivo em tempo menor que o número especificado de dias.	Mais de 0 dias.

Condição	Descrição da condição	Valores disponíveis
A verificação de atualizações do Windows Update não é executada há muito tempo	O dispositivo está visível na rede, mas a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* não foi executada no intervalo de tempo especificado.	Mais de 1 dia.
Status de criptografia inválido	O Agente de Rede está instalado no dispositivo, mas o resultado da criptografia de dispositivo é igual ao valor especificado.	• Não está em conformidade com a política devido à recusa do usuário (somente para dispositivos externos). • Não está em conformidade com a política devido a um erro. • Reiniciar é necessário ao aplicar a política. • Nenhuma política de criptografia está especificada. • Sem suporte. • Ao aplicar a política.
As configurações do dispositivo móvel não estão em conformidade com a política	As configurações do dispositivo móvel são diferentes das especificadas na política do Kaspersky Endpoint Security for Android durante a verificação das regras de conformidade.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Foram detectados problemas de segurança não processados	Alguns problemas de segurança não processados foram encontrados no dispositivo. Os problemas de segurança podem ser criados automaticamente pelos aplicativos da Kaspersky gerenciados e instalados no dispositivo cliente ou manualmente pelo administrador.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Status do dispositivo definido pelo aplicativo	O status do dispositivo é definido pelo aplicativo gerenciado. Os dispositivos gerenciados podem ter um status definido por aplicativos gerenciados, independentemente das configurações do Kaspersky Security Center Linux. Depois que esse status retorna um dos status definidos pelo Kaspersky Security Center Linux, o Servidor Administração atribui ao dispositivo gerenciado o status mais crítico entre aqueles retornados pelo aplicativo gerenciado e o atribuído pelo próprio Servidor de Administração. Os status definidos pelos aplicativos gerenciados têm suas descrições transferidas por esses próprios aplicativos. Você pode visualizar essas descrições na lista de dispositivos gerenciados, na coluna **Descrição de status**.	• O botão de alternar é desativado. • O botão de alternar é ativado.
O dispositivo está com espaço em disco insuficiente	O espaço livre em disco no dispositivo é menor do que o valor especificado ou o dispositivo não pôde ser sincronizado com o Servidor de Administração. O status *Crítico* ou *Advertência* é alterado para o status *OK* quando o dispositivo é sincronizado com sucesso com o Servidor de Administração, e o espaço livre no dispositivo é maior que ou igual ao valor especificado.	Mais de 0 MB.
O dispositivo está sem gerenciamento	Durante a descoberta de dispositivos, o dispositivo foi reconhecido como visível na rede, mas houve falha em mais de três tentativas de sincronizar com o Servidor de Administração.	• O botão de alternar é desativado. • O botão de alternar é ativado.
A proteção está desativada	O dispositivo é visível na rede, mas o aplicativo de segurança no dispositivo foi desativado por um tempo mais longo do que o intervalo de tempo especificado. Nesse caso, o estado do aplicativo de segurança é *interrompido* ou *com falha* e diferente de: *iniciando*, *em execução* ou *suspenso*.	Mais de 0 minuto.
O aplicativo de segurança não está em execução	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas não está em execução.	• O botão de alternar é desativado. • O botão de alternar é ativado.

O Kaspersky Security Center Linux permite definir a troca automática do status de um dispositivo em um grupo de administração quando as condições especificadas forem atendida. Quando as condições especificadas forem atendidas, ao dispositivo cliente é atribuído um dos seguintes status: *Crítico* ou *Aviso*. Quando as condições especificadas não são atendidas, o dispositivo cliente recebe o status *OK*.

Diferentes status poderão corresponder a diferentes valores de uma condição. Por exemplo, por padrão, se a condição **Os bancos de dados estão desatualizados** possuir o valor **Mais de 3 dias**, o dispositivo cliente receberá o status *Advertência*. Se o valor for **Mais de 7 dias**, será atribuído o status *Crítico*.

Se você atualizar o Kaspersky Security Center Linux a partir da versão anterior, os valores da condição **Os bancos de dados estão desatualizados** para a atribuição do status *Crítico* ou *Advertência* não mudam.

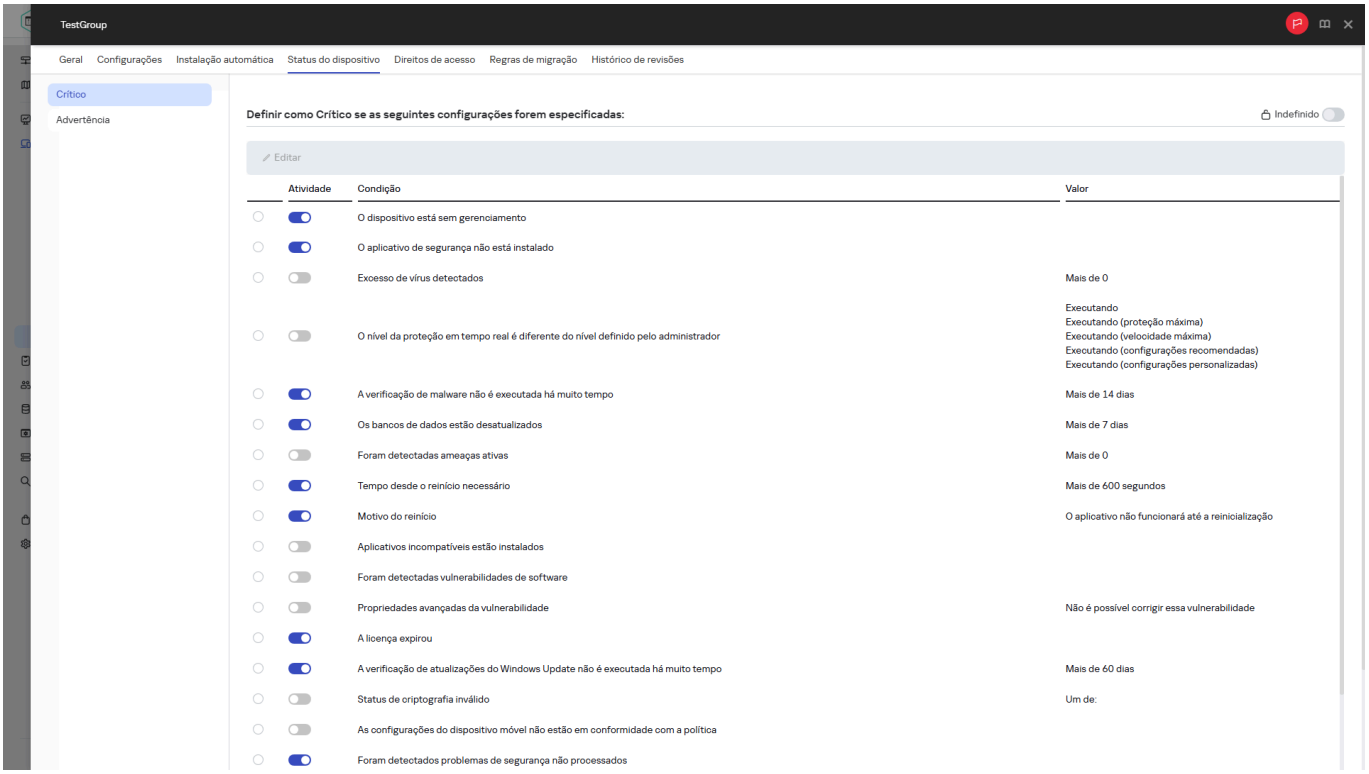
Configurar a alternância dos status do dispositivo

Você pode alterar as condições para atribuir o status *Crítico* ou *Advertência* para um dispositivo.

Para ativar a alteração do status do dispositivo para Crítico:

1. No menu principal, vá para **Gerenciamento de ativos** → **Hierarquia de grupos**.
2. Vá para as propriedades do grupo de administração para o qual você deseja alterar os status do dispositivo de uma das seguintes formas:
   - Clique no nome do grupo de administração.
   - Clique no botão **Mostrar a hierarquia** na parte superior da página. No painel de navegação exibido, passe o cursor do mouse sobre o nome do grupo desejado e clique no ícone de configurações (⚙).

   A janela Propriedades do grupo de administração é aberta.
3. Na janela de propriedades, selecione a guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Crítico**.
5. No painel direito, na seção **Definir como Crítico se as seguintes configurações forem especificadas**, ative a condição para alterar o status de um dispositivo para *Crítico*.



No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.

7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.
9. Clique em **OK**.
10. Clique em **Salvar** para salvar as alterações.

Quando condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Crítico*.

Para ativar a alteração do status do dispositivo para Advertência:

1. No menu principal, vá para **Gerenciamento de ativos → Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Advertência**.
5. No painel direito, na seção **Definir como Advertência se as seguintes configurações forem especificadas**, ative a condição para alterar o status de um dispositivo para *Advertência*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.
6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.
9. Clique em **OK**.
10. Clique em **Salvar** para salvar as alterações.

Quando as condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Advertência*.

Seleções de dispositivos

As *Seleções de dispositivos* são uma ferramenta para filtrar dispositivos de acordo com as condições específicas. É possível usar as seleções de dispositivos para gerenciar vários dispositivos: por exemplo, para visualizar um relatório apenas sobre esses dispositivos ou mover todos esses dispositivos para outro grupo.

O Kaspersky Security Center Linux fornece uma ampla variedade de *seleções predefinidas* (por exemplo, **Dispositivos com status Crítico**, **A proteção está desativada**, **Foram detectadas ameaças ativas**). As seleções predefinidas não podem ser excluídas. Também é possível criar e configurar *seleções adicionais definidas pelo usuário*.

Em seleções definidas pelos usuários, você pode definir o escopo da pesquisa e selecionar todos os dispositivos, dispositivos gerenciados ou dispositivos não atribuídos. Os parâmetros de pesquisa são especificados nas condições. Na seleção de dispositivos, você pode criar várias condições com parâmetros de pesquisa diferentes. Por exemplo, você pode criar duas condições e especificar conjuntos de IPs diferentes em cada uma delas. Se várias condições forem especificadas, uma seleção exibirá os dispositivos que atendem a alguma das condições. Por outro lado, os parâmetros de pesquisa dentro de uma condição são sobrepostos. Se um conjunto de IPs e o nome de um aplicativo instalado forem especificados em uma condição, apenas esses dispositivos serão exibidos onde o aplicativo está instalado e o endereço IP pertence ao conjunto especificado.

Visualização da lista de dispositivos a partir de uma seleção de dispositivos

O Kaspersky Security Center Linux permite exibir a lista de dispositivos a partir de uma seleção de dispositivos.

Para visualizar a lista de dispositivos na seleção de dispositivos:

1. No menu principal, vá para a seção **Gerenciamento de ativos** → **Seleções de dispositivos** ou **Descoberta e implementação** → **Seleções de dispositivos**.
2. Na lista de seleção, clique no nome da seleção de dispositivos.

   A página exibe uma tabela com informações sobre os dispositivos incluídos na seleção de dispositivos.
3. É possível agrupar e filtrar os dados da tabela do dispositivo da seguinte forma:

   - Clique no ícone de configurações (⚙) e, em seguida, selecione as colunas a serem exibidas na tabela.
   - Clique no ícone de filtro (▽), especifique e aplique o critério de filtro no menu resultante.

     A tabela filtrada de dispositivos é exibida.

Você também pode executar tarefas para seleções de dispositivos. Para fazer isso, selecione um ou mais dispositivos, clique no botão **Executar tarefa** e selecione **Criar tarefa** para criar uma tarefa a ser aplicada a esses dispositivos ou **Aplicar tarefa existente**.

Para mover os dispositivos selecionados da seleção de dispositivos para outro grupo de administração, clique no botão **Migrar para grupo** e, em seguida, selecione o grupo de administração de destino.

Criar uma seleção de dispositivos

Para criar uma seleção de dispositivos:

1. No menu principal, vá para **Gerenciamento de ativos** → **Seleções de dispositivos**.

   Uma página com uma lista de seleções de dispositivos é exibida.
2. Clique em **Adicionar**.

   A janela **Configurações de seleção de dispositivos** se abre.
3. Digite o nome da nova seleção.

4. Especifique o grupo que contém os dispositivos a serem incluídos na seleção de dispositivos:

   - **Localizar qualquer dispositivo** – Procura dispositivos que atendam aos critérios de seleção e incluídos no grupo **Dispositivos gerenciados** ou **Dispositivos não atribuídos**.
   - **Localizar dispositivos gerenciados** – Procura dispositivos que atendam aos critérios de seleção e incluídos no grupo **Dispositivos gerenciados**.
   - **Localizar dispositivos não atribuídos** – Procura dispositivos que atendam aos critérios de seleção e incluídos no grupo **Dispositivos não atribuídos**.

   É possível ativar a caixa de seleção **Incluir dados dos Servidores de Administração secundários** para ativar a pesquisa de dispositivos que atendam aos critérios de seleção e gerenciados por Servidores de Administração secundários.

5. Clique em **Adicionar**.

6. Na janela aberta, especifique as condições que devem ser atendidas para a inclusão de dispositivos nesta seleção e depois clique no botão **Salvar**.

7. Clique no botão **Salvar**.

A seleção de dispositivos é criada e adicionada à lista de seleções de dispositivos.

Configurar uma seleção de dispositivos

Para configurar uma seleção de dispositivo:

1. No menu principal, vá para **Gerenciamento de ativos → Seleções de dispositivos**.

   Uma página com uma lista de seleções de dispositivos é exibida.

2. Escolha a seleção de dispositivos definida pelo usuário relevante e clique no botão **Propriedades**.

   A janela **Configurações de seleção de dispositivos** se abre.

3. Na guia **Geral**, clique no link **Nova condição**.

4. Especifique as condições que devem ser atendidas para a inclusão de dispositivos nesta seleção.

5. Clique no botão **Salvar**.

As configurações são aplicadas e salvas.

Abaixo estão as descrições das condições para atribuir dispositivos a uma seleção. As condições são combinadas através da utilização do operador lógico OR: a seleção conterá dispositivos que estejam em conformidade com pelo menos uma das condições listadas.

Geral

Na seção **Geral**, você pode mudar o nome de uma condição de seleção e especificar se essa condição deve ser invertida:

Inverter condição de seleção

Por padrão, esta opção está desativada.

Se esta opção estiver ativada, a condição de seleção especificada será invertida. A seleção incluirá todos os dispositivos que não atendem a condição.

O exemplo a seguir mostra a lógica do trabalho de inversão:

- **Condição**: no seu dispositivo, há um sistema operacional com o tipo Linux e o número de compilação 00.0.000.
- **Condição invertida**: no seu dispositivo, há um sistema operacional com NOT (o tipo Linux e o número de compilação 00.0.000), que é equivalente ao seguinte:

  Existe um sistema operacional com o tipo NOT Linux OU número de compilação NOT 00.0.000.

Assim, a seleção incluirá os dispositivos com um sistema operacional, por exemplo, do tipo Windows e o número de compilação 00.0.000, ou o tipo Linux e qualquer número de compilação diferente de 00.0.000.

Infraestrutura de rede

Na subseção **Rede**, é possível especificar o critério que será usado para incluir dispositivos na seleção de acordo com seus dados na rede:

Nome do dispositivo

Nome da rede Windows (nome NetBIOS) do dispositivo ou o endereço IPv4 ou IPv6.

Domínio

Exibe todos os dispositivos incluídos no grupo de trabalho especificado.

Grupo de administração

Exibe os dispositivos incluídos no grupo de administração especificado.

Descrição

Texto na janela Propriedades do dispositivo: no campo **Descrição** da seção **Geral**.

Para descrever texto no campo **Descrição**, é possível usar os seguintes caracteres:

- Em uma palavra:
  - *****. Substitui qualquer sequência por qualquer número de caracteres.

    Exemplo:

    Para descrever as palavras **Servidor** ou **Servidores**, é possível inserir **Servidor***.
  - **?.** Substitui qualquer caractere único.

    Exemplo:

    Para descrever frases como **SUSE Linux Enterprise Server 12** ou **SUSE Linux Enterprise Server 15**, é possível inserir **SUSE Linux Enterprise Server 1?**.

    O asterisco (*****) ou o ponto de interrogação (**?**) não pode ser usado como o primeiro caractere na consulta.

- Para encontrar várias palavras:
  - Espaço. Exibe todos os dispositivos cujas descrições contêm qualquer uma das palavras listadas.

  Exemplo:

  Para localizar uma frase que contenha as palavras **Secundário** ou **Virtual**, você pode incluir a linha **Secundário Virtual** na consulta.

  - **+**. Quando o sinal de mais antecede uma palavra, todos os resultados de pesquisa contêm essa palavra.

  Exemplo:

  Para encontrar uma frase que contenha as palavras **Secundário** e **Virtual**, insira **+Secundário+Virtual** na consulta.

  - **-**. Quando um sinal de menos antecede uma palavra, nenhum dos resultados de pesquisa contém essa palavra.

  Exemplo:

  Para encontrar uma frase que contenha **Secundário**, mas que não contenha **Virtual**, insira **+Secundário-Virtual** na consulta.

  - **"<algum texto>"**. O texto dentro de aspas deve estar no texto.

  Exemplo:

  Para encontrar uma expressão que contenha a combinação de palavras **Servidor Secundário**, você pode inserir **"Servidor Secundário"** na consulta.

Intervalo de IPs

Se esta opção estiver ativada, você poderá inserir os endereços IP inicial e final do conjunto de IPs no qual os dispositivos relevantes devem ser incluídos.

Por padrão, esta opção está desativada.

Gerenciado por outro Servidor de Administração

Selecione um dos seguintes valores:

- **Sim**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente gerenciados por outros Servidores de Administração. Esses servidores são diferentes do servidor no qual a regra de migração de dispositivo é configurada.
- **Não**. A regra de movimentação de dispositivos aplica-se apenas a dispositivos clientes gerenciados pelo Servidor de Administração atual.
- **Nenhum valor está selecionado**. A condição não se aplica.

Na subseção **Controlador de domínio**, é possível configurar critérios para incluir dispositivos em uma seleção com base na associação ao domínio:

O dispositivo está é um domínio da unidade organizacional

Caso esta opção esteja ativada, a seleção inclui os dispositivos do domínio da unidade organizacional especificado no campo de entrada.

Por padrão, esta opção está desativada.

Este dispositivo é membro do grupo de segurança do domínio

Caso esta opção esteja ativada, a seleção incluirá os dispositivos do grupo de segurança do domínio especificado no campo de entrada.

Por padrão, esta opção está desativada.

Na subseção **Atividade de rede**, é possível especificar o critério que será usado para incluir dispositivos na seleção de acordo com a sua atividade de rede:

Atua como ponto de distribuição

Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

- **Sim**. A seleção inclui dispositivos que agem como pontos de distribuição.
- **Não**. Dispositivos que atuam como pontos de distribuição não serão incluídos na seleção.
- **Nenhum valor está selecionado**. O critério não será aplicado.

Não desconectar do Servidor de Administração

Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

- **Ativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** está selecionada.
- **Desativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** não está selecionada.
- **Nenhum valor está selecionado**. O critério não será aplicado.

Perfil de conexão trocado

Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

- **Sim**. A seleção incluirá os dispositivos que se conectaram ao Servidor de Administração após o perfil de conexão ter sido alternado.
- **Não**. A seleção não incluirá os dispositivos que se conectaram com o Servidor de Administração após o perfil de conexão ter sido alternado.
- **Nenhum valor está selecionado**. O critério não será aplicado.

Última conexão com o Servidor de Administração

Você pode usar essa caixa de seleção para configurar um critério para pesquisar por dispositivos pela hora da sua última conexão com o Servidor de Administração.

Se essa caixa de seleção estiver selecionada, é possível, nos campos de entrada especificar o intervalo de tempo (data e hora) durante o qual a última conexão entre o Agente de Rede instalado no dispositivo cliente e o Servidor de Administração foi estabelecida. A seleção inclui dispositivos que estejam no intervalo especificado.

Se essa caixa de seleção for desmarcada, o critério não é aplicado.

Por padrão, esta caixa de seleção está desmarcada.

Novos dispositivos detectados pela sondagem da rede

Procura por novos dispositivos que tenham sido detectados pela sondagem da rede ao longo dos poucos últimos dias.

Se esta opção estiver ativada, a seleção somente inclui novos dispositivos que tenham sido detectados pela descoberta de dispositivos durante a quantidade de dias especificada no campo **Período de detecção (dias)**.

Se esta opção estiver ativada, a seleção inclui todos os dispositivos que tenham sido detectados pela descoberta de dispositivos.

Por padrão, esta opção está desativada.

Dispositivo visível

Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

- **Sim**. O aplicativo é incluído na seleção de dispositivos atualmente visíveis na rede.
- **Não**. O aplicativo é incluído na seleção de dispositivos atualmente invisíveis na rede.
- **Nenhum valor está selecionado**. O critério não será aplicado.

Status do dispositivo

Na seção **Status do dispositivo gerenciado**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com a descrição do status de dispositivos de um aplicativo gerenciado:

Status do dispositivo

Lista suspensa na qual você pode selecionar um dos status do dispositivo: *OK*, *Crítico* ou *Advertência*.

Status da proteção em tempo real

Lista suspensa na qual você pode selecionar o status da proteção em tempo real. Os dispositivos com um status da proteção em tempo real especificado serão incluídos na seleção.

Descrição do status do dispositivo

Neste campo, você poderá selecionar caixas de seleção próximas das condições que, se atendidas, atribuem um dos seguintes status ao dispositivo: *OK, Crítico* ou *Advertência*.

Na subseção **Status dos componentes em aplicativos gerenciados**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o status dos componentes em aplicativos gerenciados:

Status da prevenção de vazamento de dados

Pesquise dispositivos pelo status da Prevenção de vazamento de dados (*Desconhecido, Parado, Iniciando, Pausado, Executando, Falhou*).

Status da proteção dos servidores de colaboração

Procure dispositivos pelo status da proteção de colaboração do servidor (*Desconhecido*, *Parado*, *Iniciando, Pausado*, *Executando*, *Falhou*).

Status da proteção antivírus dos servidores de correio

Procure dispositivos pelo status da proteção do servidor de e-mail (*Desconhecido, Parado, Iniciando, Pausado, Executando, Falhou*).

Status do Endpoint Sensor

Procure dispositivos pelo status do componente Endpoint Sensor (*Desconhecido, Parado, Iniciando, Pausado, Executando, Falhou*).

Na subseção **Problemas que afetam o status em aplicativos gerenciados**, é possível especificar os critérios que serão usados para incluir os dispositivos na seleção de acordo com a lista de possíveis problemas detectados por um aplicativo gerenciado. Se pelo menos um problema que você selecionar existir em um dispositivo, o dispositivo estará incluído na seleção. Quando você seleciona um problema listado para vários aplicativos, você tem a opção de selecionar esse problema em todas das listas automaticamente.

Você pode selecionar as caixas de seleção para descrições de status do aplicativo gerenciado; ao receber este status, os dispositivos serão incluídos na seleção. Quando você seleciona um status listado para vários aplicativos, você tem a opção de selecionar esse status em todas das listas automaticamente.

Detalhes do sistema

Na seção **SO**, você pode especificar o critério que será usado para incluir dispositivos na seleção de acordo com o seu tipo de sistema operacional.

Tipo de plataforma

Se esta caixa de seleção estiver marcada, você pode selecionar um sistema operacional da lista. Os dispositivos com o sistema operacional especificado instalado são incluídos nos resultados de pesquisa.

Versão do pacote de serviço do SO

Neste campo, você pode especificar a versão do pacote do sistema operacional (no formato *X.Y*), o que determinará como a regra de migração será aplicada ao dispositivo. Por padrão, nenhum valor de versão é especificado.

Arquitetura do SO

Na lista suspensa, você poderá selecionar a arquitetura para o sistema operacional, que determinará como a regra para mover será aplicada ao dispositivo (**Desconhecido**, **x86**, **AMD64** ou **IA64**). Por padrão, nenhuma opção é selecionada na lista para que a arquitetura do sistema operacional não fique definida.

Compilação do SO

> Esta configuração é aplicável somente aos sistemas operacionais Windows.

O número da compilação do sistema operacional. É possível especificar se o sistema operacional selecionado ter um número de versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de compilação, exceto o especificado.

Número da versão do SO

> Esta configuração é aplicável somente aos sistemas operacionais Windows.

O identificador (ID) da versão do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um ID da versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de ID da versão, exceto o especificado.

Na seção **Máquinas virtuais**, você pode definir o critério para incluir os dispositivos na seleção se estes são máquinas virtuais ou parte da Virtual Desktop Infrastructure (VDI):

Esta é uma máquina virtual

Na lista suspensa, você pode selecionar as seguintes opções:

- **Indefinido**.
- **Não**. Localizar dispositivos que não sejam máquinas virtuais.
- **Sim**. Localizar dispositivos que são máquinas virtuais.

Tipo de máquina virtual

Na lista suspensa, você pode selecionar o fabricante da máquina virtual.

Essa lista suspensa estará disponível se o valor **Sim** ou **Irrelevante** estiver selecionado na lista suspensa **Esta é uma máquina virtual**.

Parte da Virtual Desktop Infrastructure

Na lista suspensa, você pode selecionar as seguintes opções:

- **Indefinido**.
- **Não**. Localizar dispositivos que não fazem parte da Virtual Desktop Infrastructure.
- **Sim**. Localizar dispositivos que fazem parte da Virtual Desktop Infrastructure (VDI).

Na subseção **Registro de hardware**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o hardware instalado:

Verifique e confirme se o utilitário lshw está instalado nos dispositivos Linux a partir dos quais deseja buscar detalhes de hardware. Os detalhes de hardware obtidos de máquinas virtuais podem estar incompletos, dependendo do hipervisor usado.

Dispositivo

Na lista suspensa, você pode selecionar um tipo de unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

O campo suporta a pesquisa de texto completo.

Fornecedor

Na lista suspensa, você pode selecionar o nome do fabricante da unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

O campo suporta a pesquisa de texto completo.

Nome do dispositivo

O dispositivo com o nome especificado será incluído na seleção.

Descrição

Descrição de um dispositivo ou de uma unidade de hardware. Os dispositivos com a descrição especificada neste campo serão incluídos na seleção.

A descrição de um dispositivo em qualquer formado pode ser inserida na janela de propriedades desse dispositivo. O campo suporta a pesquisa de texto completo.

Fornecedor do dispositivo

Nome do fabricante do dispositivo. Os dispositivos produzidos pelo fabricante especificado neste campo estão incluídos na seleção.

Você pode inserir o nome do fabricante na janela de propriedades de um dispositivo.

Número de série

Todas as unidades hardware com número de série especificado nesse campo serão incluídas na seleção.

Número de inventário

Equipamentos com o número de inventário especificado neste campo serão incluídos na seleção.

Usuário

Todas as unidades hardware do usuário especificado nesse campo serão incluídas na seleção.

Localização

A localização do dispositivo ou unidade de hardware (por exemplo, na sede ou no escritório de uma filial). Computadores ou outros dispositivos que são implementados na localização especificada nesse campo serão incluídos na seleção.

Você pode descrever a localização de um dispositivo em qualquer formato na janela de propriedades desse dispositivo.

Frequência do clock da CPU em MHz, de

A taxa de clock mínima de uma CPU. Os dispositivos com uma CPU que corresponda ao intervalo de taxa de clock especificado nos campos de entrada (inclusive) serão incluídos na seleção.

Frequência do clock da CPU em MHz, para

A taxa de clock máxima de uma CPU. Os dispositivos com uma CPU que corresponda ao intervalo de taxa de clock especificado nos campos de entrada (inclusive) serão incluídos na seleção.

Número de núcleos da CPU virtual, de

O número mínimo de núcleos de CPU virtuais. Os dispositivos com uma CPU que corresponda ao intervalo do número de núcleos virtuais especificado nos campos de entrada (inclusive) serão incluídos na seleção.

Número de núcleos da CPU virtual, até

O número máximo de núcleos de CPU virtuais. Os dispositivos com uma CPU que corresponda ao intervalo do número de núcleos virtuais especificado nos campos de entrada (inclusive) serão incluídos na seleção.

Volume do disco rígido, em GB, de

O volume mínimo do disco rígido no dispositivo. Os dispositivos com um disco rígido que corresponda a faixa especificada nos campos de entrada (inclusive) serão incluídos na seleção.

Volume do disco rígido, em GB, para

O volume máximo do disco rígido no dispositivo. Os dispositivos com um disco rígido que corresponda a faixa especificada nos campos de entrada (inclusive) serão incluídos na seleção.

Tamanho da RAM em MB, de

O tamanho mínimo da RAM do dispositivo. Os dispositivos com RAM que corresponda ao intervalo de valores nos campos de entrada (inclusive) são incluídos na seleção.

Tamanho da RAM em MB, para

O tamanho máximo da RAM do dispositivo. Os dispositivos com RAM que corresponda ao intervalo de valores nos campos de entrada (inclusive) são incluídos na seleção.

Detalhes de software de terceiros

Na subseção **Registro de aplicativos**, é possível definir o critério para pesquisar dispositivos de acordo com os aplicativos neles instalados:

Nome do aplicativo

Lista suspensa na qual é possível selecionar um aplicativo. Os dispositivo nos quais o aplicativos especificado estiver instalado, serão incluídos na seleção.

Versão do aplicativo

Campo de entrada onde é possível especificar a versão do aplicativo selecionado.

Fornecedor

Lista suspensa na qual é possível selecionar o fabricante de um aplicativo instalado no dispositivo.

Status do aplicativo

Uma lista suspensa na qual é possível selecionar o status de um aplicativo (*Instalado*, *Não instalado*). Os dispositivos nos quais o aplicativo especificado está ou não instalado, dependendo do status selecionado, serão incluídos na seleção.

Localizar por atualização

Se esta opção estiver ativada, a pesquisa será executada usando os dados das atualizações para os aplicativos instalados nos dispositivos relevantes. Após selecionar a caixa de seleção, os campos **Nome do aplicativo**, **Versão do aplicativo** e **Status do aplicativo** mudam para **Nome da atualização**, **Versão da atualização** e **Status** respectivamente.

Por padrão, esta opção está desativada.

Nome do aplicativo de segurança incompatível

Lista suspensa na qual é possível selecionar aplicativos de segurança de terceiros. Durante a pesquisa, os dispositivos nos quais está instalado o aplicativo especificado, serão incluídos na seleção.

Tag do aplicativo

Na lista suspensa, você pode selecionar a tag do aplicativo. Todos os dispositivos que instalaram aplicativos com a tag selecionada na descrição são incluídos na seleção de dispositivo.

Aplicar aos dispositivos sem tags especificadas

Se esta opção estiver ativada, o perfil da política inclui dispositivos com descrições que não contêm nenhuma das tags selecionadas.

Se esta opção estiver desativada, o critério não é aplicado.

Por padrão, esta opção está desativada.

Na subseção **Vulnerabilidades e atualizações**, é possível especificar o critério que será usado para incluir dispositivos na seleção de acordo com a fonte do Windows Update:

WUA foi mudado para o Servidor de Administração

Você pode selecionar uma das seguintes opções de pesquisa da lista suspensa:

- **Sim**. Se essa opção estiver selecionada, os resultados da pesquisa incluirão os dispositivos que recebem atualizações através do Windows Update do Servidor de Administração.
- **Não**. Caso essa opção esteja selecionada, os resultados incluirão os dispositivos que recebem atualizações pelo Windows Update de outras fontes.

Detalhes de aplicativos da Kaspersky

Na subseção **Aplicativos da Kaspersky**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o aplicativo gerenciado selecionado:

Nome do aplicativo

Na lista suspensa, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome de um aplicativo da Kaspersky.

A lista somente fornece os nomes de aplicativos com plugins de gerenciamento instalados na estação de trabalho do administrador.

Se nenhum aplicativo for selecionado, o critério não será aplicado.

Versão do aplicativo

No campo de entrada, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo número da versão de um aplicativo da Kaspersky.

Se nenhum número de versão for especificado, o critério não será aplicado.

Nome da atualização crítica

No campo de entrada de dados, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome do aplicativo ou pelo número do pacote de atualização.

Se o campo for deixado em branco, o critério não será aplicado.

Status do aplicativo

Uma lista suspensa na qual é possível selecionar o status de um aplicativo (*Instalado*, *Não instalado*). Os dispositivos nos quais o aplicativo especificado está ou não instalado, dependendo do status selecionado, serão incluídos na seleção.

Selecione o período da última atualização de módulos

Você pode usar esta opção para definir um critério para pesquisar dispositivos pela hora da última atualização dos módulos de aplicativos instalados nesses dispositivos.

Se essa caixa de seleção estiver selecionada, nos campos de entrada você poderá especificar o intervalo de tempo (data e hora) durante o qual a última atualização de módulos de aplicativos instalados nesses dispositivos foi executada.

Se essa caixa de seleção for desmarcada, o critério não é aplicado.

Por padrão, esta caixa de seleção está desmarcada.

O dispositivo é gerenciado pelo Servidor de Administração

Na lista suspensa, você poderá incluir nos dispositivos selecionados gerenciados através do Kaspersky Security Center Linux:

- **Sim**. O aplicativo é incluído na seleção de dispositivos gerenciados através do Kaspersky Security Center Linux.
- **Não**. A seleção inclui dispositivos que não são gerenciados pelo Kaspersky Security Center.
- **Nenhum valor está selecionado**. O critério não será aplicado.

Aplicativo de segurança instalado

Na lista suspensa, você poderá incluir na seleção todos os dispositivos com o aplicativo de segurança instalado:

- **Sim**. O aplicativo é incluído na seleção de dispositivos com o aplicativo de segurança instalado.
- **Não**. O aplicativo inclui na seleção todos os dispositivos sem nenhum aplicativo de segurança instalado.
- **Nenhum valor está selecionado**. O critério não será aplicado.

Na subseção **Proteção antivírus**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o status da proteção:

Bancos de dados lançados

Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes por data de lançamento de versão do banco de dados antivírus. Nos campos de entrada, você pode definir o intervalo de tempo com base no qual a pesquisa é realizada.

Por padrão, esta opção está desativada.

Contagem de registros do banco de dados

Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pelo número de registros de banco de dados. Nos campos de entrada, você pode definir os valores do limite inferior e superior para os registros do banco de dados antivírus.

Por padrão, esta opção está desativada.

Última verificação

Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pela hora da última verificação de malwares. No campo de entrada, você poderá especificar o período de tempo no qual a última verificação de malwares foi executada.

Por padrão, esta opção está desativada.

Ameaças detectadas

Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pelo número de vírus detectados. Nos campos de entrada, você pode definir os valores limite inferiores e superiores pelo número de vírus encontrados.

Por padrão, esta opção está desativada.

Na subseção **Criptografia**, é possível configurar o critério de inclusão de dispositivos em uma seleção de acordo com o algoritmo de criptografia selecionado:

Algoritmo de criptografia

Algoritmo de criptografia de bloco simétrico Advanced Encryption Standard (AES). Na lista suspensa, você pode selecionar o tamanho de chave de criptografia (de 56 bits, de 128 bits, de 192 bits ou de 256 bits).

Valores disponíveis: *AES56*, *AES128*, *AES192* e *AES256*.

A subseção **Componentes do aplicativo** contém a lista de componentes desses aplicativos que têm plug-ins de gerenciamento correspondentes instalados no Kaspersky Security Center Web Console.

Na subseção **Componentes do aplicativo**, é possível especificar o critério para a inclusão de dispositivos em uma seleção de acordo com o status e os números da versão dos componentes que fazem referência ao aplicativo que for selecionado:

Status

Pesquise dispositivos segundo o status do componente enviado por um aplicativo ao Servidor de Administração. É possível selecionar um dos seguintes status: *N/A, Interrompido*, *Pausado*, *Iniciando*, *Em execução, Com falha*, *Não instalado, Não compatível com a licença*. Se o componente selecionado do aplicativo instalado em um dispositivo gerenciado tiver o status especificado, o dispositivo será incluído na seleção de dispositivos.

Status enviados pelos aplicativos:

- *Interrompido* – O componente está desativado e não está funcionando no momento atual.
- *Pausado* – O componente está suspenso, por exemplo, depois que o usuário pausou a proteção no aplicativo gerenciado.
- *Iniciando* – O componente está atualmente em processo de inicialização.
- *Executando* – O componente está ativado e funcionando corretamente.
- *Falha* – Um erro ocorreu durante a operação do componente.
- *Não instalado* – O usuário não selecionou o componente para instalação ao configurar a instalação personalizada do aplicativo.
- *Não compatível com a licença* – A licença não cobre o componente selecionado.

Diferentemente de outros status, o status *N/A* não é enviado pelos aplicativos. Esta opção mostra que os aplicativos não têm nenhuma informação sobre o status do componente selecionado. Por exemplo, isto pode acontecer quando o componente selecionado não pertence a nenhum dos aplicativos instalados no dispositivo, ou quando o dispositivo está desligado.

Versão

Pesquise dispositivos segundo o número da versão do componente que você selecionar na lista. Você pode digitar um número de versão, por exemplo `3.4.1.0`, e especificar se o componente selecionado deve ter uma versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todas as versões, exceto a especificada.

Tags

Na seção **Tags**, você pode configurar o critério para pesquisar por dispositivos com base em palavras-chave (tags) adicionadas anteriormente às descrições dos dispositivos gerenciados:

Aplicar se pelo menos uma tag especificada corresponder

Se esta opção estiver ativada, o resultado da pesquisa mostrará os dispositivos com descrições que contêm ao menos uma das tags selecionadas.

Se esta opção estiver ativada, o resultado da pesquisa irá mostrar os dispositivos com descrições que não contêm todos as tags selecionadas.

Por padrão, esta opção está desativada.

Para adicionar tags ao critério, clique no botão **Adicionar** e selecione as tags clicando no campo de entrada **Tag**. Especifique se deseja incluir ou excluir os dispositivos com as tags selecionadas na seleção de dispositivos.

Todos os dispositivos com essa tag

Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

Por padrão, esta opção está selecionada.

Todos os dispositivos sem essa tag

Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições não contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

Usuários

Na seção **Usuários**, você pode definir o critério para incluir dispositivos na seleção de acordo com as contas de usuários que efetuaram o login no sistema operacional.

Último usuário que fez login no sistema

Se a opção estiver ativada, será possível selecionar a conta de usuário para configurar o critério. Os resultados da pesquisa incluem os dispositivos nos quais o usuário selecionado efetuou o último login no sistema.

Usuário que fez login no sistema pelo menos uma vez

Se esta opção estiver ativada, clique no botão **Procurar** para especificar uma conta de usuário. Os resultados da pesquisa incluem os dispositivos nos quais o usuário especificado efetuou o login no sistema ao menos uma vez.

Proprietário do dispositivo

Na seção **Proprietário do dispositivo**, você pode configurar os critérios para incluir dispositivos na seleção de acordo com os proprietários registrados do dispositivo, suas funções e sua associação em grupos de segurança:

Proprietário do dispositivo

Selecione o nome de usuário do proprietário do dispositivo em um grupo de segurança interno. Saiba mais sobre usuários e funções de usuário nesta seção.

Somente um usuário pode ser registrado como proprietário do dispositivo.

Associação do proprietário do dispositivo no grupo de segurança do Active Directory

Selecione um grupo de segurança externo do Active Directory ao qual o proprietário do dispositivo pertence.

O usuário pode fazer parte de um grupo de segurança do Active Directory ou de um grupo incluído nesse grupo de segurança do Active Directory.

Função do proprietário do dispositivo

Selecione a função atribuída ao proprietário do dispositivo. Saiba mais sobre as funções do usuário neste artigo.

Associação do proprietário do dispositivo em um grupo de segurança interno

Selecione um grupo de segurança interno ao qual o proprietário do dispositivo pertence.

Exportação da lista de dispositivos a partir de uma seleção de dispositivos

O Kaspersky Security Center Linux permite salvar as informações sobre os dispositivos de uma seleção de dispositivos e exportá-los em um arquivo CSV ou TXT.

Para exportar a lista de dispositivos na seleção de dispositivos:

1. Abra a tabela com os dispositivos a partir da seleção de dispositivos.
2. Use uma das seguintes formas para selecionar os dispositivos que deseja exportar:
   - Para selecionar dispositivos específicos, marque as caixas de seleção ao lado deles.
   - Para selecionar todos os dispositivos da página da tabela atual, marque a caixa de seleção no cabeçalho da tabela de dispositivos e, em seguida, marque a caixa de seleção **Selecionar tudo na página atual**.
   - Para selecionar todos os dispositivos da tabela, marque a caixa de seleção no cabeçalho da tabela de dispositivos e, em seguida, marque a caixa de seleção **Selecionar tudo**.
3. Clique no botão **Exportar para CSV** ou **Exportar para TXT**. Todas as informações sobre os dispositivos selecionados incluídos na tabela serão exportadas.

Observe que, caso um critério de filtro tenha sido aplicado na tabela de dispositivos, apenas os dados filtrados das colunas exibidas serão exportados.

Remover os dispositivos de grupos de administração em uma seleção

Ao trabalhar com uma seleção de dispositivos, você poderá remigrar dispositivos dos grupos de administração diretamente nesta seleção, sem alternar para os grupos de administração dos quais estes dispositivos precisam ser removidos.

Para remigrar dispositivos de grupos de administração:

1. No menu principal, vá para **Gerenciamento de ativos → Seleções de dispositivos** ou **Descoberta e implementação → Seleções de dispositivos**.
2. Na lista de seleção, clique no nome da seleção de dispositivos.

   A página exibe uma tabela com informações sobre os dispositivos incluídos na seleção de dispositivos.
3. Selecione os dispositivos que deseja remover e, em seguida, clique em **Excluir**.

   Os dispositivos selecionados serão removidos de seus respectivos grupos de administração.

Tags de dispositivo

O Kaspersky Security Center Linux permite aplicar *tags* aos dispositivos. Uma tag é um valor de string que pode ser usado para agrupar, descrever ou localizar dispositivos. As tags atribuídas aos dispositivos podem ser usadas para criar seleções, para localizar dispositivos e para distribuir dispositivos entre grupos de administração.

Você pode identificar os dispositivos manualmente ou automaticamente. Caso não queira atribuir uma tag a um dispositivo individual, será possível usar tags manuais. A codificação automática é executada pelo Kaspersky Security Center Linux de uma das seguintes formas:

- De acordo com as regras de marcação especificadas.
- Por um aplicativo.

Não recomendamos usar diferentes formas de marcação para atribuir a mesma tag. Por exemplo, se a tag for atribuída pela regra, não é recomendável atribuir manualmente essa tag aos dispositivos.

Se as tags forem atribuídas por regras, os dispositivos serão identificados automaticamente quando as regras especificadas forem atendidas. Uma regra individual corresponde a cada tag. As regras são aplicadas às propriedades da rede do dispositivo, sistema operacional, aplicativos instalados no dispositivo e outras propriedades de dispositivo. Por exemplo, você pode definir uma regra que atribuirá o identificador `[CentOS]` a todos os dispositivos que executando o sistema operacional. CentOS. Assim, é possível usar essa tag ao criar uma seleção de dispositivos. Isso ajudará a classificar todos os dispositivos CentOS e atribuir-lhes uma tarefa.

É possível adicionar apenas uma regra de marcação automática por tag. Se uma regra nova for criada para a mesma tag, a anterior será substituída.

A tag é automaticamente removida de um dispositivo nos seguintes casos:

- Quando o dispositivo deixa de atender às condições da regra que atribui a tag.
- Quando a regra que atribui a tag é desativada ou excluída.

A lista de tags e a lista de regras em cada Servidor de Administração são independentes de todos outros Servidores de Administração, inclusive um Servidor de Administração principal ou Servidores de Administração virtuais subordinados. Uma regra é aplicada somente a dispositivos do mesmo Servidor de Administração no qual a regra é criada.

Criando uma tag de dispositivo

Para criar uma tag de dispositivo:

1. No menu principal, vá para **Repositórios → Tags de dispositivos**.
2. Na guia **Tags de dispositivos**, clique no botão **Adicionar**.
   Uma nova janela de tag é exibida.
3. No campo **Tag**, insira um nome de tag.
4. Clique em **Salvar** para salvar as alterações.

A nova tag aparece na lista de tags de dispositivo.

Renomeando uma tag de dispositivo

Para renomear uma tag de dispositivo:

1. No menu principal, vá para **Repositórios → Tags de dispositivos**.
2. Na guia **Tags de dispositivos**, selecione a tag que deseja renomear.
   A janela de propriedades do identificador é exibida.
3. No campo **Tag**, altere o nome da tag.
4. Clique em **Salvar** para salvar as alterações.

A tag atualizada aparece na lista de tags de dispositivo.

Excluindo uma tag de dispositivo

Você pode excluir somente tags atribuídas manualmente.

Para excluir uma tag de dispositivo atribuída manualmente:

1. No menu principal, vá para **Repositórios** → **Tags de dispositivos**.

   A lista de tags é exibida.

2. Na guia **Tags de dispositivos**, selecione as tags de dispositivo que deseja excluir.

3. Em seguida, clique no botão **Excluir**.

4. Na janela que se abre, clique em **Sim**.

   A tag de dispositivo é excluída. A tag excluída é automaticamente removida de todos os dispositivos aos quais foi atribuída.

Quando você exclui uma tag de dispositivo atribuída por uma regra de codificação automática, a regra não é excluída e a tag será atribuída a um novo dispositivo que atender às condições da regra pela primeira vez. Se você excluir uma regra de codificação automática, a tag especificada nas condições da regra será removida de todos os dispositivos aos quais foi atribuída, mas não será excluída da lista de tags. Se necessário, você pode excluir manualmente a tag da lista.

A tag excluída não é removida automaticamente do dispositivo caso ela seja atribuída ao dispositivo por um aplicativo ou Agente de Rede. Para gerenciar essas tags, use o utilitário klscflag.

Visualizando dispositivos aos quais uma tag está atribuída

Para visualizar dispositivos aos quais uma tag está atribuída:

1. No menu principal, vá para **Repositórios** → **Tags de dispositivos**.

2. Na guia **Tags de dispositivos**, clique no link **Visualizar dispositivos** ao lado da tag para a qual você deseja visualizar a lista de dispositivos atribuídos.

   Você será redirecionado para a seção **Dispositivos gerenciados** do menu principal, com os dispositivos filtrados pela tag para a qual você clicou no link **Visualizar dispositivos**.

3. Se você quiser retornar à lista de tags de dispositivos, clique no botão **Voltar** do navegador.

Depois de visualizar os dispositivos para os quais a tag está atribuída, será possível criar e atribuir uma nova tag ou atribuir a tag existente a outros dispositivos. Nesse caso, é necessário remover o filtro por tag, selecionar os dispositivos e, então, atribuir a tag.

Visualizando as tags atribuídas a um dispositivo

Para visualizar as tags atribuídas a um dispositivo:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo cujas tags deseja visualizar.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Tags**.

   A lista de tags atribuídas ao dispositivo selecionado é exibida. Na coluna **Tag atribuída**, é possível visualizar como a tag foi atribuída.

Na barra de ferramentas, você pode fazer o seguinte:

- Atribua outra tag ao dispositivo.
- Remova uma tag já atribuída.
- Visualizar todas as tags de dispositivos que existem no Servidor de Administração.

Você não pode visualizar as tags atribuídas localmente no dispositivo.

Identificação de um dispositivo manualmente

Para atribuir uma tag a um dispositivo manualmente:

1. Visualize as tags atribuídas ao dispositivo ao qual deseja atribuir outra tag.
2. Clique em **Adicionar**.
3. Na janela que se abre, execute uma das seguintes ações:
   - Para criar e atribuir uma nova tag, selecione **Criar nova tag** e especifique o nome da nova tag.
   - Para selecionar uma tag existente, selecione **Atribuir tag existente** e depois selecione a tag desejada na lista suspensa.
4. Clique em **OK** para aplicar as alterações.
5. Clique em **Salvar** para salvar as alterações.

   A tag selecionada é atribuída ao dispositivo.

Removendo uma tag atribuído de um dispositivo

Para remover uma tag de um dispositivo:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo cujas tags deseja visualizar.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Tags**.
4. Marque a caixa de seleção ao lado da tag que deseja remover.
5. No topo da lista, clique no botão **Desatribuir tag**.
6. Na janela que se abre, clique em **OK**.

   A tag é removida do dispositivo.

A tag de dispositivo não atribuída não é excluída. Se quiser, você poderá excluí-lo manualmente.

Não é possível remover manualmente as tags atribuídas ao dispositivo por aplicativos ou pelo Agente de Rede. Para gerenciar essas tags, use o utilitário klscflag.

Visualização de regras para identificar dispositivos automaticamente

Para visualizar regras para identificar dispositivos automaticamente,

Execute uma das seguintes ações:

- No menu principal, vá para **Repositórios** → **Tags de dispositivos** → **Regras de aplicação automática de tags**.
- Visualize as tags atribuídas a um dispositivo e, em seguida, clique no botão **Configurar regras de aplicação automática de tags**.

A lista de regras para identificar dispositivos automaticamente é exibida.

Edição de uma regra para identificar dispositivos automaticamente

Para editar uma regra para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Clique no nome da regra que deseja editar.

   Uma janela de configurações de regra é exibida.
3. Edite as propriedades gerais da regra:

   a. No campo **Nome da regra**, altere o nome da regra.

      O nome de um perfil não pode conter mais do que 256 caracteres.

   b. Execute uma das seguintes ações:

      - Ative a regra mudando o botão de alternar para **Regra ativada**.
      - Desative a regra mudando o botão de alternar para **Regra desativada**.
4. Execute uma das seguintes ações:

   - Se desejar adicionar uma nova condição, clique no botão **Adicionar** e especifique as configurações da nova condição na janela aberta.
   - Se deseja editar uma condição existente, clique no nome da condição que quer editar e edite as configurações de condição.
   - Se deseja excluir uma condição, marque a caixa de seleção ao lado do nome da condição que deseja excluir e clique em **Excluir**.
5. Clique em **OK** na janela de configurações de condições.
6. Clique em **Salvar** para salvar as alterações.

A regra editada é mostrada na lista.

Criação de uma regra para identificar dispositivos automaticamente

Para criar uma regra para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Clique em **Adicionar**.

   Uma nova janela de configurações de regra é exibida.

3. Configure as propriedades gerais da regra:

   a. No campo **Nome da regra**, insira o novo nome da regra.

      O nome não pode conter mais de 256 caracteres.

   b. Execute uma das seguintes ações:

      - Ative a regra mudando o botão de alternar para **Regra ativada**.
      - Desative a regra mudando o botão de alternar para **Regra desativada**.

   c. No campo **Tag**, digite o novo nome da tag de dispositivo ou selecione uma das tags de dispositivo existentes na lista.

      O nome não pode conter mais de 256 caracteres.

4. Na seção de condições, clique no botão **Adicionar** para adicionar uma nova condição.

   Uma nova janela de configurações de condição é exibida.

5. Insira o nome da condição.

   O nome não pode conter mais de 256 caracteres. O nome deve ser exclusivo em uma regra.

6. Configure a regra para ser acionada nas seguintes condições (você pode selecionar várias condições):

   - **Rede** – Propriedades da rede do dispositivo, como o nome DNS do dispositivo ou a sua inclusão em um domínio ou em uma subrede IP.

     Caso o agrupamento com distinção entre maiúsculas e minúsculas seja definido para o banco de dados usado para o Kaspersky Security Center Linux, mantenha maiúsculas e minúsculas ao especificar um nome DNS de dispositivo. Caso contrário, a regra de marcação automática não funcionará.

   - **Aplicativos** – Presença do Agente de Rede no dispositivo, tipo de sistema operacional, versão, arquitetura e gerenciador de pacotes.
   - **Máquinas virtuais** – O dispositivo pertence a um tipo específico da máquina virtual.
   - **Registro de aplicativos** – Presença de aplicativos de diferentes fornecedores no dispositivo.

7. Clique em **OK** para salvar as alterações.

   Se necessário, você pode definir múltiplas condições para única regra. Neste caso, a tag será atribuída um dispositivo se atender ao menos uma condição.

8. Clique em **Salvar** para salvar as alterações.

A regra recém-criada entra em vigor nos dispositivos gerenciados pelo Servidor de Administração selecionado. Se as configurações de um dispositivo atenderem as condições da regra, ao dispositivo é atribuído à tag.

Depois, a regra é aplicada nos seguintes casos:

- Automática e periodicamente, dependendo da carga de trabalho de servidor
- Depois que você editar a regra

- Quando você executar a regra manualmente
- Após o Servidor de Administração detectar uma modificação nas configurações de um dispositivo que atende às condições de regra ou nas configurações de um grupo que contém tal dispositivo

Você pode criar múltiplas regras de identificação. A um dispositivo único pode ser atribuído múltiplas regras de identificação e se as respetivas condições destas regras forem atendidas simultaneamente. Você pode exibir a lista de todas as tags atribuídas nas propriedades do dispositivo.

Execução de regras para identificar dispositivos automaticamente

Quando uma regra é executada, a tag especificada nas propriedades dessa regra é atribuída aos dispositivos que atendem às condições especificadas nas propriedades da mesma regra. Você pode executar apenas regras ativas.

Para executar regras para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Marque as caixas de seleção ao lado das regras ativas que você deseja executar.
3. Clique no botão **Executar regra**.

   As regras selecionadas são executadas.

Exclusão de uma regra para identificar dispositivos automaticamente

Para excluir uma regra para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Marque a caixa de seleção ao lado da regra que você deseja excluir.
3. Clique no botão **Excluir**.
4. Na janela que se abre, clique em **OK**.

   A regra selecionada é excluída. A tag especificada nas propriedades dessa regra tem a atribuição removida de todos dos dispositivos aos quais foi atribuída.

> A tag de dispositivo não atribuída não é excluída. Se quiser, você poderá excluí-lo manualmente.

Gerenciamento de tags de dispositivo usando o utilitário klscflag

Para atribuir um conjunto de tags a um dispositivo, é preciso executar o utilitário klscflag no dispositivo cliente ao qual se deseja atribuir as tags.

O utilitário klscflag substitui as tags existentes atribuídas ao dispositivo. Isso significa que é possível adicionar ou remover tags ao indicar o conjunto de tags desejado no comando. O utilitário não possui comandos separados para adicionar ou remover tags individuais. Em vez disso, todo o conjunto de tags é modificado.

Ao especificar os nomes de tags em comandos como o klscflag, é recomendado utilizar um padrão consistente de uso de letras maiúsculas e minúsculas, deixando todas as letras em maiúsculo, por exemplo. Usar todas as letras maiúsculas pode ajudar a evitar possíveis problemas com tags que diferem apenas em maiúsculas e minúsculas, dependendo da configuração do DBMS.

Para atribuir uma ou várias tags ao seu dispositivo usando o utilitário klscflag:

1. Execute o prompt de comando em uma conta com privilégios de raiz e, em seguida, altere seu diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado no diretório onde o Agente de Rede está instalado. O diretório de instalação padrão é /opt/kaspersky/klnagent64/sbin/.

2. Insira um dos seguintes comandos:

   - Para atribuir um conjunto de tags:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NOME DA TAG 1\",\"NOME DA TAG 2\",\"NOME DA TAG 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     onde `[\"NOME DA TAG 1\",\"NOME DA TAG 2\",\"NOME DA TAG 3\"]` é a lista de tags que se deseja atribuir ao dispositivo.

     Caso deixe os colchetes vazios, isso removerá todas as tags do dispositivo:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - Para atribuir uma nova tag a um conjunto existente de tags:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NOME DA NOVA TAG\",\"NOME DA TAG 1\",\"NOME DA TAG 2\",\"NOME DA TAG 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     onde `NOME DA NOVA TAG` é o nome da tag que se deseja atribuir ao dispositivo e `NOME DA TAG 1`, `NOME DA TAG 2` e `NOME DA TAG 3` são os nomes das tags já atribuídas ao dispositivo.

   - Para remover uma tag específica sem remover outras tags já atribuídas ao dispositivo, execute o comando com o conjunto atualizado de tags.

     Por exemplo, caso suas tags atuais sejam `NOME DA TAG 1`, `NOME DA TAG 2` e `NOME DA TAG 3` e se quiser remover `NOME DA TAG 2`, execute o seguinte comando:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NOME DA TAG 1\",\"NOME DA TAG 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. Execute o seguinte comando para reiniciar o serviço do Agente de Rede:

```
systemctl restart klnagent
```

   O utilitário klscflag atribui as tags especificadas ao seu dispositivo.

4. Se você quiser garantir que o utilitário klscflag tenha atribuído com sucesso as tags especificadas, visualize as tags atribuídas ao dispositivo.

Como alternativa, é possível atribuir tags de dispositivo manualmente.

Criptografia e proteção de dados

A criptografia de dados reduz o risco de vazamento não intencional de dados confidenciais e corporativos caso seu computador portátil ou disco rígido seja roubado ou perdido. Além disso, a criptografia de dados permite impedir o acesso de usuários e aplicativos não autorizados.

É possível usar o recurso de criptografia de dados se sua rede incluir dispositivos gerenciados baseados no Windows com o Kaspersky Endpoint Security for Windows instalado. Nesse caso, em dispositivos executando o Windosws como sistema operacional, você pode gerenciar os seguintes tipos de criptografia:

- Criptografia de Unidade de Disco BitLocker
- Kaspersky Disk Encryption

Não recomendamos ativar a criptografia na VDI.

Ao usar esses componentes do Kaspersky Endpoint Security for Windows, é possível, por exemplo, ativar ou desativar a criptografia, visualizar a lista de unidades criptografadas ou gerar e visualizar relatórios sobre criptografia.

Para configurar a criptografia, defina a política do Kaspersky Endpoint Security for Windows no Kaspersky Security Center Linux. O Kaspersky Endpoint Security for Windows executa a criptografia e a descriptografia de acordo com a política ativa em vigor. Para obter instruções detalhadas sobre como configurar regras e uma descrição dos recursos de criptografia, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

O gerenciamento de criptografia para uma hierarquia de Servidores de Administração não está atualmente disponível no Web Console. Use o Servidor de Administração principal para gerenciar dispositivos criptografados.

Você pode mostrar ou ocultar alguns dos elementos da interface relacionados ao recurso de gerenciamento de criptografia usando as configurações da interface do usuário.

Visualização da lista de unidades criptografadas

No Kaspersky Security Center Linux, é possível visualizar os detalhes sobre as unidades criptografadas e dispositivos criptografados no nível da unidade. Após as informações de uma unidade serem descriptografadas, a unidade é automaticamente removida da lista.

Para exibir a lista de unidades criptografadas,

No menu principal, vá para **Operações** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.

Se a seção não estiver no menu, isso significa que ela está oculta. Nas configurações da interface do usuário, habilite a opção **Mostrar a criptografia e proteção de dados** para exibir a seção.

É possível exportar a lista de unidades criptografadas para um arquivo CSV ou TXT. Para fazer isso, clique no botão **Exportar para CSV** ou **Exportar para TXT**.

Visualização da lista de eventos de criptografia

Ao executar tarefas de criptografia ou descriptografia de dados nos dispositivos, o Kaspersky Endpoint Security for Windows envia ao Kaspersky Security Center Linux informações sobre os eventos dos seguintes tipos:

- Não é possível criptografar ou descriptografar um arquivo, ou criar um arquivo criptografado devido à falta de espaço livre em disco.
- Não é possível criptografar ou descriptografar um arquivo, ou criar um arquivo criptografado devido a problemas com a licença.
- Não é possível criptografar ou descriptografar um arquivo, ou criar um arquivo criptografado devido à ausência de direitos de acesso.
- O aplicativo foi proibido de acessar um arquivo criptografado.
- Erros desconhecidos.

Para exibir uma lista de eventos que ocorreram durante a criptografia de dados nos dispositivos,

No menu principal, vá para **Operações** → **Criptografia e proteção de dados** → **Eventos de criptografia**.

Se a seção não estiver no menu, isso significa que ela está oculta. Nas configurações da interface do usuário, habilite a opção **Mostrar a criptografia e proteção de dados** para exibir a seção.

É possível exportar a lista de unidades criptografadas para um arquivo CSV ou TXT. Para fazer isso, clique no botão **Exportar para CSV** ou **Exportar para TXT**.

Como alternativa, você pode examinar a lista de eventos de criptografia para cada dispositivo gerenciado.

Para visualizar os eventos de criptografia de um dispositivo gerenciado:

1. No menu principal, acesse a seção **Gerenciamento de ativos** → **Dispositivos gerenciados**.
2. Clique no nome de um dispositivo gerenciado.
3. Na guia **Geral**, vá para a seção **Proteção**.
4. Clique no link **Exibir erros de criptografia de dados**.

Criação e visualização de relatórios de criptografia

É possível gerar os seguintes relatórios:

- Relatório de status da criptografia dos dispositivos gerenciados. Este relatório fornece detalhes sobre a criptografia de dados de vários dispositivos gerenciados. Por exemplo, o relatório mostra o número de dispositivos aos quais a política com regras de criptografia configuradas se aplica. Além disso, você pode descobrir, por exemplo, quantos dispositivos precisam ser reinicializados. Ele também contém informações sobre a tecnologia de criptografia e o algoritmo para cada dispositivo.
- Relatório de status da criptografia dos dispositivos de armazenamento em massa. Este relatório contém informações semelhantes ao relatório sobre o status de criptografia de dispositivos gerenciados, mas fornece dados apenas para dispositivos de armazenamento em massa e unidades removíveis.
- Relatório de direitos de acesso aos dispositivos criptografados. Este relatório mostra quais contas de usuário têm acesso a unidades criptografadas.
- Relatório de erros na criptografia de arquivos. Este relatório contém informações sobre os erros que ocorreram ao executar as tarefas de criptografia ou a descriptografia dos dados nos dispositivos.
- Relatório de bloqueio de acesso aos arquivos criptografados. Este relatório contém informações sobre como bloquear o acesso dos aplicativos aos arquivos criptografados. Este relatório será útil se um usuário ou aplicativo não autorizado tentar acessar arquivos ou unidades criptografadas.

É possível gerar qualquer relatório na seção **Monitoramento** → **Relatórios**. Alternativamente, na seção **Operações** → **Criptografia e proteção de dados**, você pode gerar os seguintes relatórios de criptografia:

- Relatório de status da criptografia dos dispositivos de armazenamento em massa
- Relatório de direitos de acesso aos dispositivos criptografados
- Relatório de erros na criptografia de arquivos

*Para gerar um relatório de criptografia na seção **Criptografia e proteção de dados**:*

1. Certifique-se de ter ativado a opção **Mostrar a criptografia e proteção de dados** nas opções de interface.
2. No menu principal, vá para **Operações** → **Criptografia e proteção de dados**.

3. Abra uma das seguintes seções:

   - **Dispositivos criptografados** gera o relatório sobre o status de criptografia de status de dispositivos de armazenamento em massa ou o relatório sobre direitos de acesso a unidades criptografadas.
   - **Eventos de criptografia** gera o relatório sobre erros de criptografia de arquivo.

4. Clique no nome do relatório que deseja gerar.

A geração do relatório começa.

Concessão de acesso a uma unidade criptografada no modo offline

Um usuário pode solicitar acesso a um dispositivo criptografado, por exemplo, quando o Kaspersky Endpoint Security não estiver instalado no dispositivo gerenciado. Depois que você receber a solicitação, poderá criar um arquivo de chave de acesso e enviá-lo ao usuário. Todos os casos de uso e instruções detalhadas são fornecidos na Ajuda do Kaspersky Endpoint Security para a plataforma necessária.

Para conceder acesso a um dispositivo criptografado no modo offline no Kaspersky Endpoint Security for Windows:

1. Obtenha um arquivo de solicitação de acesso de um usuário (com a extensão FDERTC). Siga as instruções da Ajuda do Kaspersky Endpoint Security for Windows para gerar o arquivo no Kaspersky Endpoint Security for Windows.
2. No menu principal, vá para **Operações → Criptografia e proteção de dados → Dispositivos criptografados**.

   Uma lista de unidades criptografadas é exibida.
3. Selecione a unidade à qual o usuário solicitou acesso.
4. Clique no botão **Permitir acesso ao dispositivo em modo offline**.
5. Na janela aberta, selecione o plug-in Kaspersky Endpoint Security for Windows.
6. Siga as instruções fornecidas na Ajuda do Kaspersky Endpoint Security for Windows (consulte as instruções do Kaspersky Security Center Web Console no final da seção).

Depois disso, o usuário aplica o arquivo recebido para acessar a unidade criptografada e ler os dados armazenados na unidade.

Transmitindo as chave de criptografia entre Servidores de Administração

Quando o recurso de criptografia de dados for ativado em um dispositivo gerenciado, a chave de criptografia é armazenada no Servidor de Administração. A chave de criptografia é usada para acessar dados criptografados e gerenciar a política de criptografia.

A chave de criptografia deve ser transmitida para outro Servidor de Administração nos seguintes casos:

- Reconfiguração do Agente de Rede em um dispositivo gerenciado para atribuir o dispositivo a outro Servidor de Administração. Se esse dispositivo contiver dados criptografados, a chave de criptografia deverá ser transmitida ao Servidor de Administração de destino. Caso contrário, os dados não poderão ser descriptografados.

- Criptografia de uma unidade removível conectada a um dispositivo D1 gerenciado pelo Servidor de Administração S1 e, em seguida, conexão dessa unidade removível a um dispositivo D2 gerenciado pelo Servidor de Administração S2. Para acessar os dados na unidade removível, a chave de criptografia deve ser transmitida do Servidor de Administração S1 para o Servidor de Administração S2.

- Criptografa de um arquivo em um dispositivo D1 gerenciado pelo Servidor de Administração S1 e, em seguida, tentativa de acesso ao arquivo em um dispositivo D2 gerenciado pelo Servidor de Administração S2. Para acessar o arquivo, a chave de criptografia deve ser transmitida do Servidor de Administração S1 para o Servidor de Administração S2.

Você pode transmitir chaves de criptografia das seguintes maneiras:

- Automaticamente, ativando a opção **Usar a hierarquia de Servidores de Administração para obter chaves de criptografia** nas propriedades de dois Servidores de Administração entre os quais uma chave de criptografia deve ser transmitida. Se esta opção estiver desativada para um dos Servidores de Administração, a transmissão automática de chaves de criptografia não será possível.

  Ao ativar a opção **Usar a hierarquia de Servidores de Administração para obter chaves de criptografia** nas propriedades de um Servidor de Administração, o Servidor de Administração envia as chaves de criptografia armazenadas no seu repositório para o Servidor de Administração principal (se houver) um nível acima na hierarquia.

  Quando você tenta acessar dados criptografados, o Servidor de Administração primeiro pesquisa a chave de criptografia em seu próprio repositório. Se a opção **Usar a hierarquia de Servidores de Administração para obter chaves de criptografia** estiver ativada e a chave de criptografia necessária não for encontrada no repositório, o Servidor de Administração envia adicionalmente uma solicitação aos Servidores de Administração principais (se houver) para fornecer a chave de criptografia necessária. A solicitação será enviada a todos os Servidores de Administração principais até o servidor no nível mais alto da hierarquia.

- Manualmente, de um Servidor de Administração para outro, exportando e importando o arquivo que contendo as chaves de criptografia.

  A exportação e a importação de chaves de criptografia são ações incluídas no recurso de gerenciamento da chave de criptografia. Para realizar essas ações, configure os direitos de acesso ao recurso para usuários do Kaspersky Security Center Linux da seguinte forma:

  - Conceda o direito de acesso **Ler** ao recurso de gerenciamento da chave de criptografia para um usuário que exporte chaves de criptografia do Servidor de Administração secundário.

  - Conceda o direito de acesso de **Gravação** ao recurso de gerenciamento da chave de criptografia para um usuário que importe as chaves de criptografia para o Servidor de Administração de destino.

Para ativar a transmissão automática de chaves de criptografia entre Servidores de Administração dentro da hierarquia:

1. Vá para as propriedades do Servidor de Administração desejado:

   a. No menu principal, selecione uma seção (exceto para **Marketplace**, **Navegação do console** e **Configurações**), e então, na parte superior da página, clique no botão **Mostrar a hierarquia**.

   b. No painel de navegação exibido, passe o cursor do mouse sobre o nome do Servidor de Administração desejado e clique no ícone de configurações (⚙).

   Como alternativa, é possível clicar no nome do Servidor de Administração e, depois que o nome for exibido no menu principal, clicar nele para abrir a janela de propriedades do servidor.

2. Na janela de propriedades exibida, selecione a seção **Algoritmo de criptografia**.

3. Ative a opção **Usar a hierarquia de Servidores de Administração para obter chaves de criptografia**.

4. Clique em **Salvar** para aplicar as alterações.

As chaves de criptografia serão transmitidas aos Servidores de Administração principais (se houver) na próxima sincronização (a pulsação). Este Servidor de Administração também fornecerá, mediante solicitação, uma chave de criptografia de seu repositório para um Servidor de Administração secundário.

Para transmitir chaves de criptografia entre Servidores de Administração manualmente:

1. Vá para as propriedades do Servidor de Administração para o qual você deseja exportar as chaves de criptografia:

   a. No menu principal, selecione uma seção (exceto para **Marketplace**, **Navegação do console** e **Configurações**), e então, na parte superior da página, clique no botão **Mostrar a hierarquia**.

   b. No painel de navegação exibido, passe o cursor do mouse sobre o nome do Servidor de Administração desejado e clique no ícone de configurações (⚙).

   Como alternativa, é possível clicar no nome do Servidor de Administração e, depois que o nome for exibido no menu principal, clicar nele para abrir a janela de propriedades do servidor.

2. Na janela de propriedades exibida, selecione a seção **Algoritmo de criptografia**.

3. Clique em **Exportar chaves de criptografia**.

   Certifique-se de que um usuário que exporta chaves de criptografia do Servidor receba o direito de acesso **Leitura** ao recurso de gerenciamento da chave de criptografia.

4. Na janela **Exportar chaves de criptografia do Servidor de Administração?**, faça o seguinte:

   a. Especifique uma senha para proteger o arquivo contra acesso não autorizado.

   b. Especifique onde você deseja salvar o arquivo.

   > Memorize a senha. Uma senha perdida não pode ser recuperada. Se a senha for perdida, você deverá repetir o procedimento de exportação. Portanto, anote a senha e mantenha-a à mão.

5. Transmitir o arquivo para outro Servidor de Administração, por exemplo, através de uma pasta compartilhada ou unidade removível.

6. Vá para as propriedades do Servidor de Administração para o qual você deseja importar as chaves de criptografia.

7. Na janela de propriedades, selecione a seção **Algoritmo de criptografia**.

8. Clique em **Importar chaves de criptografia**.

   Verifique e confirme se um usuário que importa as chaves de criptografia para o Servidor recebeu o direito de acesso de **Gravação** ao recurso de gerenciamento da chave de criptografia.

9. Selecione o arquivo que contém as chaves de criptografia.

10. Insira a senha e clique em **OK**.

As chaves de criptografia são transmitidas para o Servidor de Administração de destino.

Alterar o Servidor de Administração para dispositivos cliente

Você pode alterar o Servidor de Administração para dispositivos clientes específicos. Para isso, use a tarefa *Alterar o Servidor de Administração*.

Para alterar o Servidor de Administração que gerencia dispositivos cliente para outro servidor:

1. Conecte-se ao Servidor de Administração que gerencia os dispositivos.

2. Crie a tarefa do Servidor de Administração.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente. Na janela **Nova tarefa** do Assistente para novas tarefas, selecione o aplicativo **Kaspersky Security Center 17** e o tipo de tarefa **Alterar o Servidor de Administração**. Depois disso, especifique os dispositivos para os quais você deseja alterar o Servidor de Administração:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

     Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

     Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

   - **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**

     Você pode especificar nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

     Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

- **Atribuir tarefa a uma seleção de dispositivos**

  A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

  Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

3. Execute a tarefa criada.

Após a conclusão da tarefa, os dispositivos cliente, para os quais a mesma foi criada, são colocados sob gerenciamento pelo Servidor de Administração especificado nas configurações da tarefa.

Caso o Servidor de Administração seja compatível com a criptografia e a proteção dos dados e o usuário esteja criando uma tarefa *Alterar o Servidor de Administração*, uma advertência é exibida. O aviso indica que se quaisquer dados criptografados forem armazenados nos dispositivos, após o novo servidor começar a gerenciar os dispositivos, os usuários somente serão capazes de acessar os dados criptografados com os quais eles anteriormente trabalharam. Em outros casos, nenhum acesso a dados criptografados será fornecido. Para obter descrições detalhadas de cenários nos quais o acesso aos dados criptografados não é fornecido, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

Evitar conflitos entre vários Servidores de Administração

Caso haja mais de um Servidor de Administração em sua rede, eles poderão ver os mesmos dispositivos cliente. Isso pode resultar, por exemplo, no Servidor de Administração instalando um aplicativo que já foi instalado por outro Servidor de Administração, ou outros conflitos. Para evitar que um aplicativo seja instalado em um dispositivo gerenciado por outro Servidor de Administração, ative a opção **Instalar somente em dispositivos gerenciados por este Servidor de Administração** em propriedades da tarefa *Instalar o aplicativo remotamente*.

Se você ativar a opção **Instalar somente em dispositivos gerenciados por este Servidor de Administração** e, executar a tarefa *Instalar o aplicativo remotamente* em seguida, uma verificação será feita para determinar se os dispositivos são gerenciados por outro Servidor de Administração. Para dispositivos gerenciados por outro Servidor de Administração, o valor do atributo **Gerenciado por outro Servidor de Administração** será `true`. A tarefa *Instalar o aplicativo remotamente* não aplicará a esses dispositivos.

Os valores do atributo **Gerenciado por outro Servidor de Administração** são exibidos na coluna **Gerenciado por outro Servidor de Administração** na lista de dispositivos gerenciados e na lista de dispositivos não atribuídos.

Você também pode usar a propriedade **Gerenciado por outro Servidor de Administração** como um critério com os seguintes objetivos:

- Exibir dispositivos gerenciados
- Seleções de dispositivos
- Regras de migração de dispositivos
- Regras de identificação automática

Para redefinir o atributo Gerenciado por outro Servidor de Administração:

1. No menu principal do Kaspersky Security Center Web Console, vá para **Gerenciamento de ativos** → **Dispositivos não atribuídos**.
2. Selecione o dispositivo necessário e clique no botão **Remova o atributo Gerenciado por um Servidor de Administração diferente**.

O atributo **Gerenciado por outro Servidor de Administração** é redefinido.

Migração de dispositivos conectados com o Servidor de Administração por meio de gateways de conexão para outro Servidor de Administração

É possível migrar os dispositivos conectados com o Servidor de Administração por meio de gateways de conexão para outro Servidor de Administração. Por exemplo, esse procedimento pode ser necessário se você instalar outra versão do Servidor de Administração e não quiser reinstalar o Agente de Rede nos dispositivos, pois isso pode levar muito tempo.

Os comandos descritos na instrução devem ser executados em dispositivos clientes em uma conta com direitos de administrador.

Para migrar um dispositivo conectado por meio do gateway de conexão para outro Servidor de Administração:

1. Execute o utilitário klmover com o parâmetro `-address <endereço do servidor>` para mudar para o novo Servidor de Administração.
2. Execute o comando `klnagchk -nagwait -tl 4`.
3. Execute os seguintes comandos para definir um novo gateway de conexão:
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<gateway ip or name>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Aqui, `<ip ou nome do gateway>` é o endereço do gateway de conexão acessível pela Internet.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` é o número da porta TCP que o gateway de conexão está escutando.
4. Execute o comando `klnagchk -restart -tl 4` para iniciar o serviço do Agente de Rede.

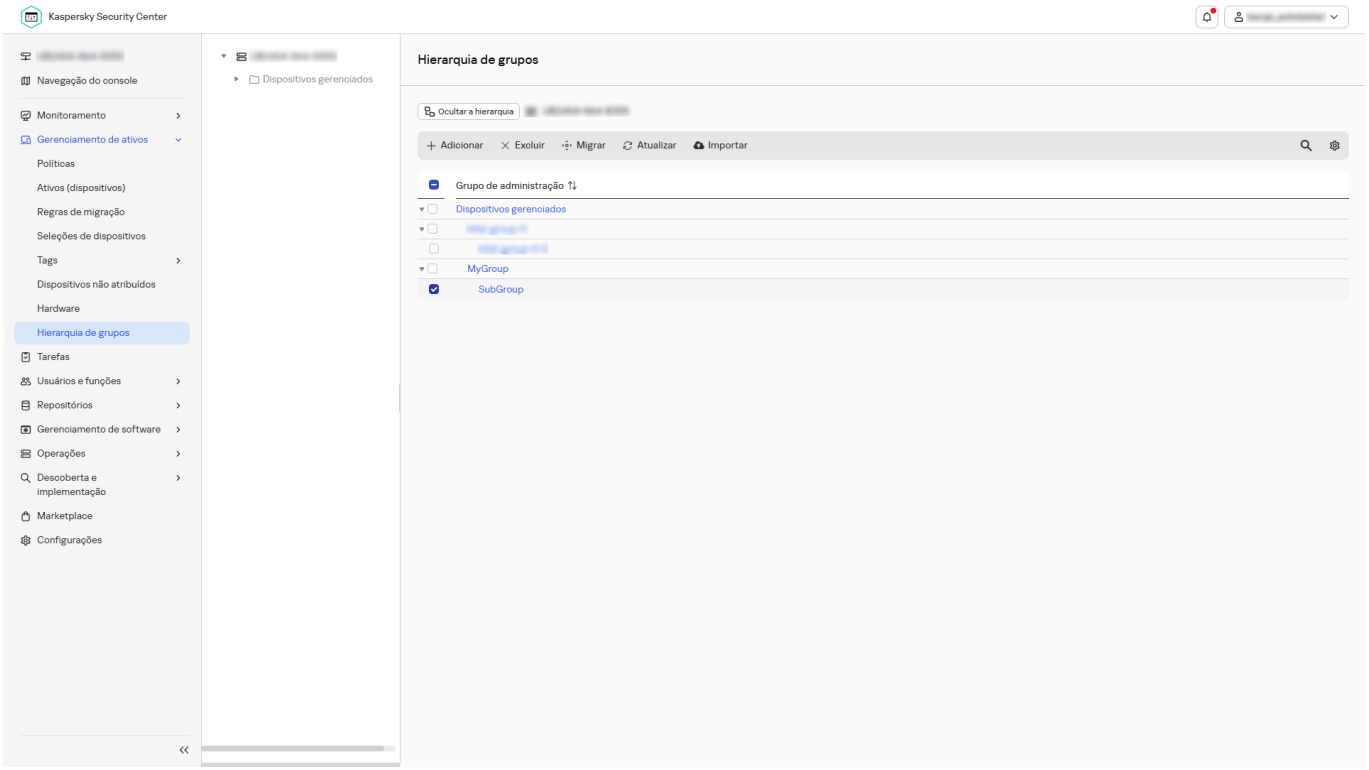
O dispositivo é migrado e conectado com o novo Servidor de Administração por meio do novo gateway conectado.

Exibir e configurar as ações quando os dispositivos mostram inatividade

Se os dispositivos clientes em um grupo estiverem inativos, você poderá receber notificações sobre isso. Você também pode excluir automaticamente esses dispositivos.

Para exibir ou configurar as ações quando os dispositivos no grupo mostrarem inatividade:

1. No menu principal, vá para **Gerenciamento de ativos** → **Hierarquia de grupos**.
2. Vá para as propriedades do grupo de administração desejado por uma das seguintes formas:
   - Clique no nome do grupo de administração.
   - Clique no botão **Mostrar a hierarquia** na parte superior da página. No painel de navegação exibido, passe o cursor do mouse sobre o nome do grupo desejado e clique no ícone de configurações (⚙).



Hierarquia do grupo de administração

   A janela Propriedades do grupo de administração é aberta.

3. Na janela Propriedades, siga para a guia **Configurações**.
4. Na seção **Herança**, ative ou desative as seguintes opções:

   Herdar do grupo principal

   As configurações desta seção serão herdadas do grupo principal no qual o dispositivo cliente está incluído. Se esta opção estiver ativada, as configurações sob **Atividade de dispositivos na rede** serão bloqueadas contra quaisquer alterações.

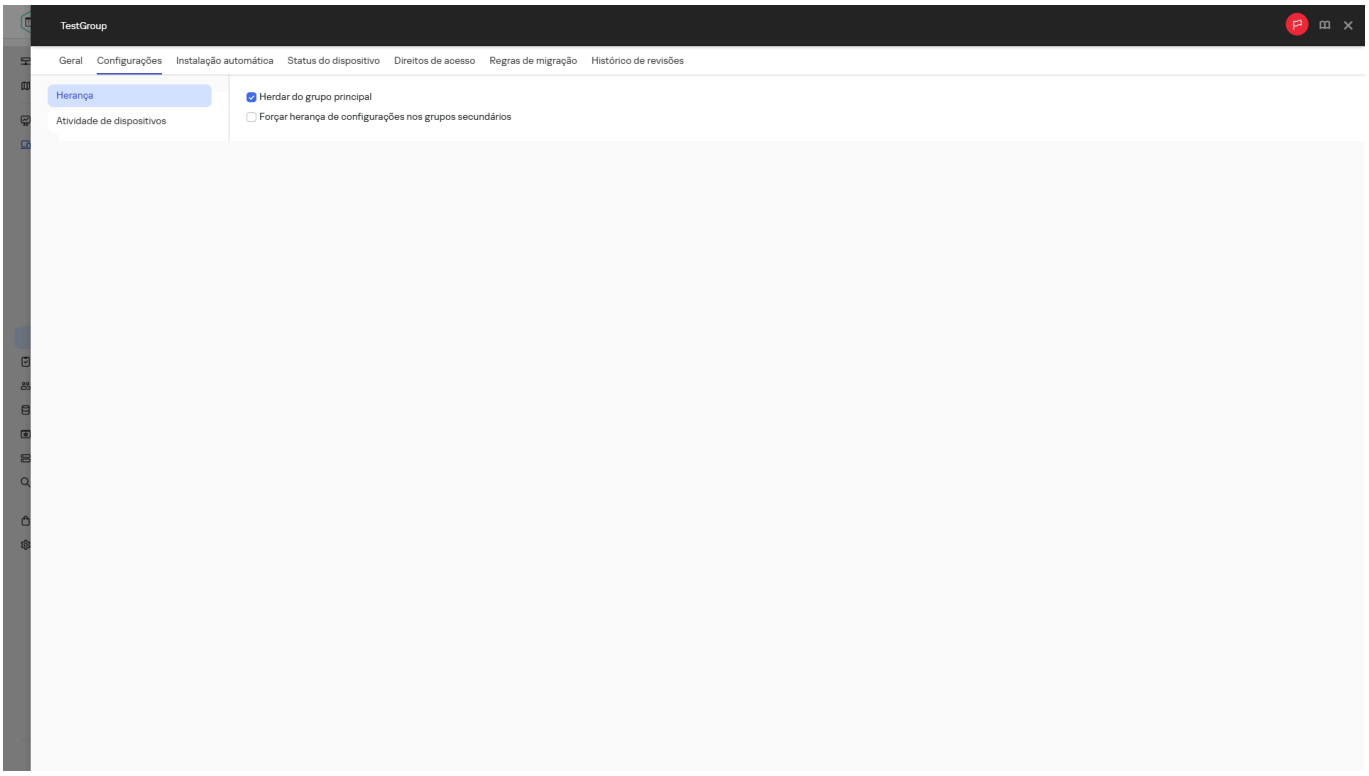
   Esta opção está disponível somente se o grupo de administração tiver um grupo principal.

Por padrão, esta opção está ativada.

Forçar herança de configurações nos grupos secundários

Os valores de configuração serão distribuídos aos grupos secundários, mas essas configurações são bloqueadas nas propriedades dos grupos secundários.

Por padrão, esta opção está desativada.



Propriedades do grupo de administração

5. Na seção **Atividade de dispositivos**, ative ou desative as seguintes opções:

   Notificar o administrador se o dispositivo estiver inativo por mais de (dias)

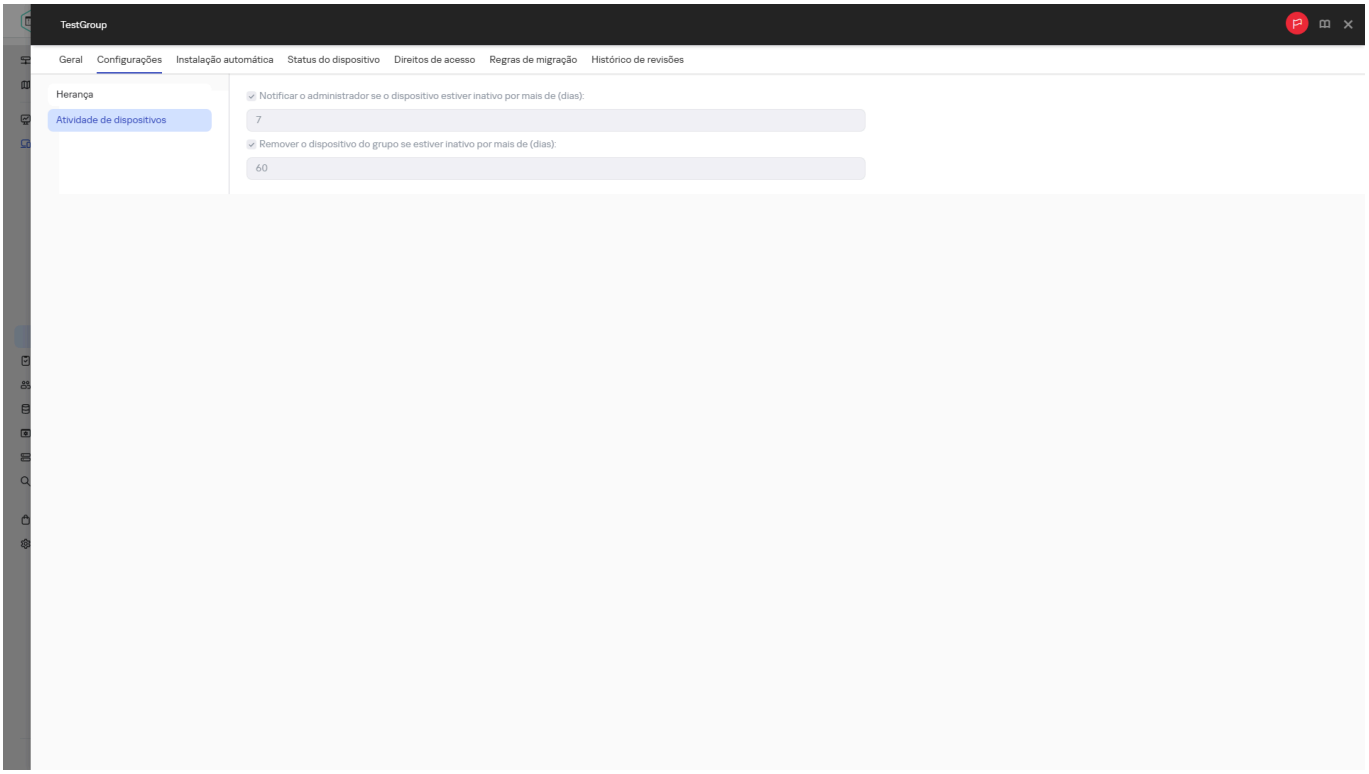
   Se esta opção estiver ativada, o administrador receberá notificações sobre os dispositivos inativos. Você pode especificar o intervalo de tempo após o qual o evento **O dispositivo permaneceu inativo na rede por muito tempo** será criado. O intervalo de tempo predefinido é de 7 dias.

   Por padrão, esta opção está ativada.

   Remover o dispositivo do grupo se estiver inativo por mais de (dias)

   Se esta opção estiver selecionada, você poderá especificar o intervalo de tempo após o qual o dispositivo será automaticamente removido do grupo. O intervalo de tempo predefinido é de 60 dias.

Por padrão, esta opção está ativada.



Propriedades do grupo de administração

6. Clique no botão **Salvar**.

   As suas alterações serão salvas e aplicadas.

Enviar mensagens aos usuários de dispositivos

Para enviar uma mensagem aos usuários de dispositivos:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.
3. Na lista suspensa **Tipo de tarefa**, selecione **Enviar mensagem ao usuário**.
4. Selecione uma opção para especificar o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.
5. Execute a tarefa criada.

Após a conclusão da tarefa, a mensagem criada será enviada aos usuários dos dispositivos selecionados. A tarefa **Enviar mensagem ao usuário** está disponível apenas para os dispositivos que executam o Windows.

Ativar, desativar e reiniciar remotamente dispositivos clientes

O Kaspersky Security Center Linux permite gerenciar dispositivos clientes remotamente, ligando-os, desligando-os ou reiniciando-os.

Para gerenciar remotamente os dispositivos cliente:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.
3. Na lista suspensa **Tipo de tarefa**, selecione **Gerenciar dispositivos**.
4. Selecione uma opção para especificar o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.
5. Selecione o comando (ligar, desligar ou reiniciar).
6. Caso necessário, defina as seguintes configurações para os comandos desativar e reiniciar:

   - Ative o botão **Solicitar confirmação ao usuário** para especificar a mensagem de solicitação ao usuário e os intervalos de tempo após os quais você deseja repetir a solicitação e reiniciar ou desativar os dispositivos.
   - Marque a caixa de seleção **Tempo de espera antes do fechamento forçado de aplicativos nas sessões bloqueadas (min)** e especifique o tempo.

   Estas configurações são aplicáveis somente aos dispositivos clientes Windows. Os dispositivos Linux serão reiniciados ou desativados imediatamente após a conclusão da tarefa.
7. Execute a tarefa criada.

Após a conclusão da tarefa, o comando (ativar, desativar ou reiniciar) será executado nos dispositivos selecionados.

Acesso remoto aos dispositivos gerenciados

O Kaspersky Security Center Linux permite estabelecer uma conexão remota com dispositivos gerenciados. O administrador pode obter acesso remoto ao dispositivo gerenciado por meio de um Agente de Rede instalado no dispositivo. A conexão remota a um dispositivo por meio do Agente de Rede é possível mesmo que as portas TCP e UDP do dispositivo cliente estejam fechadas. Ao estabelecer uma conexão com o dispositivo, o administrador obtém acesso total às informações armazenadas neste dispositivo e pode gerenciar os aplicativos instalados nele.

Os métodos para estabelecer uma conexão remota dependem de qual plataforma é usada no dispositivo com o Kaspersky Security Center Web Console. O Kaspersky Security Center Web Console pode ser instalado em um dispositivo diferente do Servidor de Administração, em um dispositivo baseado em Windows ou Linux.

No Kaspersky Security Center Web Console instalado em um dispositivo Linux, é possível estabelecer as seguintes conexões:

- Para um dispositivo gerenciado baseado em Linux usando:
  - Conexão de desktop remoto (RDP)
  - Computação de rede virtual (VNC)
- Para um dispositivo gerenciado baseado no Windows usando:
  - Conexão de desktop remoto (RDP)
  - Computação de rede virtual (VNC)

No Kaspersky Security Center Web Console instalado em um dispositivo Windows, é possível estabelecer as seguintes conexões:

- Para um dispositivo gerenciado baseado em Linux usando:
  - Conexão de desktop remoto (RDP)
  - Computação de rede virtual (VNC)
- Para um dispositivo gerenciado baseado no Windows usando:
  - Conexão de desktop remoto (RDP)
  - Windows Desktop Sharing (WDS)

A conexão remota com dispositivos gerenciados não é suportada ao acessar o Kaspersky Security Center Web Console a partir de um dispositivo executando o Microsoft Windows on Arm.

Para estabelecer uma conexão remota com um dispositivo, o seguintes item é necessário:

- utilitário klsctunnel

  O utilitário da Kaspersky é usado para criar um túnel de conexão entre um dispositivo gerenciado e o Servidor de Administração.

  O Kaspersky Security Center Linux possibilita o tunelamento de conexões TCP do Kaspersky Security Center Web Console pelo Servidor de Administração e, posteriormente, pelo Agente de Rede até uma porta específica em um dispositivo gerenciado. O tunelamento foi criado para conectar um aplicativo cliente em um dispositivo que tenha o Kaspersky Security Center Web Console instalado a uma porta TCP em um dispositivo gerenciado, quando não for possível estabelecer uma conexão direta entre o Kaspersky Security Center Web Console e o dispositivo de destino.

  A conexão em túnel entre um dispositivo cliente remoto e Servidor de Administração é necessária se a porta usada para a conexão ao Servidor de Administração não estiver disponível no dispositivo. A porta no dispositivo poderá estar indisponível nos seguintes casos:

  - O dispositivo remoto é conectado à uma rede local que usa o mecanismo NAT.
  - Um dispositivo remoto é parte da rede local, do Servidor de Administração, mas sua porta está fechada por um firewall.

Você pode baixar o utilitário no Kaspersky Security Center Web Console se uma conexão remota for estabelecida usando o Web Console ou manualmente no site da Kaspersky.

O utilitário klsctunnel é instalado no Servidor de Administração e é usado para todos os tipos de conexão remota, como RDP, VNC e WDS.

- Cliente RDP ou VNC

  Um cliente RDP ou VNC é instalado no dispositivo do Servidor de Administração. Esse cliente permite obter acesso remoto ao dispositivo gerenciado com o uso do endereço e a porta para a conexão local fornecida pelo utilitário klsctunnel.

  Uma conexão RDP com a sessão atual do desktop remoto do usuário é estabelecida sem o conhecimento do usuário. Depois que o administrador se conecta com a sessão, o usuário do dispositivo é desconectado da sessão sem receber nenhuma notificação.

- Windows Desktop Sharing (somente para dispositivos gerenciados baseados no Windows)

  Esse recurso permite se conectar com uma sessão existente em um dispositivo cliente sem desconectar o usuário nesta sessão. Nesse caso, o administrador e o usuário da sessão no dispositivo compartilham o acesso à área de trabalho.

  Ao conectar-se a uma sessão da área de trabalho remota existente, o usuário da sessão no dispositivo recebe uma solicitação para a conexão do administrador. Nenhuma informação sobre atividade remota no dispositivo e seus resultados serão salvos em relatórios criados pelo Kaspersky Security Center Linux.

  O administrador pode configurar uma auditoria da atividade do usuário em um dispositivo cliente remoto. Durante a auditoria, o aplicativo salva as informações sobre os arquivos que tenham sido abertos e/ou modificados pelo administrador no dispositivo cliente.

Acesso remoto de um dispositivo baseado em Linux com o Kaspersky Security Center Web Console para um dispositivo gerenciado baseado em Linux

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- No dispositivo gerenciado que executa Linux, o Agente de Rede versão 15.3 ou posterior está instalado.
- No dispositivo gerenciado que executa o Linux, o servidor RDP está instalado (caso se conecte ao dispositivo gerenciado usando a Conexão de ambiente de trabalho remoto).
- No dispositivo gerenciado que executa Linux, o servidor VNC é instalado (caso se conecte ao dispositivo gerenciado com o uso da Computação em Rede Virtual).
- A porta para tunelamento de conexões RDP está aberta (a opção **Porta aberta para tunelamento de conexões RDP** está ativada na seção **Portas de conexão** da janela Propriedades do Servidor de Administração).

- O administrador tem o direito de **Iniciar sessões RDP** para estabelecer conexões RDP (caso se conecte com o dispositivo gerenciado com o uso da Conexão de Desktop Remoto).

- O administrador tem o direito de **Iniciar túnel** para estabelecer a conexão de túnel para o VNC (caso você se conecte ao dispositivo gerenciado por meio do Virtual Network Computing).

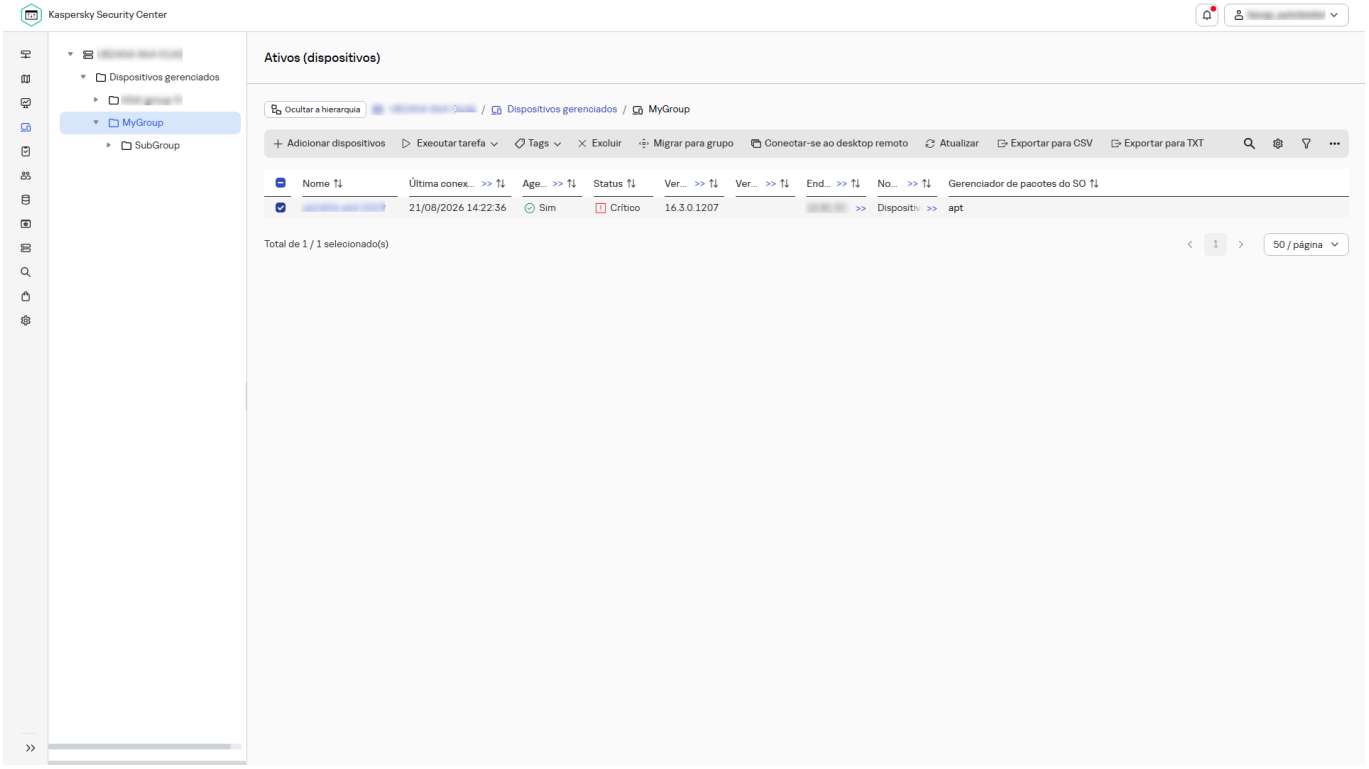
Para se conectar-se a um dispositivo gerenciado com Linux usando RDP ou VNC a partir de um dispositivo com Linux com o Kaspersky Security Center Web Console aberto:

1. No menu principal, vá para a seção **Gerenciamento de ativos** → **Dispositivos gerenciados** ou abra uma seleção de dispositivos.

2. Marque a caixa de seleção ao lado do dispositivo gerenciado ao qual deseja se conectar remotamente e clique no botão **Conectar-se ao desktop remoto**.

   A janela **Conectar-se ao desktop remoto** é aberta.

   Caso selecione vários dispositivos, um dispositivo móvel ou um dispositivo que execute macOS, o botão **Conectar-se ao desktop remoto** será desativado.



A lista de dispositivos gerenciados

3. Baixe o utilitário klsctunnel ao clicar no botão **Baixar** para executá-lo em seguida.

   Ao baixar o utilitário, leve em consideração o seguinte:

   - Para obter uma versão atualizada do utilitário klsctunnel, certifique-se de que o Servidor de Administração tenha acesso aos servidores de atualização Kaspersky.

     Você pode executar a tarefa *Baixar atualizações para o repositório do Servidor de Administração* e selecionar os servidores de atualização Kaspersky como uma fonte de atualizações. Se a tarefa for concluída com sucesso, o Servidor de Administração terá acesso aos servidores de atualização Kaspersky.

   - Caso o arquivo utilitário não esteja disponível para download, uma mensagem de erro será exibida. Neste caso, baixe o utilitário manualmente e, em seguida, coloque-o no dispositivo do Servidor de Administração no diretório /var/opt/kaspersky/klnagent_srv.

4. Na janela **Conectar-se ao desktop remoto**, especifique a porta de conexão. O número da porta padrão é 3389.

5. Gere um blob de texto com os parâmetros de conexão codificados ao clicar no botão **Gerar blob** e, em seguida, copie e cole o texto no campo correspondente no utilitário klsctunnel.

   Um blob contém as configurações necessárias para estabelecer uma conexão entre o Servidor de Administração e o dispositivo gerenciado. Um blob é válido por três minutos. Caso tenha expirado, gere um novo blob.

6. No utilitário klsctunnel, caso use um servidor proxy, especifique as configurações de conexão do servidor proxy.

   O utilitário klsctunnel exibe o endereço e a porta para a conexão local de um cliente de acesso remoto.

   O utilitário permite que o administrador feche a conexão do túnel. Caso a conexão do túnel seja fechada, a conexão atual com o desktop remoto será encerrada.

7. Execute um cliente de acesso remoto (RDP ou VNC) para conectá-lo com o dispositivo gerenciado com o uso do endereço e porta fornecidos pelo utilitário klsctunnel.

A conexão com o dispositivo gerenciado é estabelecida. A área de trabalho está disponível na janela do cliente de acesso remoto.

Acesso remoto de um dispositivo baseado em Linux com o Kaspersky Security Center Web Console para um dispositivo gerenciado baseado em Windows

Conexão de desktop remoto (RDP)

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- Uma conexão remota é permitida nas configurações do sistema operacional do dispositivo gerenciado.
- No dispositivo gerenciado que executa Windows, o Agente de Rede versão 13 ou posterior está instalado.
- O administrador tem o direito de **Iniciar sessões RDP** para estabelecer conexões RDP.
- A porta para tunelamento de conexões RDP está aberta (a opção **Porta aberta para tunelamento de conexões RDP** está ativada na seção **Portas de conexão** da janela Propriedades do Servidor de Administração).

Para conectar-se a um dispositivo gerenciado baseado em Windows usando RDP com o Kaspersky Security Center Web Console aberto em um dispositivo com Linux:

1. No menu principal, vá para a seção **Gerenciamento de ativos** → **Dispositivos gerenciados** ou abra uma seleção de dispositivos.

2. Marque a caixa de seleção ao lado do dispositivo gerenciado ao qual deseja se conectar remotamente e clique no botão **Conectar-se ao desktop remoto**.

   A janela **Conectar-se ao desktop remoto** é aberta.

   Caso selecione vários dispositivos, um dispositivo móvel ou um dispositivo que execute macOS, o botão **Conectar-se ao desktop remoto** será desativado.

3. Na janela **Conectar-se ao desktop remoto**, selecione o tipo de conexão **RDP**.

4. Caso uma conexão remota não seja permitida nas configurações do sistema operacional do dispositivo gerenciado, permita centralmente a conexão remota ao clicar no botão **Alterar configurações**.

   Caso as configurações sejam aplicadas corretamente, uma notificação será exibida. Além disso, no dispositivo gerenciado, na seção **Configurações** → **Sistema** → **Desktop Remoto**, a opção **Ativar Desktop Remoto** está ativada.

   Caso a conexão remota seja permitida nas configurações do sistema operacional do dispositivo gerenciado, o botão **Alterar configurações** não será exibido.

5. Baixe o utilitário klsctunnel ao clicar no botão **Baixar** para executá-lo em seguida.

   Ao baixar o utilitário, leve em consideração o seguinte:

   - Para obter uma versão atualizada do utilitário klsctunnel, certifique-se de que o Servidor de Administração tenha acesso aos servidores de atualização Kaspersky.

     Você pode executar a tarefa *Baixar atualizações para o repositório do Servidor de Administração* e selecionar os servidores de atualização Kaspersky como uma fonte de atualizações. Se a tarefa for concluída com sucesso, o Servidor de Administração terá acesso aos servidores de atualização Kaspersky.

   - Caso o arquivo utilitário não esteja disponível para download, uma mensagem de erro será exibida. Neste caso, baixe o utilitário manualmente e, em seguida, coloque-o no dispositivo do Servidor de Administração no diretório /var/opt/kaspersky/klnagent_srv.

6. Gere um texto blob com os parâmetros de conexão codificados ao clicar no botão **Gerar blob** e, em seguida, copie e cole o texto no campo correspondente no utilitário klsctunnel.

   Um blob contém as configurações necessárias para estabelecer uma conexão entre o Servidor de Administração e o dispositivo gerenciado. Um blob é válido por três minutos. Caso tenha expirado, gere um novo blob.

7. No utilitário klsctunnel, caso use um servidor proxy, especifique as configurações de conexão do servidor proxy.

   O utilitário klsctunnel exibe o endereço e a porta da conexão com o dispositivo remoto.

   O utilitário permite que o administrador feche a conexão do túnel. Caso a conexão do túnel seja fechada, a conexão atual com o desktop remoto será encerrada.

8. Execute um cliente RDP para conectá-lo ao dispositivo gerenciado por meio do endereço e da porta fornecidos pelo utilitário klsctunnel.

A conexão com o dispositivo gerenciado é estabelecida. A área de trabalho está disponível na janela do cliente RDP.

A conexão com a sessão de área de trabalho remota atual do usuário é estabelecida sem o conhecimento do usuário. Depois que o administrador se conecta com a sessão, o usuário do dispositivo é desconectado da sessão sem receber nenhuma notificação.

Sistema de Computação de Rede por Virtualização (VNC)

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- No dispositivo gerenciado que executa Windows, o Agente de Rede versão 13 ou posterior está instalado.
- No dispositivo gerenciado que executa o Windows, o servidor VNC está instalado.
- O administrador tem o direito de **Iniciar túnel** para estabelecer a conexão de túnel para VNC.
- A porta para tunelamento de conexões RDP está aberta (a opção **Porta aberta para tunelamento de conexões RDP** está ativada na seção **Portas de conexão** da janela Propriedades do Servidor de Administração).

Para conectar-se a um dispositivo gerenciado baseado em Windows usando VNC com o Kaspersky Security Center Web Console aberto em um dispositivo com Linux:

1. No menu principal, vá para a seção **Gerenciamento de ativos** → **Dispositivos gerenciados** ou abra uma seleção de dispositivos.
2. Marque a caixa de seleção ao lado do dispositivo gerenciado ao qual deseja se conectar remotamente e clique no botão **Conectar-se ao desktop remoto**.

   A janela **Conectar-se ao desktop remoto** é aberta.

   Caso selecione vários dispositivos, um dispositivo móvel ou um dispositivo que execute macOS, o botão **Conectar-se ao desktop remoto** será desativado.
3. Na janela **Conectar-se ao desktop remoto**, selecione o tipo de conexão **VNC**.
4. Baixe o utilitário klsctunnel ao clicar no botão **Baixar** para executá-lo em seguida.

   Caso o arquivo utilitário não esteja disponível para download, uma mensagem de erro será exibida. Neste caso, baixe manualmente o utilitário.
5. Na janela **Conectar-se ao desktop remoto**, especifique a porta de conexão VNC. O número da porta padrão é 5900.
6. Gere um blob de texto com os parâmetros de conexão codificados ao clicar no botão **Gerar blob** e, em seguida, copie e cole o texto no campo correspondente no utilitário klsctunnel.

   Um blob contém as configurações necessárias para estabelecer uma conexão entre o Servidor de Administração e o dispositivo gerenciado. Um blob é válido por três minutos. Caso tenha expirado, gere um novo blob.
7. No utilitário klsctunnel, caso use um servidor proxy, especifique as configurações de conexão do servidor proxy.

   O utilitário klsctunnel exibe o endereço e porta para a conexão local do cliente VNC.

   O utilitário permite que o usuário remoto feche a conexão do túnel. Caso a conexão do túnel seja fechada, a conexão atual com o desktop remoto será encerrada.
8. Execute um cliente VNC para conectá-lo com o dispositivo gerenciado com o uso do endereço e porta fornecidos pelo utilitário klsctunnel.

A conexão com o dispositivo gerenciado é estabelecida. O desktop está disponível na janela do cliente VNC.

Acesso remoto de um dispositivo baseado em Windows com o Kaspersky Security Center Web Console para um dispositivo gerenciado baseado em Linux

Conexão de desktop remoto (RDP)

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- No dispositivo gerenciado que executa o Linux, o servidor RDP está instalado.
- No dispositivo gerenciado que executa Linux, o Agente de Rede versão 15.3 ou posterior está instalado.
- O administrador tem o direito de **Iniciar sessões RDP** para estabelecer conexões RDP.
- A porta para tunelamento de conexões RDP está aberta (a opção **Porta aberta para tunelamento de conexões RDP** está ativada na seção **Portas de conexão** da janela Propriedades do Servidor de Administração).

Para conectar-se a um dispositivo gerenciado baseado em Linux usando RDP com o Kaspersky Security Center Web Console aberto em um dispositivo com Windows:

1. No menu principal, vá para a seção **Gerenciamento de ativos** → **Dispositivos gerenciados** ou abra uma seleção de dispositivos.
2. Marque a caixa de seleção ao lado do dispositivo gerenciado ao qual deseja se conectar remotamente e clique no botão **Conectar-se ao desktop remoto**.

   A janela **Conectar-se ao desktop remoto** é aberta.

   Caso selecione vários dispositivos, um dispositivo móvel ou um dispositivo que execute macOS, o botão **Conectar-se ao desktop remoto** será desativado.
3. Na janela **Conectar-se ao desktop remoto**, selecione o tipo de conexão **RDP**.
4. Baixe o utilitário klsctunnel ao clicar no botão **Baixar** para executá-lo em seguida.

   Ao baixar o utilitário, leve em consideração o seguinte:

   - Para obter uma versão atualizada do utilitário klsctunnel, certifique-se de que o Servidor de Administração tenha acesso aos servidores de atualização Kaspersky.

     Você pode executar a tarefa *Baixar atualizações para o repositório do Servidor de Administração* e selecionar os servidores de atualização Kaspersky como uma fonte de atualizações. Se a tarefa for concluída com sucesso, o Servidor de Administração terá acesso aos servidores de atualização Kaspersky.
   - Caso o arquivo utilitário não esteja disponível para download, uma mensagem de erro será exibida. Neste caso, baixe o utilitário manualmente e, em seguida, coloque-o no dispositivo do Servidor de Administração no diretório /var/opt/kaspersky/klnagent_srv.

5. Gere um texto blob com os parâmetros de conexão codificados ao clicar no botão **Gerar blob** e, em seguida, copie e cole o texto no campo correspondente no utilitário klsctunnel.

   Um blob contém as configurações necessárias para estabelecer uma conexão entre o Servidor de Administração e o dispositivo gerenciado. Um blob é válido por três minutos. Caso tenha expirado, gere um novo blob.

6. No utilitário klsctunnel, caso use um servidor proxy, especifique as configurações de conexão do servidor proxy.

   Para fazer isso, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão.

7. Clique no botão **Abrir porta**.

   A janela de login da Conexão de Área de Trabalho Remota é aberta.

8. Especifique as credenciais da conta com a qual ocorre a conexão com o Kaspersky Security Center Web Console e estabeleça conexão com o dispositivo gerenciado.

   O utilitário klsctunnel exibe o endereço e a porta da conexão com o dispositivo remoto.

   O utilitário permite que o administrador feche a conexão do túnel. Caso a conexão do túnel seja fechada, a conexão atual com o desktop remoto será encerrada.

Quando a conexão com o dispositivo for estabelecida, a área de trabalho ficará disponível na janela Conexão remota do Microsoft Windows.

A conexão com a sessão de área de trabalho remota atual do usuário é estabelecida sem o conhecimento do usuário. Depois que o administrador se conecta com a sessão, o usuário do dispositivo é desconectado da sessão sem receber nenhuma notificação.

Sistema de Computação de Rede por Virtualização (VNC)

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- No dispositivo gerenciado que executa Linux, o Agente de Rede versão 15.3 ou posterior está instalado.
- No dispositivo gerenciado que executa o Linux, o servidor VNC está instalado.
- O administrador tem o direito de **Iniciar túnel** para estabelecer a conexão de túnel para VNC.
- A porta para tunelamento de conexões RDP está aberta (a opção **Porta aberta para tunelamento de conexões RDP** está ativada na seção **Portas de conexão** da janela Propriedades do Servidor de Administração).

Para conectar-se a um dispositivo gerenciado baseado em Linux usando VNC com o Kaspersky Security Center Web Console aberto em um dispositivo com Windows:

1. No menu principal, vá para a seção **Gerenciamento de ativos** → **Dispositivos gerenciados** ou abra uma seleção de dispositivos.

2. Marque a caixa de seleção ao lado do dispositivo gerenciado ao qual deseja se conectar remotamente e clique no botão **Conectar-se ao desktop remoto**.

   A janela **Conectar-se ao desktop remoto** é aberta.

Caso selecione vários dispositivos, um dispositivo móvel ou um dispositivo que execute macOS, o botão **Conectar-se ao desktop remoto** será desativado.

3. Na janela **Conectar-se ao desktop remoto**, selecione o tipo de conexão **VNC**.

4. Baixe o utilitário klsctunnel ao clicar no botão **Baixar** para executá-lo em seguida.

   Caso o arquivo utilitário não esteja disponível para download, uma mensagem de erro será exibida. Neste caso, baixe manualmente o utilitário.

5. Na janela **Conectar-se ao desktop remoto**, especifique a porta de conexão VNC. O número da porta padrão é 5900.

6. Gere um blob de texto com os parâmetros de conexão codificados ao clicar no botão **Gerar blob** e, em seguida, copie e cole o texto no campo correspondente no utilitário klsctunnel.

   Um blob contém as configurações necessárias para estabelecer uma conexão entre o Servidor de Administração e o dispositivo gerenciado. Um blob é válido por três minutos. Caso tenha expirado, gere um novo blob.

7. No utilitário klsctunnel, caso use um servidor proxy, especifique as configurações de conexão do servidor proxy.

   Para fazer isso, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão.

8. Clique no botão **Abrir porta**.

   O utilitário klsctunnel exibe o endereço e porta para a conexão local do cliente VNC.

   O utilitário permite que o usuário remoto feche a conexão do túnel. Caso a conexão do túnel seja fechada, a conexão atual com o desktop remoto será encerrada.

9. Execute um cliente VNC para conectá-lo com o dispositivo gerenciado com o uso do endereço e porta fornecidos pelo utilitário klsctunnel.

A conexão com o dispositivo gerenciado é estabelecida. O desktop está disponível na janela do cliente VNC.

Acesso remoto de um dispositivo baseado em Windows com o Kaspersky Security Center Web Console para um dispositivo gerenciado baseado em Windows

Conexão de desktop remoto (RDP)

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- No dispositivo gerenciado que executa Windows, o Agente de Rede versão 13 ou posterior está instalado.
- O administrador tem o direito de **Iniciar sessões RDP** para estabelecer conexões RDP.

- A porta para tunelamento de conexões RDP está aberta (a opção **Porta aberta para tunelamento de conexões RDP** está ativada na seção **Portas de conexão** da janela Propriedades do Servidor de Administração).

- Uma conexão remota é permitida nas configurações do sistema operacional do dispositivo gerenciado.

Para conectar-se a um dispositivo gerenciado baseado no Windows usando RDP com o Kaspersky Security Center Web Console aberto em um dispositivo com Windows:

1. No menu principal, vá para a seção **Gerenciamento de ativos** → **Dispositivos gerenciados** ou abra uma seleção de dispositivos.

2. Marque a caixa de seleção ao lado do dispositivo gerenciado ao qual deseja se conectar remotamente e clique no botão **Conectar-se ao desktop remoto**.

   A janela **Conectar-se ao desktop remoto** é aberta.

   Caso selecione vários dispositivos, um dispositivo móvel ou um dispositivo que execute macOS, o botão **Conectar-se ao desktop remoto** será desativado.

3. Na janela **Conectar-se ao desktop remoto**, selecione o tipo de **Conexão do desktop remoto**.

4. Caso uma conexão remota não seja permitida nas configurações do sistema operacional do dispositivo gerenciado, permita centralmente a conexão remota ao clicar no botão **Alterar configurações**.

   Caso as configurações sejam aplicadas corretamente, uma notificação será exibida. Além disso, no dispositivo gerenciado, na seção **Configurações** → **Sistema** → **Desktop Remoto**, a opção **Ativar Desktop Remoto** está ativada.

   Caso a conexão remota seja permitida nas configurações do sistema operacional do dispositivo gerenciado, o botão **Alterar configurações** não será exibido.

5. Baixe o utilitário klsctunnel ao clicar no botão **Baixar** para executá-lo em seguida.

   Ao baixar o utilitário, leve em consideração o seguinte:

   - Para obter uma versão atualizada do utilitário klsctunnel, certifique-se de que o Servidor de Administração tenha acesso aos servidores de atualização Kaspersky.

     Você pode executar a tarefa *Baixar atualizações para o repositório do Servidor de Administração* e selecionar os servidores de atualização Kaspersky como uma fonte de atualizações. Se a tarefa for concluída com sucesso, o Servidor de Administração terá acesso aos servidores de atualização Kaspersky.

   - Caso o arquivo utilitário não esteja disponível para download, uma mensagem de erro será exibida. Neste caso, baixe o utilitário manualmente e, em seguida, coloque-o no dispositivo do Servidor de Administração no diretório /var/opt/kaspersky/klnagent_srv.

6. Gere um texto blob com os parâmetros de conexão codificados ao clicar no botão **Gerar blob** e, em seguida, copie e cole o texto no campo correspondente no utilitário klsctunnel.

   Um blob contém as configurações necessárias para estabelecer uma conexão entre o Servidor de Administração e o dispositivo gerenciado. Um blob é válido por três minutos. Caso tenha expirado, gere um novo blob.

7. No utilitário klsctunnel, caso use um servidor proxy, especifique as configurações de conexão do servidor proxy.

   Para fazer isso, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão.

8. Clique no botão **Abrir porta**.

   A janela de login da Conexão de Área de Trabalho Remota é aberta.

9. Especifique as credenciais da conta com a qual ocorre a conexão com o Kaspersky Security Center Web Console e estabeleça conexão com o dispositivo gerenciado.

   O utilitário klsctunnel exibe o endereço e a porta da conexão com o dispositivo remoto.

   O utilitário permite que o administrador feche a conexão do túnel. Caso a conexão do túnel seja fechada, a conexão atual com o desktop remoto será encerrada.

Quando a conexão com o dispositivo for estabelecida, a área de trabalho ficará disponível na janela Conexão remota do Microsoft Windows.

A conexão com a sessão de área de trabalho remota atual do usuário é estabelecida sem o conhecimento do usuário. Depois que o administrador se conecta com a sessão, o usuário do dispositivo é desconectado da sessão sem receber nenhuma notificação.

Windows Desktop Sharing (WDS)

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- No dispositivo gerenciado que executa Windows, o Agente de Rede versão 13 ou posterior está instalado.
- O administrador tem o direito de **Conectar a sessões RDP existentes** para estabelecer a conexão WDS.
- O licenciamento para Gerenciamento de patches e vulnerabilidades está disponível.
- Microsoft Windows Vista ou mais recente instalado na estação de trabalho do administrador. O tipo de sistema operacional do dispositivo que hospeda o Servidor de Administração não impõe restrições à conexão através do Compartilhamento da área de trabalho do Windows.

  Verifique se o recurso Windows Desktop Sharing está incluído na sua edição do Windows e se a chave CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} existe no Registro do Windows.
- O Microsoft Windows Vista ou mais recente está instalado no dispositivo cliente.

Para conectar-se a um dispositivo gerenciado baseado em Windows usando VNC com o Kaspersky Security Center Web Console aberto em um dispositivo com Windows:

1. No menu principal, vá para a seção **Gerenciamento de ativos** → **Dispositivos gerenciados** ou abra uma seleção de dispositivos.
2. Marque a caixa de seleção ao lado do dispositivo gerenciado ao qual deseja se conectar remotamente e clique no botão **Conectar-se ao desktop remoto**.

   A janela **Conectar-se ao desktop remoto** é aberta.

   Caso selecione vários dispositivos, um dispositivo móvel ou um dispositivo que execute macOS, o botão **Conectar-se ao desktop remoto** será desativado.
3. Na janela **Conectar-se ao desktop remoto**, selecione o tipo de conexão **Windows Desktop Sharing**.

   Caso o licenciamento de Gerenciamento de patches e vulnerabilidades não esteja disponível, uma mensagem de erro será exibida.

4. Baixe o utilitário klsctunnel ao clicar no botão **Baixar** para executá-lo em seguida.

   Caso o arquivo utilitário não esteja disponível para download, uma mensagem de erro será exibida. Neste caso, baixe manualmente o utilitário.

5. Na lista de sessões de usuário disponíveis e ativas na seleção de dispositivos, selecione a sessão com a qual deseja se conectar.

   O usuário remoto deve permitir a conexão. Caso o usuário remoto se recuse a conectar ou caso não permita a conexão durante o período de tempo limite, uma mensagem de erro será exibida.

6. Gere um blob de texto com os parâmetros de conexão codificados ao clicar no botão **Gerar blob** e, em seguida, copie e cole o texto no campo correspondente no utilitário klsctunnel.

   Um blob contém as configurações necessárias para estabelecer uma conexão entre o Servidor de Administração e o dispositivo gerenciado. Um blob é válido por três minutos. Caso tenha expirado, gere um novo blob.

7. No utilitário klsctunnel, caso use um servidor proxy, especifique as configurações de conexão do servidor proxy.

   Para fazer isso, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão.

8. Clique no botão **Abrir porta**.

   O utilitário klsctunnel exibe o endereço e porta para a conexão local do cliente VNC.

   O utilitário permite que o usuário remoto feche a conexão do túnel. Caso a conexão do túnel seja fechada, a conexão atual com o desktop remoto será encerrada.

O compartilhamento da área de trabalho é iniciado em uma nova janela. Caso queira interagir com o dispositivo, clique no ícone Menu () no canto superior esquerdo da janela e selecione **Modo interativo**.

Gerenciamento de Dispositivos Móveis

O gerenciamento da proteção de dispositivos móveis por meio do Kaspersky Security Center é executado usando o recurso de Gerenciamento de Dispositivos Móveis. Você precisa adicionar uma chave de licença em cada dispositivo móvel para ativar o aplicativo de proteção. Se você pretende gerenciar dispositivos móveis que pertencem a funcionários da sua organização, ative e configure o Gerenciamento de Dispositivos Móveis.

O Gerenciamento de Dispositivos Móveis permite gerenciar os dispositivos Android e iOS dos profissionais. A proteção é fornecida pelo aplicativo Kaspersky Endpoint Security for Android e pelo sistema de gerenciamento de dispositivos iOS instalado nos dispositivos móveis. Esses aplicativos móveis garantem a proteção de dispositivos móveis contra ameaças da Web, vírus e outros programas que representam riscos. Para gerenciamento centralizado por meio Kaspersky Security Center Web Console, você deve instalar os seguintes plugins de gerenciamento da web no dispositivo onde o Kaspersky Security Center Web Console está instalado:

- Kaspersky Mobile Devices Protection and Management

  O plug-in do Kaspersky Mobile Devices Protection and Management permite gerenciar dispositivos que executam Android e iOS no Kaspersky Security Center Web Console.

- Configurações do Servidor de MDM do iOS

  O plug-in de configurações do Servidor de MDM do iOS possibilita definir as configurações do servidor de MDM do iOS usado para conectar dispositivos iOS ao Servidor de Administração e gerenciar dispositivos iOS.

Para obter informações sobre a implementação de proteção e gerenciamento de dispositivos móveis, consulte a ajuda do Kaspersky Security for Mobile e a ajuda do Kaspersky Secure Mobility Management.

Usar o Firebase Cloud Messaging

Para garantir a entrega oportuna de comandos para dispositivos Android, o Kaspersky Security Center Linux usa o mecanismo de notificações push. As notificações push são trocadas entre os dispositivos Android e o Servidor de Administração por meio do Firebase Cloud Messaging (aqui referido como FCM). No Kaspersky Security Center Web Console, é possível especificar as configurações do Firebase Cloud Messaging para conectar dispositivos Android ao serviço.

Para recuperar as configurações do Firebase Cloud Messaging, é necessário ter uma conta do Google.

Para ativar o uso do FCM:

1. Na janela principal do Kaspersky Security Center Web Console, selecione **Gerenciamento de ativos** → **Mobile** → **Devices**.
2. Abra o menu de 3 pontos (⋮) e selecione **Forced Android device synchronization**.
3. No campo **Firebase project number**, especifique a ID do remetente do FCM.
4. No campo **Private key**, selecione o arquivo de chave privada.

   Na próxima sincronização com o Servidor de Administração, os dispositivos Android serão conectados com o Firebase Cloud Messaging.

Ao alternar para um projeto diferente do Firebase, é necessário aguardar 10 minutos para que o FCM seja retomado.

O serviço FCM é executado nas seguintes faixas de endereços:

- Do dispositivo Android, o acesso é necessário às portas 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) e 5230 (HTTPS) dos seguintes endereços:
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - Todos dos endereços IP listados no ASN da Google de 15169
- No Servidor de Administração, o acesso é necessário à porta 443 (HTTPS) dos seguintes endereços:
  - fcm.googleapis.com
  - Todos dos endereços IP listados no ASN da Google de 15169

Caso as configurações do servidor proxy tenham sido especificadas nas propriedades do Servidor de Administração no Kaspersky Security Center Web Console, elas serão usadas para a interação com o FCM.

Como configurar o FCM: obter o ID do remetente e o arquivo de chave privada

Para configurar o FCM:

1. Registre-se no portal do Google.
2. Acesse o Console do Firebase.
3. Execute uma das seguintes ações:
   - Para criar um novo projeto, clique em **Criar um projeto** e siga as instruções na tela.
   - Abra um projeto existente.
4. Clique no ícone de engrenagem e escolha **Configurações do projeto**.
   A janela **Configurações do projeto** é aberta.
5. Selecione a guia **Mensagens na nuvem**.
6. Obtenha o ID do remetente relevante no campo **ID do remetente** na seção **Firebase Cloud Messaging API (V1)**.
7. Selecione a guia **Contas de serviço** e clique em **Gerar nova chave privada**.
8. Na janela exibida, clique em **Gerar chave** para gerar e baixar um arquivo de chave privada.

O Firebase Cloud Messaging agora está configurado.

Integração com a infraestrutura de chaves públicas

É possível integrar a emissão de certificados com a Autoridade de Certificação (CA) da Microsoft por meio da Infraestrutura de Chaves Públicas (PKI). A integração com a PKI visa simplificar a emissão de certificados de usuários de domínio pelo Servidor de Administração. Após a integração, os certificados são emitidos automaticamente.

Para obter informações detalhadas sobre como configurar a integração com a PKI para emitir certificados, consulte a Ajuda do Kaspersky Secure Mobility Management.

Você pode executar a integração da PKI com as configurações especificadas e atribuir a PKI para atuar como a fonte de certificados para tipos específicos de certificados. As configurações de integração da PKI possibilitam definir o modelo padrão individual para todos os tipos de certificados.

As especificidades do uso da integração da PKI para emitir certificados:

- A integração da PKI é desativada por padrão. Para obter informações detalhadas sobre como ativar a PKI e definir suas configurações, consulte a Ajuda do Kaspersky Secure Mobility Management.

- Os certificados são emitidos usando o Agente de Rede para Windows. Isso garante a integração entre o Servidor de Administração e a CA da Microsoft. Como pode haver vários dispositivos com o Agente de Rede instalado, você pode especificar o dispositivo que se conectará à CA da Microsoft nas **Issuance rules**. Esse dispositivo deve ter um Certificado de agente de inscrição (EA) instalado no repositório de certificados da conta sob a qual a integração com a PKI é executada. O certificado é emitido pelo administrador da CA do domínio.

- A conta sob a qual a integração com a PKI é executada deve ser um usuário de domínio e ter o direito de fazer *Logon como serviço*.

- O Kaspersky Security Center Linux pode funcionar somente com uma integração da PKI (CA da Microsoft) por vez.

Gerenciamento de grupos de administração

Esta seção fornece informações sobre como gerenciar grupos de administração.

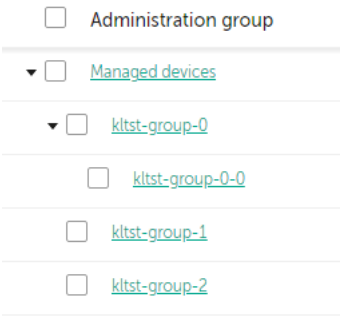
Você pode executar as seguintes ações nos grupos de administração:

- Adicione qualquer número de grupos aninhados de qualquer nível de hierarquia aos grupos de administração.
- Adicionar dispositivos aos grupos de administração.
- Altere a hierarquia de grupos de administração ao migrar dispositivos individuais e grupos inteiros para outros grupos.
- Remover grupos aninhados e dispositivos dos grupos de administração.
- Adicionar Servidores de Administração secundários e virtuais aos grupos de administração.
- Mover dispositivos cliente dos grupos de administração de um Servidor de Administração para aqueles de outro Servidor.
- Definir quais aplicativos Kaspersky que serão instalados automaticamente em dispositivos incluídos em um grupo.

Será possível executar essas ações somente se você tiver a permissão **Modificar** na área **Gerenciamento de grupos de administração** para os grupos de administração que deseja gerenciar (ou para o Servidor de Administração ao qual esses grupos pertencem).

Criação de grupos de administração

Imediatamente após a instalação do Kaspersky Security Center, a hierarquia dos grupos de administração contém apenas um grupo de administração chamado **Dispositivos gerenciados**. Ao criar uma hierarquia de grupos de administração, você poderá adicionar dispositivos e máquinas virtuais à pasta **Dispositivos gerenciados**, e adicionar grupos aninhados (veja a figura abaixo).

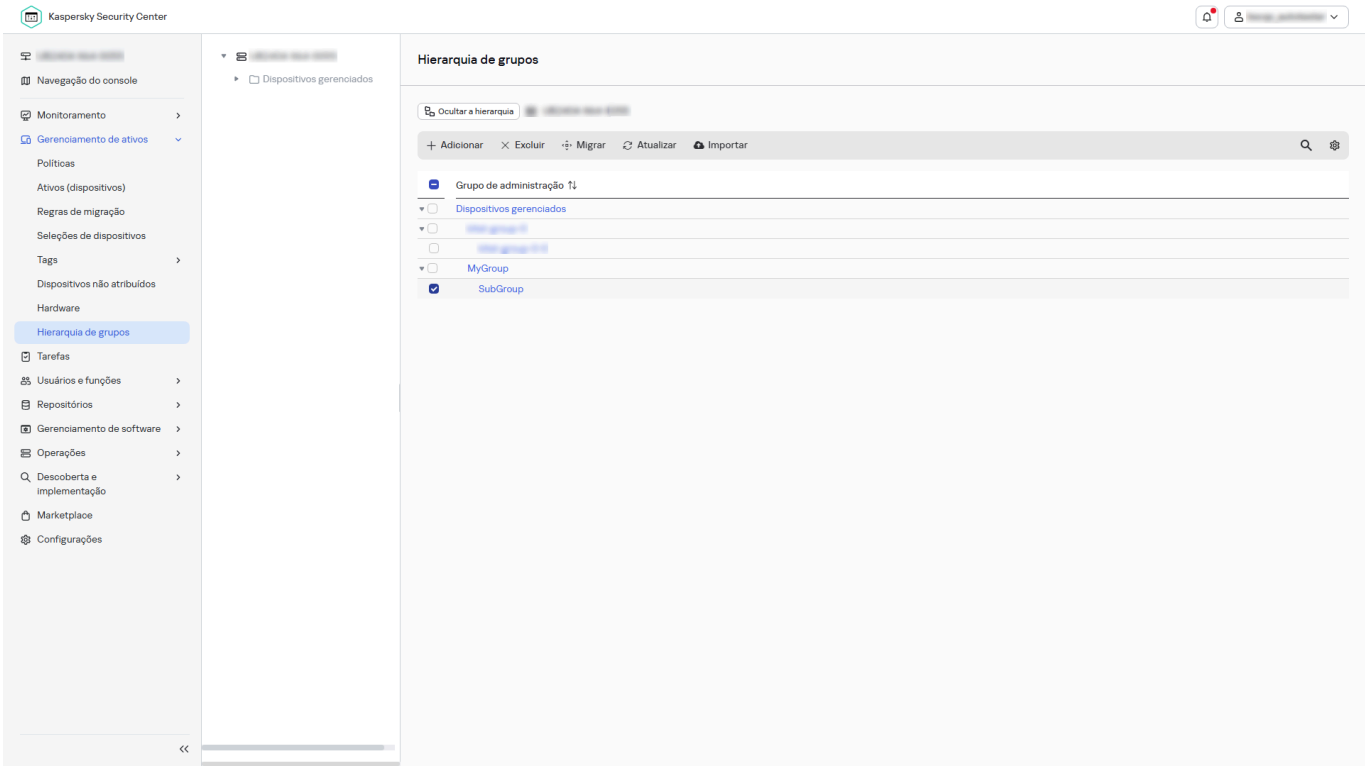


Exibir hierarquia de grupos de administração

Para criar um grupo de administração:

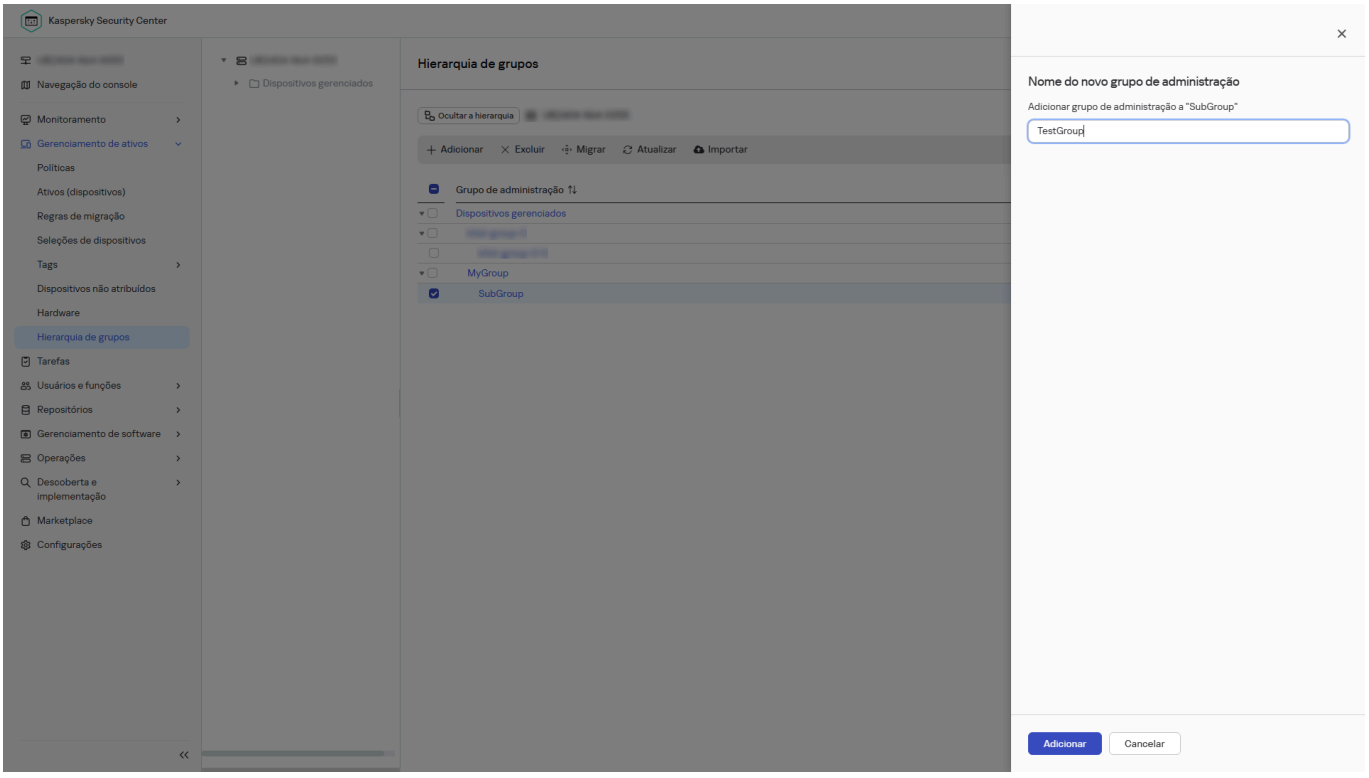
1. No menu principal, vá para **Gerenciamento de ativos** → **Hierarquia de grupos**.

2. Na estrutura do grupo de administração, selecione o grupo de administração que deve incluir o novo grupo de administração.



3. Clique em **Adicionar**.

4. Na janela **Nome do novo grupo de administração** que se abre, insira um nome para o grupo e clique no botão **Adicionar**.



Um novo grupo de administração com o nome especificado aparece na hierarquia dos grupos de administração.

Para criar a estrutura de grupos de administração:

1. No menu principal, vá para **Gerenciamento de ativos** → **Hierarquia de grupos**.
2. Clique em **Importar**.

O Assistente de nova estrutura de grupos de administração é iniciado. Siga as etapas do Assistente.

Instalação automática de aplicativos nos dispositivos em um grupo de administração

É possível especificar quais pacotes de instalação devem ser usados para a instalação remota automática de aplicativos da Kaspersky em dispositivos clientes em um grupo de administração.

Para configurar a instalação automática de aplicativos em dispositivos em um grupo de administração:

1. No menu principal, vá para **Gerenciamento de ativos** → **Hierarquia de grupos**.
2. Vá para as propriedades do grupo de administração desejado por uma das seguintes formas:
   - Clique no nome do grupo de administração.
   - Clique no botão **Mostrar a hierarquia** na parte superior da página. No painel de navegação exibido, passe o cursor do mouse sobre o nome do grupo desejado e clique no ícone de configurações (⚙).

   A janela Propriedades do grupo de administração é aberta.
3. Na janela de propriedades, vá para a guia **Instalação automática**.
4. Selecione os pacotes de instalação dos aplicativos a serem instalados nos dispositivos e clique no botão **Salvar**.

   Caso selecione vários pacotes de instalação do mesmo aplicativo que se diferenciem apenas nas versões, o pacote de instalação com a versão mais recente será salvo.

Depois de selecionar os pacotes de instalação, um grupo de tarefas para instalação dos aplicativos nos dispositivos no grupo de administração é criado para cada aplicativo. Estas tarefas são executadas nos dispositivos cliente imediatamente após serem adicionadas ao grupo de administração.

Mover grupos de administração

Você pode mover grupos de administração alojados dentro da hierarquia dos grupos.

Um grupo de administração é migrado juntamente com todos os grupos aninhados, Servidores de Administração secundários, dispositivos, políticas de grupo e tarefas. O sistema aplicará ao grupo todas as configurações que corresponderem a sua nova posição na hierarquia dos grupos de administração.

O nome do grupo deve ser único dentro de um nível da hierarquia. Se um grupo com o mesmo nome já existir na pasta para a qual você move o grupo de administração, você deve alterar o nome do último. Se você não tiver alterado o nome do grupo movido, um índice no formato **(<próximo número de sequência>)** é automaticamente adicionado ao seu nome após ser movido, por exemplo: **(1)**, **(2)**.

Não é possível renomear e mover o grupo **Dispositivos gerenciados**.

Para mover um grupo de administração para outro nível da hierarquia do grupo de administração:

1. No menu principal, acesse **Gerenciamento de ativos** → **Hierarquia de grupos** e marque a caixa de seleção ao lado do grupo de administração que deseja mover.
2. Clique no botão **Migrar** na barra de ferramentas.
3. Na janela que é aberta, selecione para onde deseja mover o grupo de administração, e então clique no botão **Migrar**.

A janela será fechada e o grupo de administração será movido para outro nível da hierarquia de grupos.

Exclusão de grupos de administração

Se você excluir um grupo de administração com Servidores de Administração secundários, grupos aninhados, dispositivos cliente, tarefas de grupo ou políticas criadas para esse grupo, todos eles também serão excluídos.

Antes de excluir um grupo de administração, você deve excluir todos os Servidores de Administração secundários, grupos aninhados e dispositivos cliente daquele grupo.

Para excluir um grupo de administração:

1. No menu principal, acesse **Gerenciamento de ativos** → **Hierarquia de grupos** e marque a caixa de seleção ao lado do grupo de administração que deseja excluir.
2. Clique no botão **Excluir** na barra de ferramentas.

O grupo de administração é excluído.

Implementação de aplicativos Kaspersky

Esta seção descreve a implementação de aplicativos da Kaspersky em dispositivos gerenciados, usando o Kaspersky Security Center Web Console.

Cenário: Verificando a implementação dos aplicativos Kaspersky

Este cenário explica como implementar aplicativos Kaspersky por meio do Kaspersky Security Center Web Console. É possível usar o assistente de início rápido, o Assistente de implementação da proteção ou concluir todas as etapas necessárias manualmente.

Os seguintes aplicativos estão disponíveis para implementação usando o Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

Fases

A implementação dos aplicativos da Kaspersky é feita em fases:

1. **Download do plugin de gerenciamento da web para o aplicativo**

   Esta etapa faz parte do Assistente de início rápido. Caso opte por não executar o assistente, baixe os plug-ins manualmente.

2. **Baixando e criando pacotes de instalação**

   Esta etapa faz parte do Assistente de início rápido.

   O assistente de início rápido permite baixar o pacote de instalação com o plug-in da Web de gerenciamento. Se você não selecionou esta opção ao executar o assistente, ou se não executou o assistente, deve baixar o pacote manualmente.

   Caso não consiga instalar os aplicativos da Kaspersky pelo Kaspersky Security Center Linux em alguns dispositivos, como em dispositivos de funcionários remotos, é possível criar pacotes de instalação independentes para aplicativos. Caso os pacotes autônomos sejam usados para instalar os aplicativos Kaspersky, não será preciso criar e executar uma tarefa de instalação remota, nem criar e configurar tarefas para o Kaspersky Endpoint Security for Windows.

   Como alternativa, é possível baixar os pacotes de distribuição do Agente de Rede e aplicativos de segurança pelo site da Kaspersky. Caso a instalação remota dos aplicativos não seja possível por algum motivo, é possível usar os pacotes de distribuição baixados para instalar os aplicativos localmente.

3. **Criação, configuração e execução da tarefa de instalação remota**

   Esta etapa faz parte do Assistente de implementação da proteção. Se optar por não executar o Assistente de implementação da proteção, você deverá criar e configurar essa tarefa manualmente.

Você também pode criar manualmente várias tarefas de instalação remotas para grupos de administração ou seleções de dispositivos diferentes. Você pode implementar versões diferentes de um aplicativo nessas tarefas.

Certifique-se de que todos os dispositivos na sua rede sejam descobertos; e execute a(s) tarefa(s) de instalação remotas.

Caso queira instalar o agente de rede em dispositivos com o sistema operacional SUSE Linux Enterprise Server 15, instale o pacote insserv-compat primeiro para configurar o agente de rede.

Se você deseja instalar o Agente de Rede em dispositivos que usam o sistema operacional RED OS 7.3.4 ou posterior ou MSVSPHERE 9.2 ou posterior, instale o pacote libxcrypt-compat para a função correta do Agente de Rede.

4. **Criação e configuração de tarefas**

   A tarefa de *Atualização* do Kaspersky Endpoint Security deve ser configurada.

   Essa etapa faz parte do assistente de início rápido: a tarefa é criada e configurada automaticamente com as configurações padrão. Se não tiver executado o assistente, você deverá criar essa tarefa manualmente e configurá-la manualmente. Caso use o assistente de início rápido, verifique e confirme se o cronograma da tarefa atende aos seus requisitos. (Por padrão, o início agendado da tarefa é definido como **Manualmente**, mas é possível escolher outra opção.)

5. **Criar políticas**

   Crie a política do Kaspersky Endpoint Security manualmente ou por meio do assistente de início rápido. Você pode usar as configurações padrão da política. Você também pode modificar as configurações padrão da política de acordo com suas necessidades a qualquer momento.

6. **Verificar os resultados**

   Certifique-se de que a implementação tenha sido concluída com sucesso: você tem políticas e tarefas para cada aplicativo, e esses aplicativos são instalados nos dispositivos gerenciados.

Resultados

A conclusão do cenário produz o seguinte:

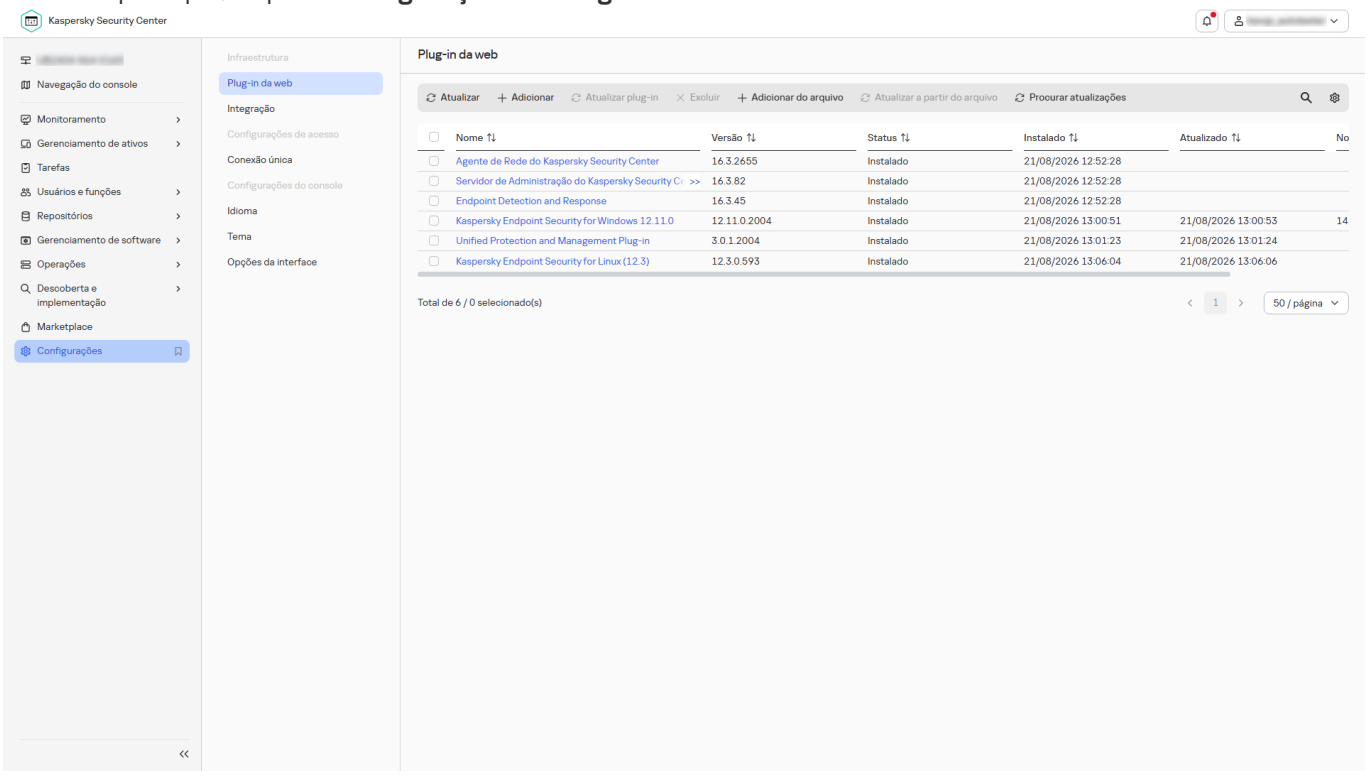
- Todas as políticas e tarefas necessárias dos aplicativos selecionados são criadas.
- As programações de tarefas são configuradas segundo as suas necessidades.
- Os aplicativos selecionados são implementados ou planejados para ser implementados nos dispositivos clientes selecionados.

Adicionando plugins de gerenciamento para aplicativos Kaspersky

Para implementar um aplicativo Kaspersky, como o Kaspersky Endpoint Security for Linux ou o Kaspersky Endpoint Security for Windows, você deve adicionar e instalar o plug-in da web para gerenciamento do aplicativo.

Para baixar um plug-in para gerenciamento de um aplicativo Kaspersky:

1. No menu principal, vá para **Configurações → Plug-in da web**.



A lista de plug-ins da web instalados

2. Na janela que se abre, clique no botão **Adicionar**.

   A lista de plugins disponíveis é exibida.

3. Na lista de plug-ins disponíveis, selecione aquele que deseja baixar (por exemplo, Kaspersky Endpoint Security for Linux) clicando no seu nome.

   Uma página de descrição de plugin é exibida.

4. Na página de descrição do plugin, clique em **Instalar o plug-in**.

5. Quando a instalação for concluída, clique em **OK**.

O plug-in da Web de gerenciamento é baixado com a configuração padrão e exibido na lista de plug-ins da Web de gerenciamento.

Você pode adicionar plugins e atualizar plugins baixados de um arquivo. É possível baixar plug-ins de gerenciamento da Web pelo site da Kaspersky.

Para baixar ou atualizar o plug-in da Web de gerenciamento de um arquivo:

1. No menu principal, vá para **Configurações → Plug-in da web**.

2. Especifique o arquivo do plugin e a assinatura do arquivo:

   - Clique em **Adicionar do arquivo** para baixar um plugin de um arquivo.

   - Clique em **Atualizar a partir do arquivo** para baixar uma atualização de um plugin de um arquivo.

3. Especifique o arquivo e a assinatura do arquivo.

4. Baixe os arquivos especificados.

O plug-in da Web de gerenciamento é baixado a partir do arquivo e exibido na lista de plug-ins da Web de gerenciamento.

Pacotes

O *pacote de instalação* é um conjunto de arquivos criados para instalação remota de um aplicativo da Kaspersky. O pacote de instalação contém um intervalo de configurações necessárias para instalar o aplicativo e colocá-lo em funcionamento imediatamente após a instalação. As configurações correspondem aos padrões do aplicativo. O pacote de instalação é criado usando arquivos com as extensões .kpd e .kud incluídas no kit de distribuição do aplicativo.

Os pacotes de Instalação são gerados com o uso dos seguintes métodos:

- Automaticamente, pelos pacotes de distribuição especificados, com base em *descritores* incluídos (arquivos com a extensão .kud que contêm regras para a instalação, análise de resultados e outras informações).

- Tendo como origem um arquivo compactado ZIP, CAB, TAR ou TAR.GZ para os aplicativos padrão ou compatíveis.

Os pacotes de instalação gerados são organizados hierarquicamente como pastas com subpastas e arquivos. Além do pacote de distribuição original, um pacote de instalação contém configurações editáveis (incluindo as configurações do instalador e as regras para processar os casos tal como necessidade de reiniciar o sistema operacional para concluir a instalação), assim como os módulos auxiliares secundários.

Os valores das configurações de instalação que seriam específicos para o aplicativo individual compatível podem ser definidos na interface do usuário do Kaspersky Security Center Web Console quando o pacote de instalação for criado. Ao executar a instalação remota de aplicativos usando as ferramentas do Kaspersky Security Center Linux, os pacotes de instalação são entregues aos dispositivos para que, ao executar o instalador de um aplicativo, todas as configurações definidas pelo administrador fiquem à disposição daquele aplicativo. Ao usar as ferramentas de terceiros para a instalação de aplicativos Kaspersky, você somente tem de assegurar a disponibilidade de todo o pacote de instalação no dispositivo, ou seja, a disponibilidade do pacote de distribuição e de suas configurações. Os pacotes de instalação são criados e armazenados pelo Kaspersky Security Center Linux em uma subpasta dedicada da pasta compartilhada.

Não especifique nenhum detalhe de contas privilegiadas nos parâmetros dos pacotes de instalação.

A implementação usando políticas de grupo do Microsoft Windows não é compatível.

Imediatamente após a instalação do Kaspersky Security Center Linux, alguns pacotes de instalação são automaticamente gerados; eles estão prontos para a instalação e incluem pacotes do Agente de Rede e pacotes de aplicativos de segurança para o Microsoft Windows.

Embora a chave de licença para um aplicativo possa ser definida nas propriedades de um pacote de instalação, é aconselhável evitar este método de distribuição da licença porque é fácil obter o acesso de leitura para pacotes de instalação. Você deve usar as chaves automaticamente distribuídas ou as tarefas de instalação para chaves de licença.

Download e criação de pacotes de instalação para aplicativos Kaspersky

Você poderá criar pacotes de instalação para aplicativos Kaspersky de servidores Web da Kaspersky se o Servidor de Administração tiver acesso à Internet.

Ao criar pacotes de instalação para instalar o aplicativo em dispositivos Windows, se você receber a mensagem **Ocorreu um erro. Tente fazer o download novamente**:

1. Crie o sinalizador RIUtilsArchiveDirUsed executando o seguinte comando:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Execute o seguinte comando para reiniciar o serviço do Servidor de Administração:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Baixe os módulos adicionais, "Arquivos para instalação remota via Kaspersky Security Center", no site da Kaspersky.

   Os arquivos baixados têm os seguintes nomes:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Não renomeie os arquivos comprimidos.

4. Coloque os arquivos no diretório /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

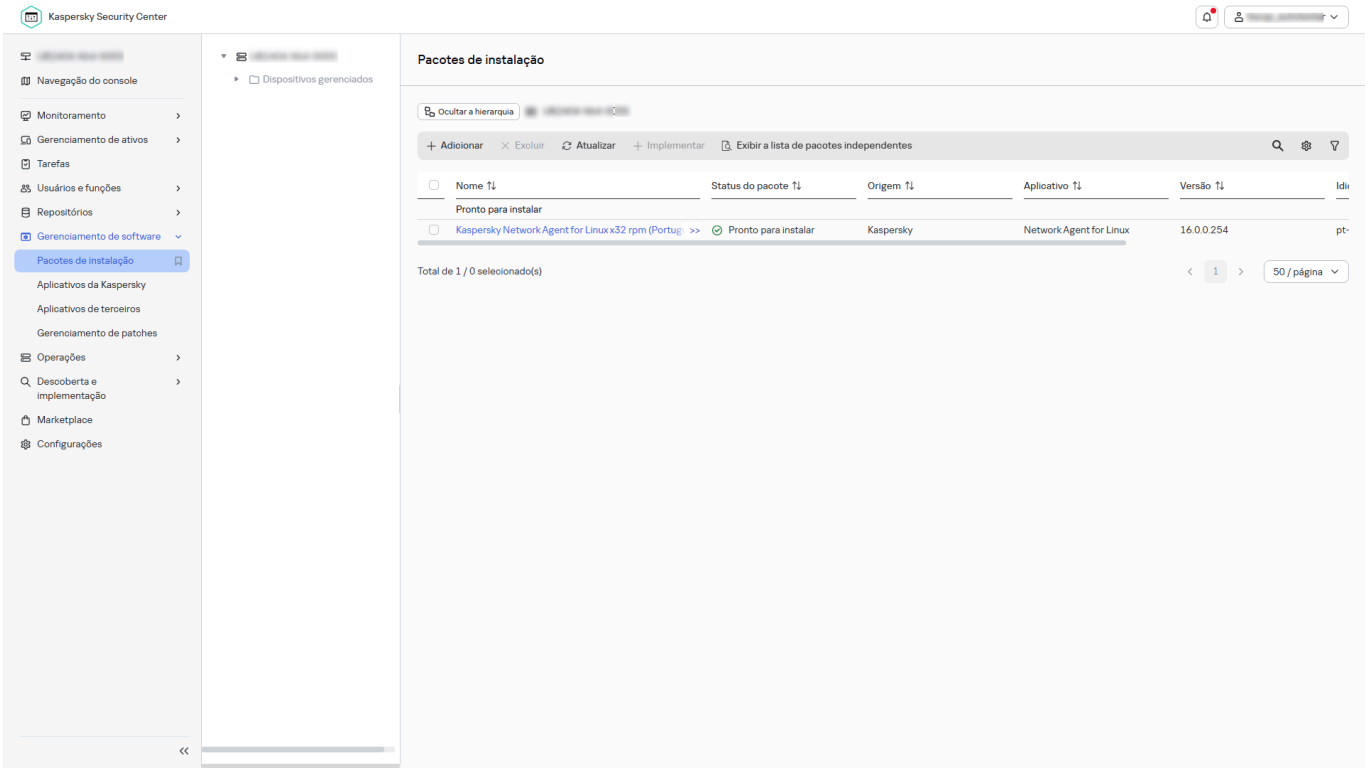
Agora você pode criar um pacote de instalação para instalar o aplicativo em dispositivos Windows.

Para baixar e criar o pacote de instalação para aplicativos Kaspersky:

1. No menu principal, vá para **Gerenciamento de software → Pacotes de instalação**.

   Você também pode visualizar as notificações sobre novos pacotes para aplicativos Kaspersky na lista de notificações na tela. Se houver notificações sobre um novo pacote, você poderá clicar no link ao lado da notificação e prosseguir para a lista de pacotes de instalação disponíveis.

Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

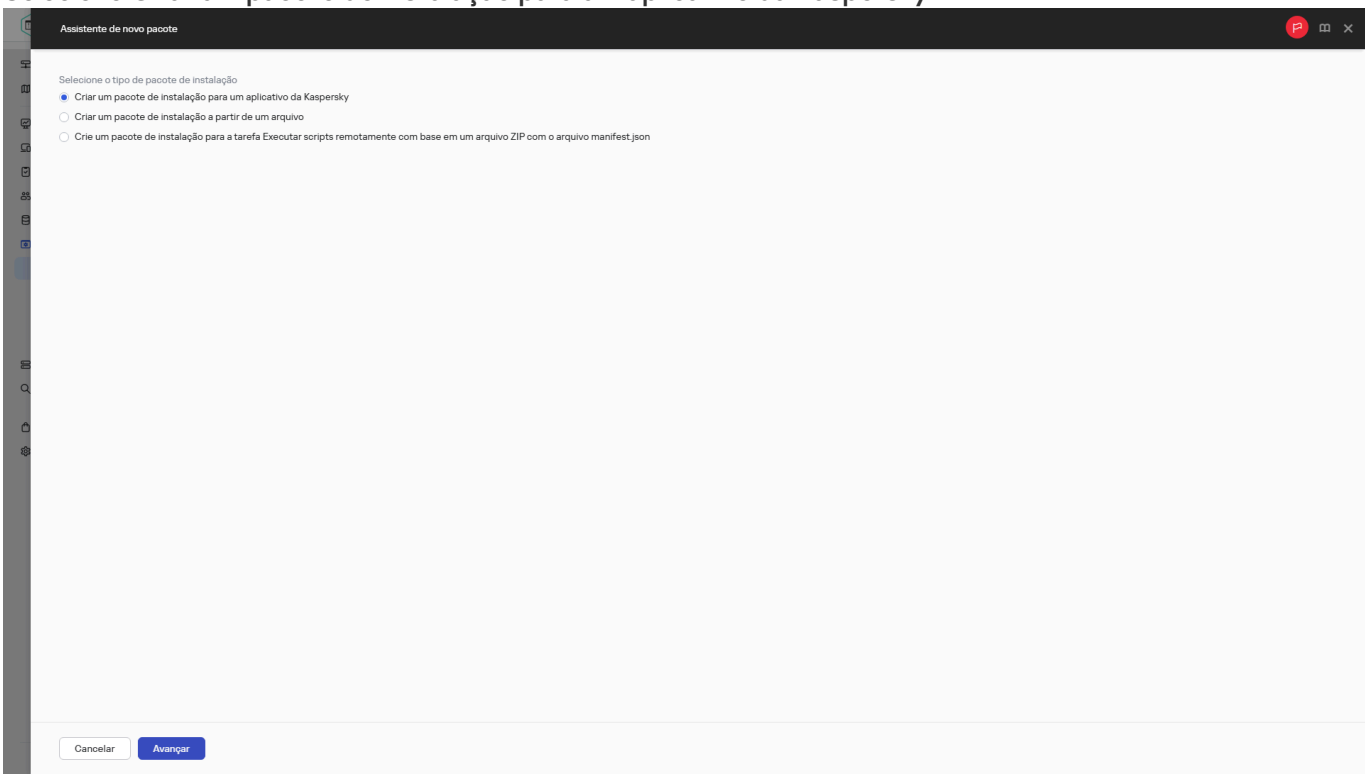


A lista de pacotes de instalação

2. Clique em **Adicionar**.

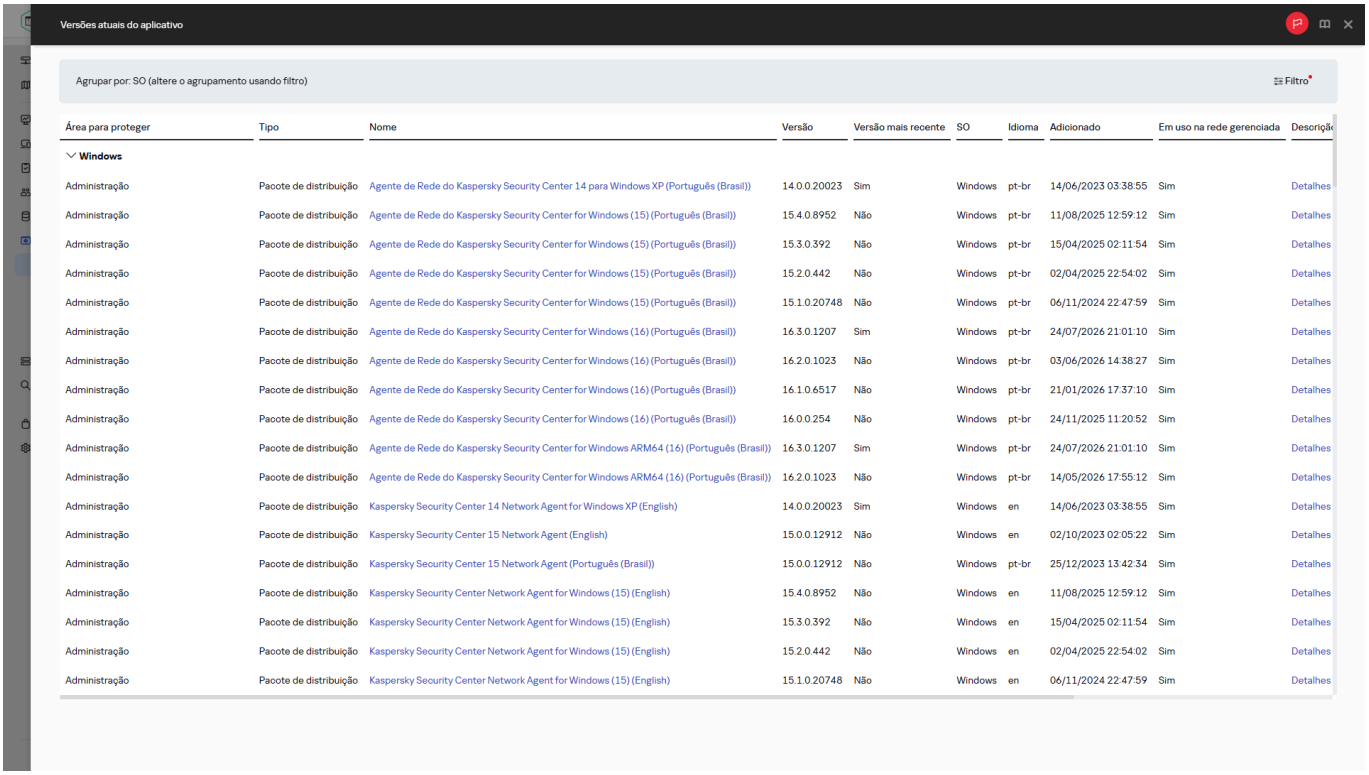
   O Assistente de novo pacote inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Selecione **Criar um pacote de instalação para um aplicativo da Kaspersky**.



Seleção do tipo de pacote de instalação

Uma lista dos pacotes de instalação disponíveis nos servidores da Web Kaspersky é exibida. A lista contém pacotes de instalação apenas para os aplicativos compatíveis com a versão atual do Kaspersky Security Center Linux. Por padrão, a lista mostra somente aplicativos com o idioma inglês e com o idioma que corresponde ao da interface. Para exibir outros idiomas, clique em **Filtrar** e defina as configurações de filtro.



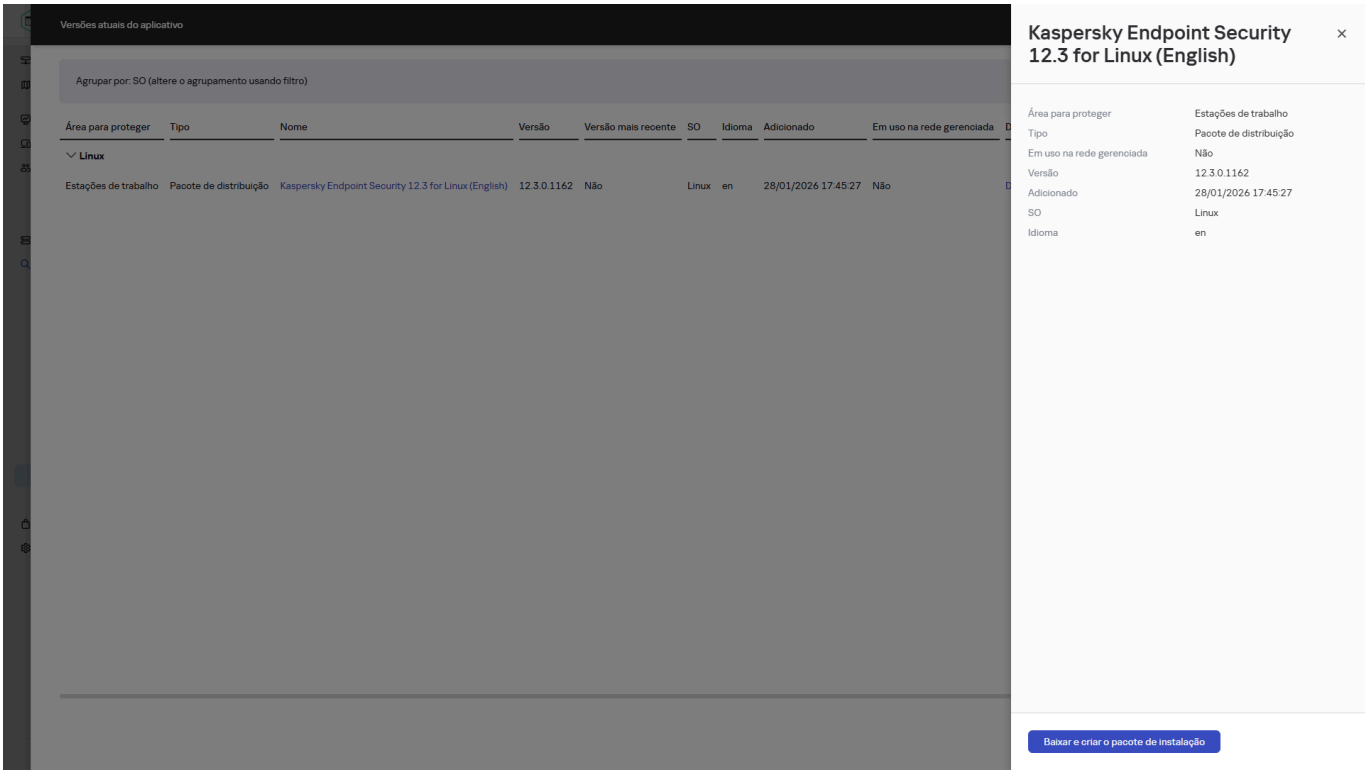
Área para proteger	Tipo	Nome	Versão	Versão mais recente	SO	Idioma	Adicionado	Em uso na rede gerenciada	Descriçã
Windows									
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center 14 para Windows XP (Português (Brasil))	14.0.0.20023	Sim	Windows	pt-br	14/06/2023 03:38:55	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows (15) (Português (Brasil))	15.4.0.8952	Não	Windows	pt-br	11/08/2025 12:59:12	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows (15) (Português (Brasil))	15.3.0.392	Não	Windows	pt-br	15/04/2025 02:11:54	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows (15) (Português (Brasil))	15.2.0.442	Não	Windows	pt-br	02/04/2025 22:54:02	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows (15) (Português (Brasil))	15.1.0.20748	Não	Windows	pt-br	06/11/2024 22:47:59	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows (16) (Português (Brasil))	16.3.0.1207	Sim	Windows	pt-br	24/07/2026 21:01:10	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows (16) (Português (Brasil))	16.2.0.1023	Não	Windows	pt-br	03/06/2026 14:38:27	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows (16) (Português (Brasil))	16.1.0.6517	Não	Windows	pt-br	21/01/2026 17:37:10	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows (16) (Português (Brasil))	16.0.0.254	Não	Windows	pt-br	24/11/2025 11:20:52	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows ARM64 (16) (Português (Brasil))	16.3.0.1207	Sim	Windows	pt-br	24/07/2026 21:01:10	Sim	Detalhes
Administração	Pacote de distribuição	Agente de Rede do Kaspersky Security Center for Windows ARM64 (16) (Português (Brasil))	16.2.0.1023	Não	Windows	pt-br	14/05/2026 17:55:12	Sim	Detalhes
Administração	Pacote de distribuição	Kaspersky Security Center 14 Network Agent for Windows XP (English)	14.0.0.20023	Sim	Windows	en	14/06/2023 03:38:55	Sim	Detalhes
Administração	Pacote de distribuição	Kaspersky Security Center 15 Network Agent (English)	15.0.0.12912	Não	Windows	en	02/10/2023 02:05:22	Sim	Detalhes
Administração	Pacote de distribuição	Kaspersky Security Center 15 Network Agent (Português (Brasil))	15.0.0.12912	Não	Windows	pt-br	25/12/2023 13:42:34	Sim	Detalhes
Administração	Pacote de distribuição	Kaspersky Security Center Network Agent for Windows (15) (English)	15.4.0.8952	Não	Windows	en	11/08/2025 12:59:12	Sim	Detalhes
Administração	Pacote de distribuição	Kaspersky Security Center Network Agent for Windows (15) (English)	15.3.0.392	Não	Windows	en	15/04/2025 02:11:54	Sim	Detalhes
Administração	Pacote de distribuição	Kaspersky Security Center Network Agent for Windows (15) (English)	15.2.0.442	Não	Windows	en	02/04/2025 22:54:02	Sim	Detalhes
Administração	Pacote de distribuição	Kaspersky Security Center Network Agent for Windows (15) (English)	15.1.0.20748	Não	Windows	en	06/11/2024 22:47:59	Sim	Detalhes

A lista de pacotes de distribuição disponíveis

4. Clique no nome de um pacote de instalação, por exemplo, Kaspersky Endpoint Security for Linux.

   Uma janela é exibida com informações sobre o pacote de instalação.

Se estiver em conformidade com as leis e os regulamentos aplicáveis, você poderá baixar e usar um pacote de instalação que inclui ferramentas criptográficas que implementam criptografia forte. Para baixar o pacote de instalação do Kaspersky Endpoint Security for Windows válido para as necessidades da sua organização, consulte a legislação do país em que os dispositivos clientes da sua organização estão localizados.



Baixar o pacote de instalação

5. Leia as informações e clique no botão **Baixar e criar o pacote de instalação**.

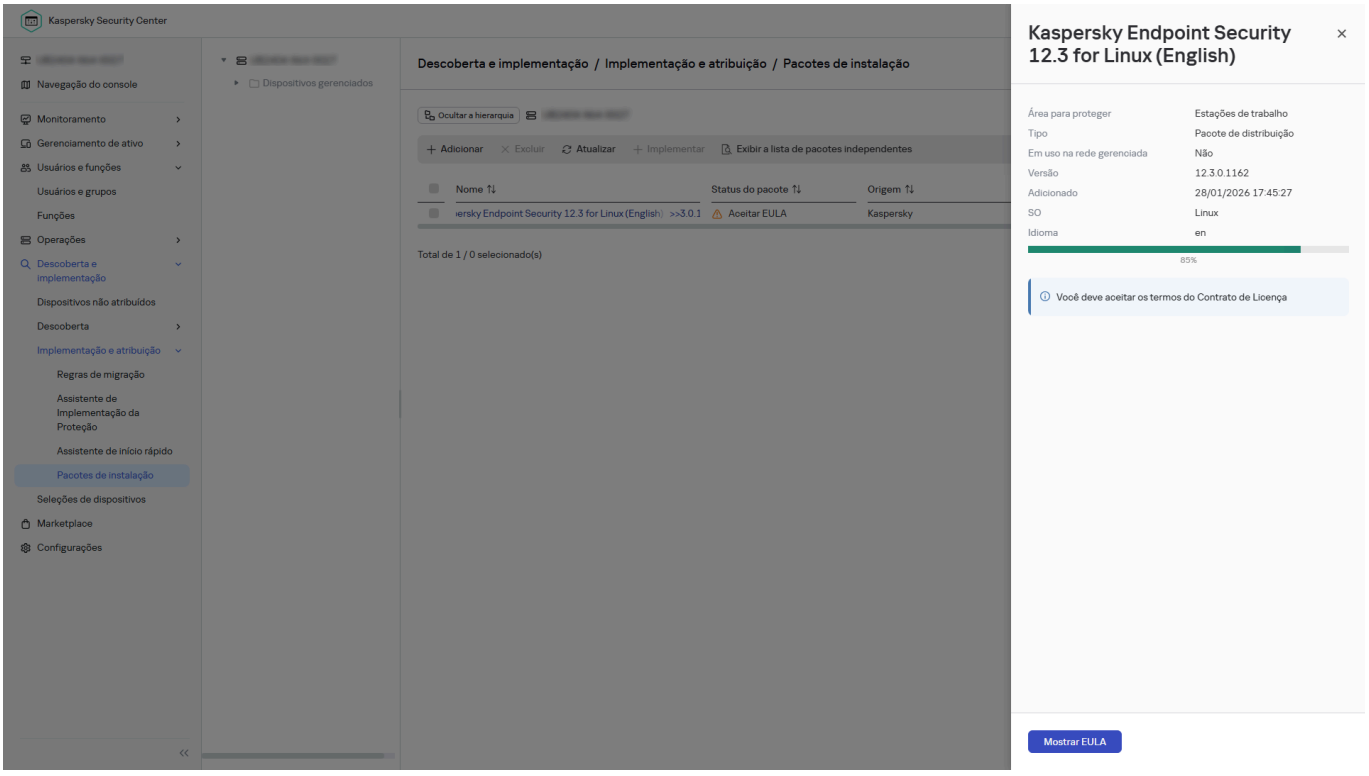
   Se um pacote de distribuição não puder ser convertido em um pacote de instalação, o botão **Baixar e criar o pacote de instalação** é exibido em vez da opção **Baixar o pacote de distribuição**.

Para alguns aplicativos da Kaspersky, o botão **Mostrar EULA** será exibido antes ou durante o processo de download. Se ele for exibido, faça o seguinte:

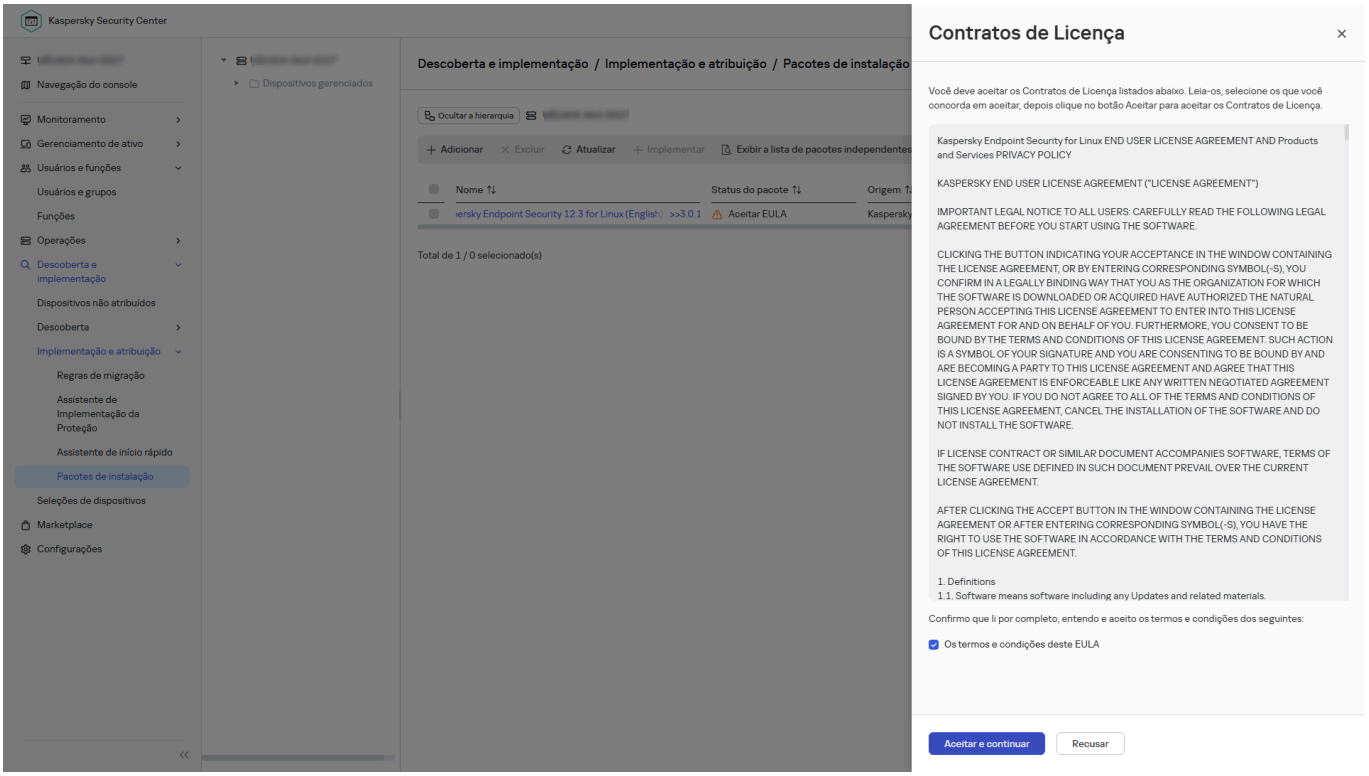
a. Clique em **Mostrar EULA** para ler o Contrato de Licença do Usuário Final (EULA).

b. Leia o EULA exibido na tela e clique em **Aceitar**.

O download continua depois que você aceita o EULA. Se clicar em **Recusar**, o download será interrompido.



Baixar o pacote de instalação



Aceitação do EULA

Feche a janela do assistente. Nesse caso, o processo de download continuará no modo segundo plano. É possível rastrear o status do download do pacote de instalação, filtrar e classificar os status na coluna **Status do pacote**.

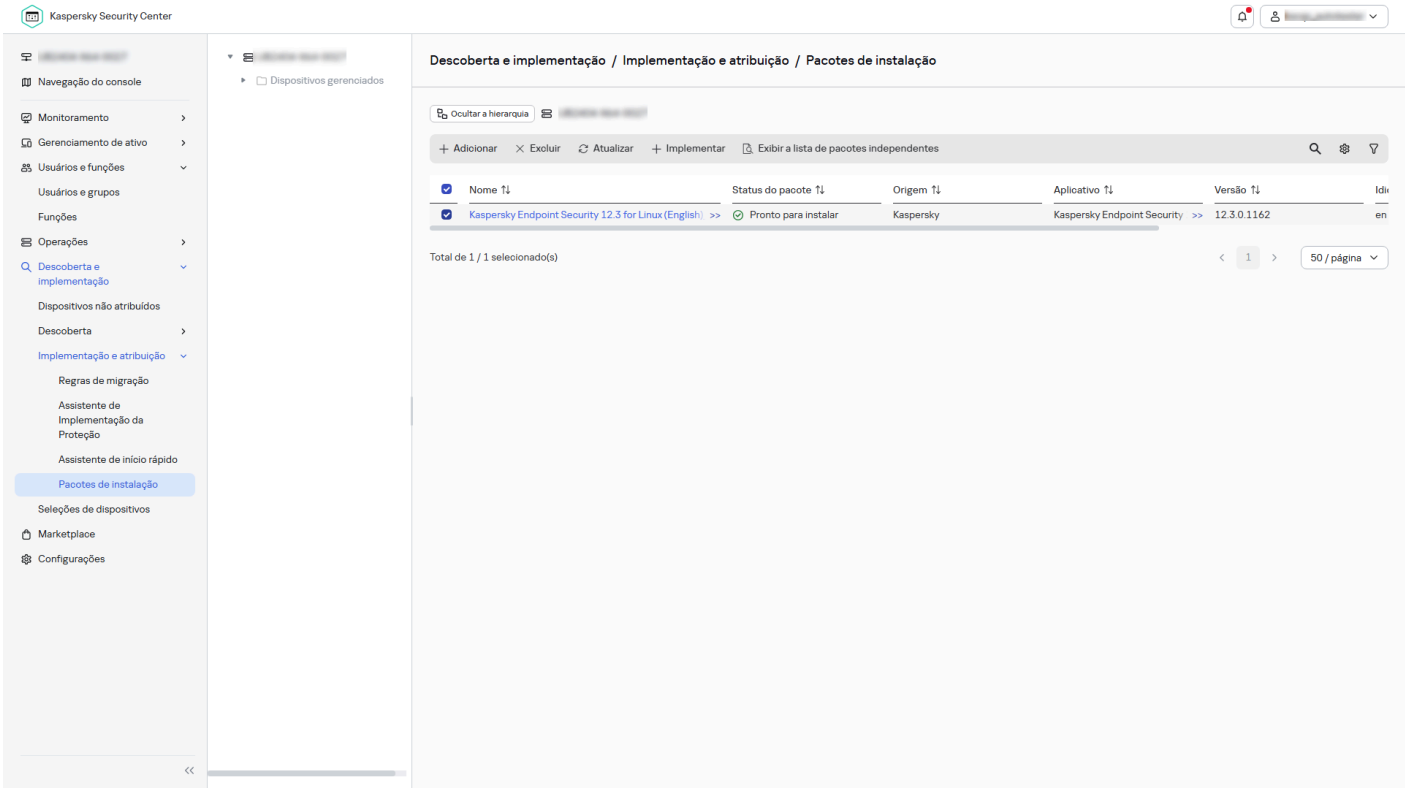
Caso o processo de download pare e o status do download mude para **Aceitar EULA**, clique no nome do pacote de instalação e siga as etapas 5.a e 5.b.

Por padrão, os pacotes de instalação com status **Em andamento** e **Aceitar EULA** aparecem no início da lista.

Se o tamanho dos dados contidos no pacote de distribuição selecionado exceder o limite atual, uma mensagem de erro será exibida. É possível alterar o valor limite e prosseguir com a criação do pacote de instalação.

6. Quando o download for concluído, clique no botão **Fechar**.

O pacote de instalação selecionado é baixado para a pasta compartilhada do Servidor de Administração, na subpasta Pacotes. Após o download, o pacote de instalação é exibido na lista de pacotes de instalação.



A lista de pacotes de instalação

Criando pacotes de instalação a partir de um arquivo

Você pode usar os pacotes de instalação personalizada para fazer o seguinte:

- Instalar qualquer aplicativo (como um editor de texto) em um dispositivo cliente, por exemplo, através de uma tarefa.
- Para criar um pacote de instalação independente.

Um pacote de instalação personalizada é uma pasta com um conjunto de arquivos. Uma fonte para criar um pacote de instalação personalizado é um *arquivo morto*. O arquivo de compactação contém um ou mais arquivos que devem ser incluídos no pacote de instalação personalizada.

Se o Servidor de Administração tiver acesso ao repositório de pacotes de distribuição de aplicativos para instalação remota, use a tarefa **Baixar atualizações no repositório do Servidor de Administração** para baixar as dependências necessárias para criar pacotes de instalação para instalar aplicativos em dispositivos Windows.

Se o Servidor de Administração não tiver acesso ao repositório de pacotes de distribuição de aplicativos para instalação remota:

1. Crie o sinalizador RIUtilsArchiveDirUsed executando o seguinte comando:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Execute o seguinte comando para reiniciar o serviço do Servidor de Administração:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Baixe os módulos adicionais, "Arquivos para instalação remota via Kaspersky Security Center", no site da Kaspersky.

   Os arquivos baixados têm os seguintes nomes:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Não renomeie os arquivos comprimidos.

4. Coloque os arquivos no diretório /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives.

   Caso contrário, ao criar um pacote de instalação, o seguinte erro será exibido: **Utilitários de instalação remota para win32 não encontrados**.

O Servidor de Administração agora tem as dependências necessárias.

Ao criar um pacote de instalação personalizado, é possível especificar parâmetros da linha de comandos, por exemplo, para instalar o aplicativo em modo silencioso.

Assista ao vídeo para saber como criar e implementar um pacote de instalação personalizada para Windows. A versão de texto deste tutorial para dispositivos Windows e Linux está disponível abaixo.

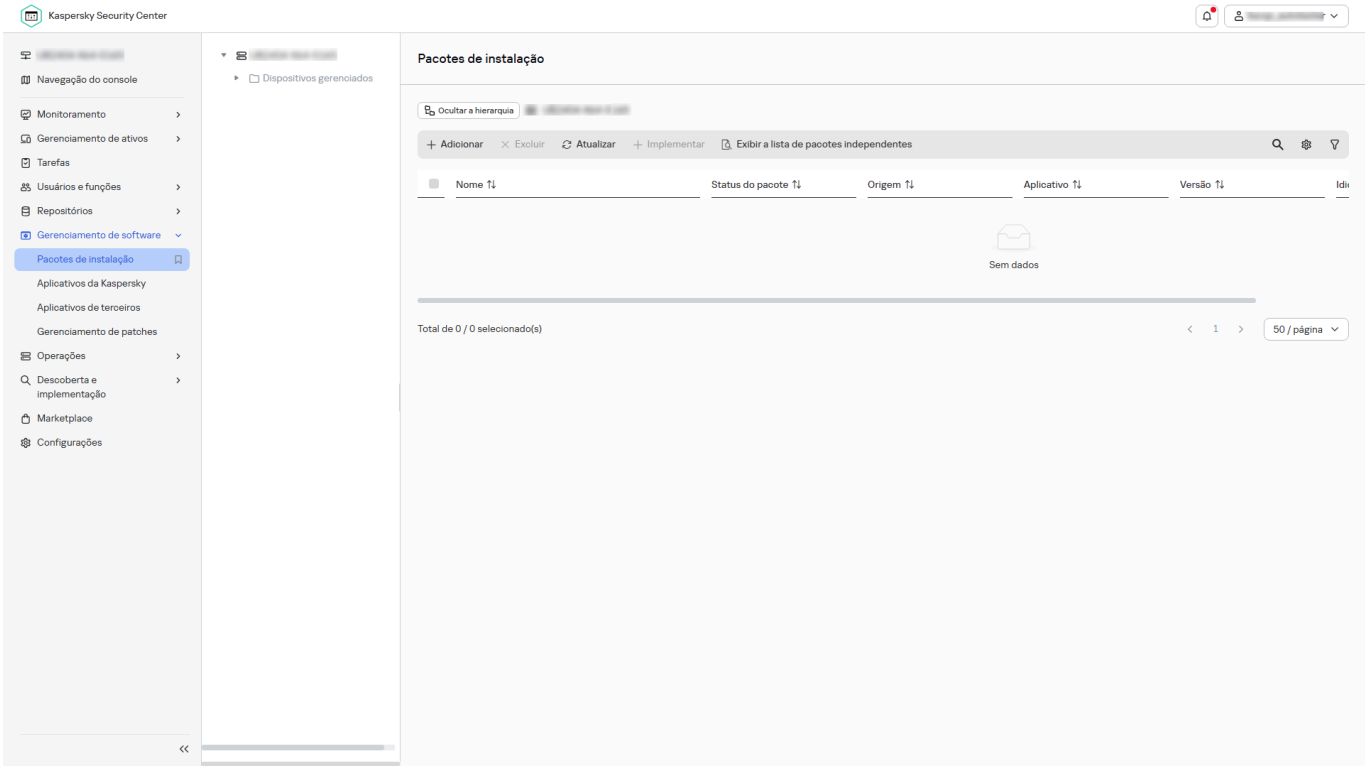


Criar e implementar um pacote de instalação personalizado no Windows usando um arquivo. Vídeo

Para criar um pacote de instalação personalizado:

1. No menu principal, vá para **Gerenciamento de software → Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

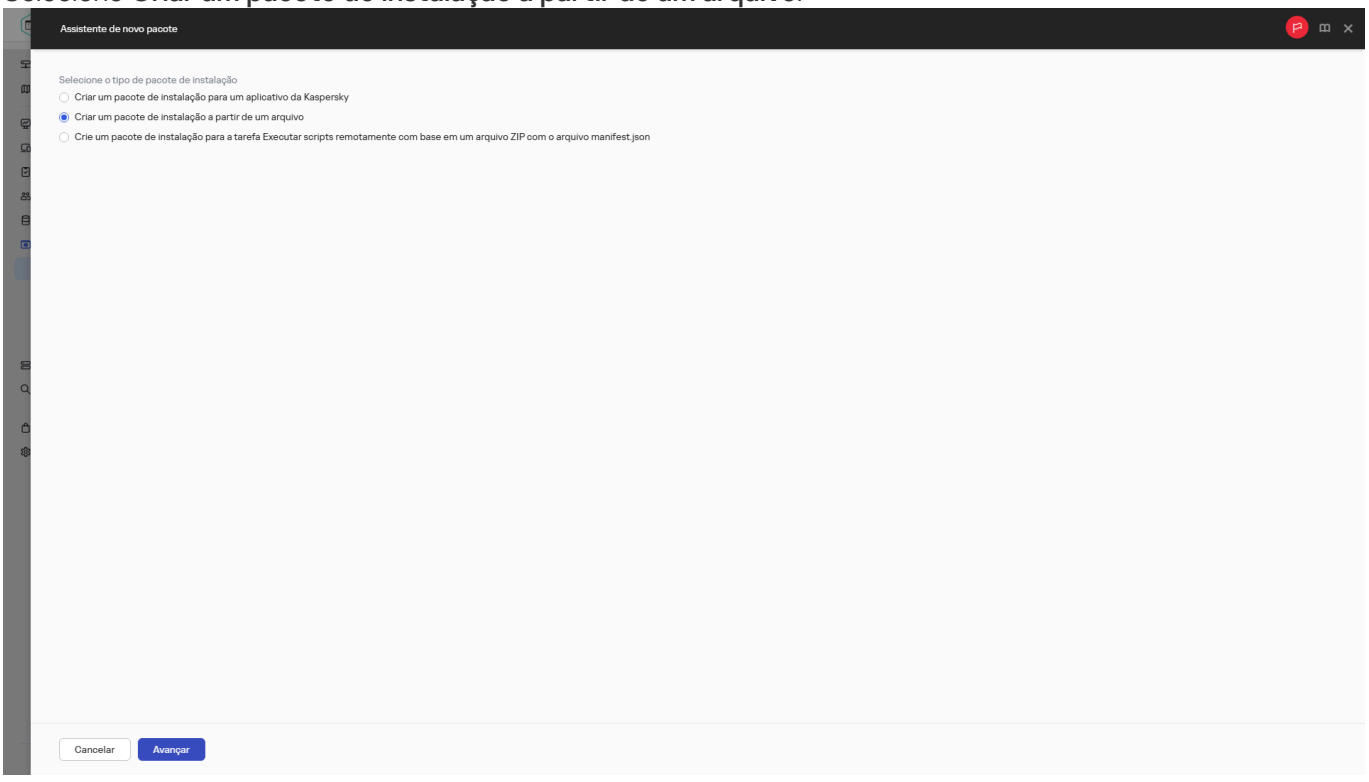


A lista de pacotes de instalação

2. Clique em **Adicionar**.

   O Assistente de novo pacote inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Selecione **Criar um pacote de instalação a partir de um arquivo**.



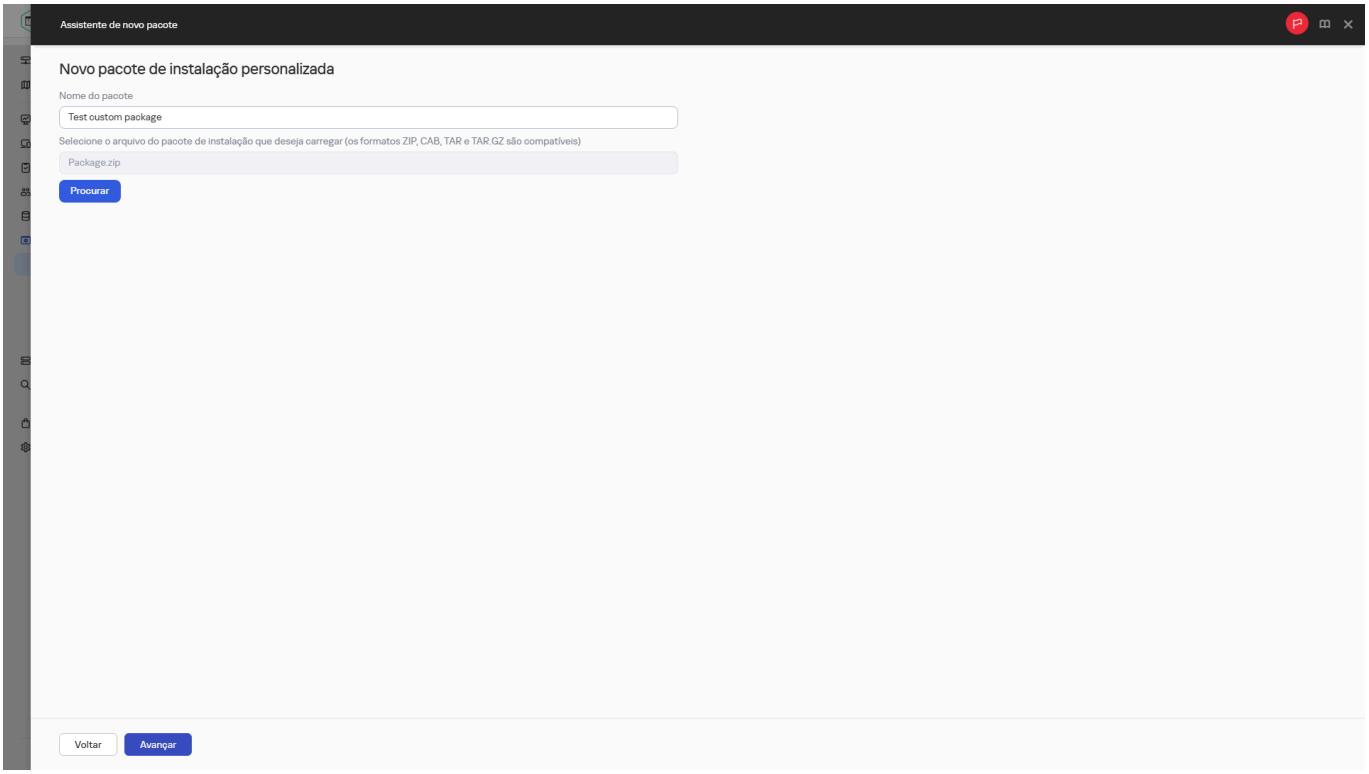
Seleção do tipo de pacote de instalação

4. Especifique o nome do pacote e clique no botão **Procurar**.

5. Na janela aberta, escolha o arquivamento localizado nos discos disponíveis.

   Você pode carregar um arquivo ZIP, CAB, TAR ou TAR.GZ. Não é possível criar um pacote de instalação a partir do arquivo SFX (arquivo de extração automática).

   Upload de arquivo para o Servidor de Administração é iniciado.



Especificação do arquivo do pacote de instalação

6. Se você especificou um arquivo de um aplicativo Kaspersky, receber uma solicitação para ler e aceitar o Contrato de Licença do Usuário Final (EULA) para o aplicativo. Para continuar, você deve aceitar o EULA. Selecione a opção **Aceitar os termos e condições deste Contrato de Licença de Usuário Final** se você leu, compreendeu e aceito integralmente os termos do EULA.

   Além disso, você receber uma solicitação para ler e aceitar a Política de Privacidade. Para continuar, você deve aceitar a Política de Privacidade. Selecione a opção comando abaixo **Eu aceito a Política de Privacidade** somente se você entender e concordar que seus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade.

7. Selecione um arquivo (na lista de arquivos extraídos do arquivo de compactação escolhido) e especifique os parâmetros da linha de comando de um arquivo executável.

   Como criar um pacote de instalação no formato deb ou rpm

   1. Crie um script `.sh` com os seguintes comandos:

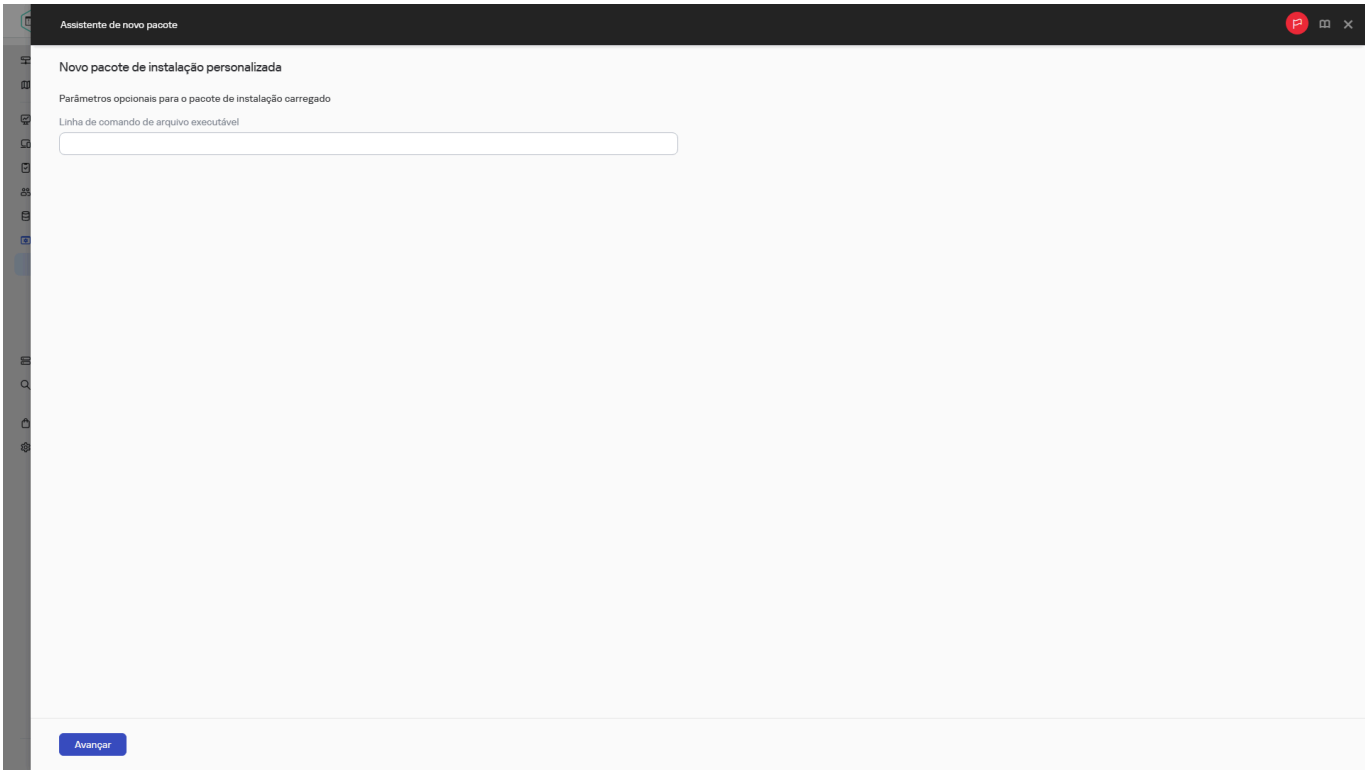
```
#!/bin/sh
script_dir="$(dirname "$0")"
apt-get install --yes "$script_dir/<package_name>.deb" </dev/null
```

      O conteúdo e os comandos do script podem variar dependendo do formato do pacote e de outras informações. Você pode modificar o script para adequá-lo à sua configuração específica.

   2. Coloque o script criado em um arquivo comprimido, junto com o arquivo `.deb` ou `.rpm`.

   3. Ao criar o pacote de instalação, selecione o script criado como o arquivo executável.

Você pode especificar parâmetros da linha de comando, para instalar o aplicativo a partir do pacote de instalação em um modo silencioso. A especificação de parâmetros da linha de comando é opcional.



Especificação dos parâmetros opcionais da linha de comando

O processo para criar o pacote de instalação é iniciado.

O assistente informa quando o processo é concluído.

Se o pacote de instalação não for criado, a mensagem apropriada será exibida.

8. Clique no botão **Concluir** para fechar o assistente.

O pacote de instalação que você criou é baixado na subpasta Packages da pasta compartilhada do Servidor de Administração. Após o download, o pacote de instalação aparece na lista de pacotes de instalação.

Na lista de pacotes de instalação disponíveis no Servidor de Administração, clicando no link com o nome de um pacote de instalação personalizado, você pode:

- Visualize as seguintes propriedades de um pacote de instalação:
  - **Nome**. Nome do pacote de instalação personalizada.
  - **Status do pacote**. Status do download do pacote de instalação.
  - **Origem**. Nome do fornecedor do aplicativo.
  - **Aplicativo**. Nome do aplicativo compactado no pacote de instalação personalizada.
  - **Versão**. Versão do aplicativo.
  - **Idioma**. Idioma do aplicativo compactado no pacote de instalação personalizada.
  - **Tamanho (MB)**. Tamanho do pacote de instalação.
  - **SO**. Tipo do sistema operacional ao qual o pacote de instalação se destina.

- **Criação**. Data de criação do pacote de instalação.
- **Modificação**. Data de modificação do pacote de instalação.
- **Tipo**. Tipo do pacote de instalação.

- Mude os parâmetros de linha de comando.

Criar pacote de instalação autônomo

Você e os usuários de dispositivos na sua organização podem usar pacotes de instalação independente para instalar os aplicativos no dispositivo manualmente.

Um pacote de instalação independente é um arquivo executável que pode ser armazenado em um Servidor Web ou pasta compartilhada, enviado por e-mail ou transferido para um dispositivo cliente usando outro método. No dispositivo cliente, o usuário pode executar o arquivo recebido localmente para instalar um aplicativo sem envolver o Kaspersky Security Center Linux. Você pode criar pacotes de instalação independentes para aplicativos Kaspersky e de terceiros. Para criar um pacote de instalação independente para um aplicativo de terceiros, você deve criar um pacote de instalação personalizado.

Verifique se o pacote de instalação independente não está disponível para terceiros.

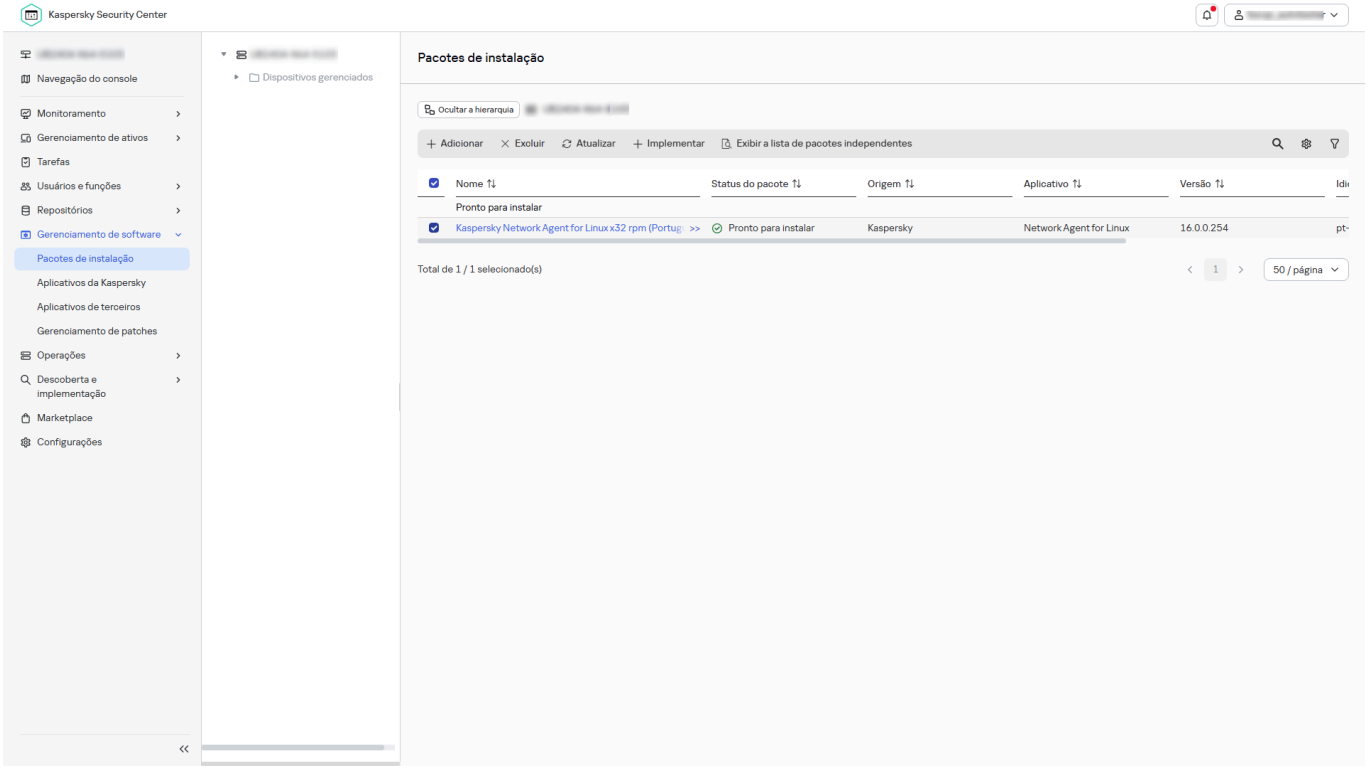
Para criar um pacote de instalação independente:

1. No menu principal, vá para **Gerenciamento de software → Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

   Informações sobre tamanho, hash de arquivo e caminho não estão disponíveis na lista de pacotes de instalação do pacote independente do Agente de Rede ou de quaisquer pacotes criados em Servidores de Administração virtuais. Os pacotes independentes são gerados no momento do download.

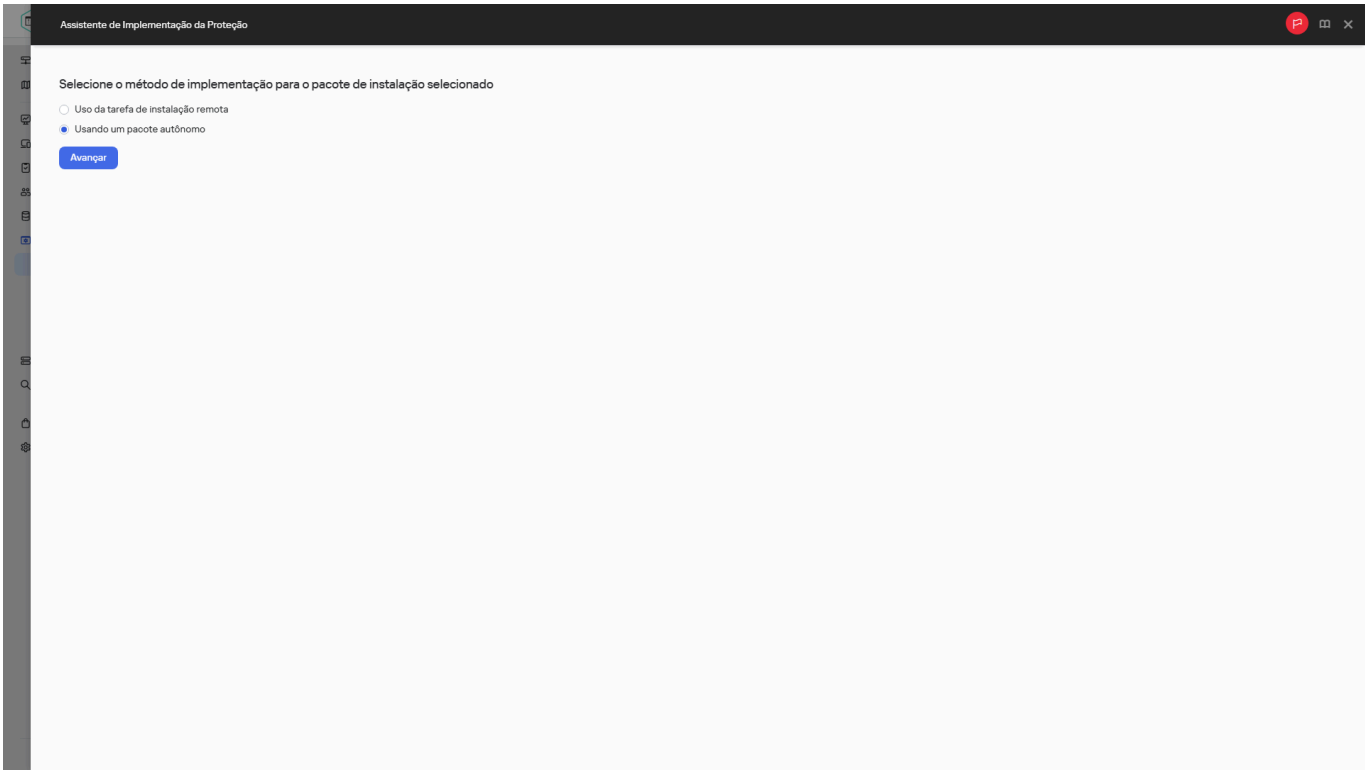
2. Na lista de pacotes de instalação, selecione um pacote de instalação e, acima da lista, clique no botão **Implementar**.



A lista de pacotes de instalação

3. Selecione a opção **Usando um pacote autônomo**.

   O Assistente de Criação de Pacote de Instalação Independente é iniciado. Prossiga pelo assistente usando o botão **Avançar**.



Seleção do método de implementação para o pacote de instalação

4. Verifique e confirme se a opção **Instalar o Agente de Rede junto com este aplicativo** está ativada caso deseje instalar o Agente de Rede juntamente com o aplicativo selecionado.

A opção é exibida conforme o aplicativo para o qual você está criando um pacote de instalação independente.

Por padrão, esta opção está ativada. É recomendável ativar esta opção se não tiver certeza se o Agente de Rede está instalado no dispositivo. Se o Agente de Rede já estiver instalado no dispositivo, após a instalação do pacote de instalação independente com o Agente de Rede, esse será atualizado para a versão mais recente.

Se você desativar esta opção, o Agente de Rede não será instalado no dispositivo e esse não será gerenciado.

Se já existir um pacote de instalação independente para o aplicativo selecionado no Servidor de Administração, o assistente informará a respeito. Nesse caso, você deve selecionar uma das seguintes ações:

- **Criar pacote de instalação independente**. Selecione esta opção, por exemplo, se deseja criar um pacote de instalação independente para uma nova versão do aplicativo e também deseja manter um pacote de instalação independente criado para uma versão anterior do aplicativo. O novo pacote de instalação independente é colocado em outra pasta.

- **Usar pacote de instalação independente existente**. Selecione esta opção se desejar usar um pacote de instalação independente existente. O processo de criação do pacote não será iniciado.

- **Recriar pacote de instalação independente existente**. Selecione esta opção se desejar criar um pacote de instalação independente para o mesmo aplicativo novamente. O pacote de instalação independente é colocado na mesma pasta.

5. Na etapa **Migrar para a lista de dispositivos gerenciados**, a opção **Não migrar dispositivos** está selecionada por padrão. Se você não quiser mover o dispositivo cliente para algum grupo de administração após a instalação do Agente de Rede, mantenha esta opção selecionada.

   Se quiser mover os dispositivos clientes após a instalação do Agente de Rede, selecione a opção **Migrar dispositivos não atribuídos para este grupo** e especifique um grupo de administração para o qual você deseja mover o dispositivo cliente. Por padrão, o dispositivo é movido para o grupo **Dispositivos gerenciados**.



Seleção do grupo de administração para mover o dispositivo cliente

6. Quando o processo de criação do pacote de instalação independente for concluído, clique no botão **CONCLUIR**.

   O Assistente de Criação de Pacote de Instalação Independente é fechado.

O pacote de instalação independente é criado e colocado na subpasta PkgInst da pasta compartilhada do Servidor de Administração. Você pode visualizar a lista de pacotes independentes, clicando no botão **Exibir a lista de pacotes independentes** acima da lista de pacotes de instalação.

Configurações do pacote de instalação do Agente de Rede

Para configurar um pacote de instalação do Agente de Rede:

1. No menu principal, vá para **Gerenciamento de software → Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Clique no nome do pacote de instalação do Agente de Rede.

A janela de propriedades do pacote de instalação do Agente de Rede abre.

As configurações de um pacote de instalação do Agente de Rede estão agrupadas nas seguintes guias:

- Guia **Geral**

  Essa guia apresenta as seguintes informações sobre o pacote de instalação:

  - Nome do pacote de instalação
  - Nome e versão do aplicativo para o qual o pacote de instalação foi criado
  - Tamanho do pacote de instalação
  - Data de criação do pacote de instalação
  - Caminho para a pasta do pacote de instalação

- Guia **Configurações**

  Essa guia apresenta as configurações necessárias para garantir o funcionamento adequado do Agente de Rede imediatamente após a instalação.

  - Seção **Configurações**

    Instalar na pasta padrão

    Se esta opção estiver selecionada, o Agente de Rede será instalado na pasta <Unidade>:\Program Files\Kaspersky Lab\NetworkAgent. Se essa pasta não existir, ela será criada automaticamente.

    Por padrão, esta opção está selecionada.

    Instalar na pasta especificada

    Se esta opção estiver selecionada, o Agente de Rede será instalado na pasta especificada no campo de entrada.

    Usar senha de desinstalação

Se esta opção estiver ativada, você pode inserir a senha de desinstalação (disponível somente para o Agente de Rede em dispositivos que executam sistemas operacionais Windows).

Por padrão, esta opção está desativada.

Proteger serviço do Agente de Rede contra remoção ou interrupção não autorizada e impedir alterações nas configurações

Quando esta opção estiver ativado, após o Agente de Rede ter sido instalado em um dispositivo gerenciado, o componente não poderá ser removido ou reconfigurado sem os privilégios necessários. O serviço Agente de Rede não pode ser interrompido. Essa opção não tem efeito nos controladores de domínio.

Ative esta opção para proteger o Agente de Rede em estações de trabalho operadas com direitos de administrador local.

Por padrão, esta opção está desativada.

Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido

Caso essa opção esteja ativada, todas as atualizações e patches baixados para o Servidor de Administração, Agente de Rede, o Kaspersky Security Center Web Console e o Servidor de MDM do iOS serão instalados automaticamente.

Se esta opção estiver desativada, todas as atualizações e patches baixados somente serão instalados após você modificar seu status para *Aprovado*. As atualizações e patches com o status *Indefinido* não serão instaladas.

Por padrão, esta opção está ativada.

- Seção **Conexão**

  Nesta seção, é possível configurar a conexão do agente de rede para o Servidor de Administração. Para estabelecer uma conexão, é possível usar o protocolo SSL ou UDP. Para configurar a conexão, especifique as seguintes configurações:

  Endereço do Servidor de Administração

  Endereço do dispositivo com o Servidor de Administração instalado.

  Número da porta

  O número da porta que é usada para conexão.

  Porta SSL

  Número da porta que é usada para conexão através do protocolo SSL.

  Usar certificado do Servidor

  Se esta opção estiver ativada, a autenticação de acesso do Agente de Rede ao Servidor de Administração usará o arquivo de certificado, que pode ser especificado clicando no botão **Selecionar arquivo de certificado**.

  Se esta opção estiver desativada, o arquivo de certificado será recebido do Servidor de Administração na primeira conexão do Agente de Rede ao endereço especificado no campo **Endereço do Servidor de Administração**.

  Não recomendamos desativar esta opção porque o recebimento automático de um certificado do Servidor de Administração pelo Agente de Rede na conexão ao Servidor de Administração é considerado inseguro.

  Por padrão, esta opção está desativada.

  Usar conexão SSL

  Se esta opção estiver ativada, a conexão com o Servidor de Administração é estabelecida através de uma porta segura via SSL.

Por padrão, esta opção está desativada. Recomendamos não desativar a opção para que a conexão permaneça segura.

Usar porta UDP

Se esta opção estiver ativada, o Agente de Rede é conectado ao Servidor de Administração através de uma porta UDP. Isso permite gerenciar os dispositivos clientes e receber as informações sobre eles.

A porta UDP deve ser aberta nos dispositivos gerenciados onde o agente de rede está instalado. Portanto, recomendamos não desativar a opção.

Por padrão, esta opção está ativada.

Porta UDP

Neste campo, é possível especificar a porta para conectar o Servidor de Administração com o Agente de Rede usando protocolo UDP.

A porta UDP padrão é 15000.

Não usar servidor proxy

Se essa opção estiver ativada, a conexão direta será usada para conectar o dispositivo ao Servidor de Administração.

Usar o servidor proxy

Se essa opção estiver ativada, especifique os parâmetros do servidor proxy:

- **Endereço do servidor proxy**
- **Porta do servidor proxy**

Se o servidor proxy exigir autenticação, ative a opção **Autenticação do servidor proxy** e especifique o **Nome do usuário** e a **Senha** da conta sob a qual a conexão com o servidor proxy será estabelecida. Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

Abrir portas do Agente de Rede no firewall do Microsoft Windows

Caso essa opção esteja ativada, as portas usadas pelo Agente de Rede serão adicionadas na lista de exclusões do Firewall do Microsoft Windows.

Por padrão, esta opção está ativada.

> Esta opção está disponível somente para pacotes de instalação do Agente de Rede destinados a dispositivos que executam Windows.

- Seção **Avançado**

  Nesta seção, é possível configurar como usar o gateway de conexão.

  No grupo de configurações do **Gateway de conexão**, é possível configurar o método de conexão entre um dispositivo e o Servidor de Administração:

  Usar o Agente de Rede como um gateway de conexão na DMZ

  Se esta opção estiver ativada, o Agente de Rede será usado como um gateway de conexão na zona desmilitarizada (DMZ) para se conectar ao Servidor de Administração, estabelecer comunicação com ele e manter os dados no Agente de Rede seguros durante a transmissão de dados.

  Conectar-se ao Servidor de Administração usando o gateway de conexão

Se esta opção estiver ativada, será estabelecida uma conexão com o Servidor de Administração usando um gateway de conexão para reduzir o número de conexões com o Servidor de Administração. Nesse caso, insira o endereço do dispositivo que atuará como gateway de conexão no campo **Endereço do gateway de conexão**.

No grupo de configurações da **Máquina virtual**, é possível configurar a conexão para a Virtual Desktop Infrastructure (VDI) se sua rede incluir máquinas virtuais:

Ativar modo dinâmico para VDI

Se esta opção estiver ativada, o modo dinâmico para a Infraestrutura de Virtual Desktop Infrastructure (VDI) será habilitado para o Agente de Rede instalado em uma máquina virtual.

Por padrão, esta opção está desativada.

Otimizar as configurações para VM

Se esta opção estiver ativada, os seguintes recursos estarão desativados nas configurações do Agente de Rede:

- Recuperar informações sobre o software instalado
- Recuperar informações sobre o hardware
- Recuperar informações sobre as vulnerabilidades detectadas
- Recuperar informações sobre as atualizações necessárias

Por padrão, esta opção está desativada.

Se você quiser solicitar automaticamente que os usuários se registrem como proprietários de dispositivos após instalar o Agente de Rede em dispositivos Linux, ative a opção **Permitir a execução do utilitário de registro do usuário após a instalação do Agente de Rede**.

Se esta opção estiver ativada, o registro do usuário como um utilitário de proprietário do dispositivo será executado após a instalação do Agente de Rede. Por padrão, esta opção está desativada.

- Seção **Tags**

  A seção **Tags** exibe uma lista de palavras-chave (tags) que podem ser adicionadas aos dispositivos cliente após a instalação do Agente de Rede. Você pode adicionar e remover tags da lista, bem como renomeá-las.

  Se a caixa de seleção estiver marcada ao lado da tag, essa será automaticamente adicionada aos dispositivos gerenciados durante a instalação do Agente de Rede.

  Se a caixa de seleção estiver desmarcada ao lado da tag, essa não será automaticamente adicionada aos dispositivos gerenciados durante a instalação do Agente de Rede. Você pode adicionar manualmente essa tag aos dispositivos.

  Ao remover uma tag da lista, ele será automaticamente removido de todos os dispositivos aos quais foi adicionada.

  > As regras de atribuição de tags automática não se aplicam aos pacotes de instalação do Agente de Rede destinados a dispositivos que executam Linux e macOS.

- Guia **Pacotes independentes**

Nessa guia, é possível fazer o seguinte:

- Visualizar a lista de pacotes de instalação independentes.
- Publique um pacote de instalação independente no Servidor Web, clicando no botão **Publicar**. O pacote de instalação independente publicado está disponível para download para usuários aos quais você enviou o link para o pacote de instalação independente.
- Anular publicação de um pacote de instalação independente no Servidor Web clicando no botão **Cancelar a publicação**. O pacote de instalação independente não publicado está disponível para download apenas para você e outros administradores.
- Baixe um pacote de instalação independente para o seu dispositivo clicando no botão **Baixar**.
- Envie um e-mail com o link para um pacote de instalação independente clicando no botão **Enviar por e-mail**.
- Remova um pacote de instalação independente clicando no botão **Remover**.

- Guia **Histórico de revisões**

  Nessa guia, é possível visualizar o histórico de revisões do pacote de instalação. Você pode comparar revisões, exibir revisões, salvar revisões em um arquivo, e adicionar e editar descrições da revisão.

Execução de pacotes independentes criados pelo Kaspersky Security Center Linux

Os métodos acima descritos da implementação inicial do Agente de Rede e de outros aplicativos nem sempre podem ser implementados porque não é possível atender todas as condições aplicáveis. Em tais casos, é possível criar um arquivo executável comum denominado *pacote de instalação independente* usando o Kaspersky Security Center Linux com o uso de pacotes de instalação com as configurações de instalação relevantes que foram preparadas pelo administrador. Um pacote de instalação independente pode ser publicado em um servidor Web interno (incluído no Kaspersky Security Center Linux), se isso for considerado razoável (o acesso externo a esse servidor Web foi configurado para usuários do dispositivo de destino) ou em um servidor Web implantado exclusivamente. Servidor incluído no Kaspersky Security Center Web Console. Você também pode copiar pacotes independentes para outro Servidor da Web.

Você pode usar o Kaspersky Security Center Linux para enviar aos usuários selecionados uma mensagem de e-mail contendo um link para o arquivo do pacote independente no servidor Web usado atualmente, solicitando que executem o arquivo (no modo interativo ou com o "-s" chave para instalação silenciosa). Você pode anexar o pacote de instalação independente a uma mensagem de e-mail e então enviá-lo aos usuários dos dispositivos que não tenham acesso ao Servidor da Web. O administrador também pode copiar o pacote independente em uma unidade removível, entregá-lo a um dispositivo relevante e, em seguida, executá-lo mais tarde.

Você pode criar um pacote independente a partir de um pacote de Agente de Rede, de um pacote de outro aplicativo (por exemplo, o aplicativo de segurança), ou ambos. Se o pacote independente foi criado a partir do Agente de Rede e de outro aplicativo, a instalação inicia com o Agente de Rede.

Ao criar um pacote independente com o Agente de Rede, você pode especificar o grupo de administração ao qual os novos dispositivos (aqueles que não foram alocados à nenhum dos grupos de administração) serão automaticamente movidos quando a instalação do Agente de Rede for concluída neles.

Os pacotes independentes podem ser executados no modo interativo (por padrão), exibindo o resultado da instalação de aplicativos que eles contêm, ou eles podem ser executados no modo silencioso (quando executados com a chave "-s"). O modo silencioso pode ser usado para a instalação de scripts, por exemplo, de scripts configurados para ser executados após a implementação da imagem do sistema operacional. O resultado da instalação no modo silencioso é determinado pelo código de retorno do processo.

Instalação de aplicativos usando pacotes independentes

O Kaspersky Security Center permite criar pacotes de instalação independentes para aplicativos. Um pacote de instalação independente é um arquivo executável que pode estar localizado em um Servidor Web, ser enviado por e-mail ou transferido de outra maneira para um dispositivo cliente. O arquivo recebido pode ser executado localmente no dispositivo cliente para instalar um aplicativo sem envolver o Kaspersky Security Center.

Para instalar um aplicativo usando um pacote de instalação independente:

1. No menu principal, vá para **Gerenciamento de software → Pacotes de instalação**.
2. Marque a caixa de seleção ao lado do pacote de instalação do aplicativo necessário e clique no botão **Implementar**.
3. Na janela exibida, selecione **Usando um pacote autônomo** e clique no botão **Avançar**.

   O Assistente de criação de pacote de instalação independente é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
4. Selecione a opção **Criar pacote de instalação independente**.
5. Especifique se os dispositivos devem ser movidos para um grupo de administração depois da instalação do Agente de Rede.
6. Na etapa final do assistente, selecione um método para transferir o pacote de instalação independente para o dispositivo cliente e clique no botão **Concluir** para concluir o assistente.
7. Transfira o pacote de instalação independente para o dispositivo cliente.
8. Execute o pacote de instalação independente no dispositivo cliente.

O aplicativo será instalado no dispositivo cliente com as configurações especificadas no pacote independente.

Ao criar um pacote de instalação independente, ela é automaticamente publicada no Servidor Web. Um link para o download do pacote independente é exibido na lista de pacotes de instalação independentes criados. Se necessário, você pode cancelar a publicação do pacote independente selecionado e publicá-lo novamente no Servidor Web. Por padrão, a porta 8060 é usada para o download de pacotes de instalação independentes.

Adequabilidade da atualização dos bancos de dados em um pacote de instalação de um aplicativo de segurança

Antes de iniciar a implementação da proteção, você deve ter em mente a possibilidade de atualizar os bancos de dados antivírus (incluindo os módulos de patches automáticas), fornecidos junto com o pacote de distribuição do aplicativo de segurança. É útil atualizar os bancos de dados no pacote de instalação do aplicativo antes de iniciar a implementação (por exemplo, usando o comando correspondente no menu de contexto de um pacote de instalação selecionado). Isto reduzirá o número de reinícios necessários para a conclusão da implementação da proteção em dispositivos alvo.

Alteração do limite de tamanho dos dados de pacotes de instalação personalizada

O tamanho total dos dados descompactados durante a criação de um pacote de instalação personalizada é limitado. O limite padrão é 1 GB.

Se você tentar carregar um arquivo compactado que contém dados que excedam o limite atual, uma mensagem de erro será exibida. Pode ser necessário aumentar esse valor limite ao criar pacotes de instalação a partir de pacotes de distribuição grandes.

Para alterar o valor limite para o tamanho do pacote de instalação personalizada:

1. No dispositivo do Servidor de Administração, execute o prompt de comando na conta que foi usada para instalar o Servidor de Administração.

2. Altere o diretório atual para a pasta de instalação do Kaspersky Security Center Linux (geralmente, /opt/kaspersky/ksc64/sbin).

3. Dependendo do tipo de instalação do Servidor de Administração, digite um dos seguintes comandos na conta root:

   - Instalação local normal:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número of bytes>
     ```

   - Instalação no cluster de failover do Kaspersky Security Center Linux:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número de bytes> --stp
     klfoc
     ```

   Em que <número de bytes> é um número de bytes em formato hexadecimal ou decimal.

   Por exemplo, caso o limite necessário seja 2 GB, é possível especificar o valor decimal 2147483648 ou o valor hexadecimal 0x80000000. Neste caso, para uma instalação local do Servidor de Administração, você pode usar o seguinte comando:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

O limite de tamanho dos dados de pacotes de instalação personalizada é alterado.

Distribuindo pacotes de instalação para Servidores de Administração secundários

O Kaspersky Security Center Linux permite que o usuário crie pacotes de instalação para aplicativos da Kaspersky e para aplicativos de terceiros, além de distribuir pacotes de instalação para dispositivos clientes e instalar aplicativos por meio dos pacotes. Para otimizar a carga no Servidor de Administração principal, você pode distribuir pacotes de instalação para Servidores de Administração secundários. Depois disso, os servidores secundários transmitem os pacotes para os dispositivos clientes e você pode executar a instalação remota dos aplicativos nos dispositivos clientes.

Para distribuir pacotes de instalação para Servidores de Administração secundários:

1. Verifique se os Servidores de Administração secundários estão conectados ao Servidor de Administração principal.

2. No menu principal, vá para **Tarefas**.

   A lista de tarefas é exibida.

3. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

4. Na página **Novas configurações de tarefa**, na lista suspensa **Aplicativo**, selecione **Kaspersky Security Center**. Em seguida, na lista suspensa **Tipo de tarefa**, selecione **Distribuir pacote de instalação** e especifique o nome da tarefa.

5. Na página **Escopo da tarefa**, selecione os dispositivos aos quais a tarefa é atribuída de uma das seguintes maneiras:

   - Se desejar criar uma tarefa para todos os Servidores de Administração secundários em um grupo de administração específico, selecione este grupo e, em seguida, crie uma tarefa de grupo para ele.

   - Se desejar criar uma tarefa para Servidores de Administração secundários específicos, selecione tais Servidores e, em seguida, crie uma tarefa para eles.

6. Na página **Pacotes de instalação distribuídos**, selecione os pacotes de instalação que devem ser copiados para os Servidores de Administração secundários.

7. Especifique uma conta para executar a tarefa *Distribuir pacote de instalação* nesta conta. É possível usar a conta e manter a opção **Conta padrão** ativada. Como alternativa, é possível especificar que a tarefa seja executada em outra conta com os direitos de acesso necessários. Para isso, selecione a opção **Especificar conta** e, em seguida, insira as credenciais dessa conta.

8. Na página **Concluir a criação da tarefa**, é possível ativar a opção **Abrir detalhes da tarefa quando a criação for concluída** para abrir a janela de propriedades da tarefa e modificar as configurações padrão da tarefa. Caso contrário, será possível definir as configurações da tarefa posteriormente, no momento oportuno.

9. Clique no botão **Concluir**.

   A tarefa criada para distribuir pacotes de instalação para os Servidores de Administração secundários é exibida na lista de tarefas.

10. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que especificou nas configurações da tarefa.

Após a conclusão da tarefa, os pacotes de instalação selecionados serão copiados nos Servidores de Administração secundários especificados.

Visualizar a lista de pacotes de instalação independente

Você pode visualizar a lista de pacotes de instalação independente e as propriedades de cada pacote de instalação independente.

Para visualizar a lista de pacotes de instalação independente para todos os pacotes de instalação:

Acima da lista, clique no botão **Exibir a lista de pacotes independentes**.

Na lista de pacotes de instalação independentes, suas propriedades são exibidas da seguinte maneira:

- **Nome do pacote**. Nome do pacote de instalação independente que é formado automaticamente como o nome do aplicativo incluído no pacote e na versão do aplicativo.
- **Nome do aplicativo**. Nome do aplicativo incluído no pacote de instalação independente.
- **Versão do aplicativo**.
- **Nome do pacote de instalação do Agente de Rede**. A propriedade será exibida apenas se o Agente de Rede estiver incluído no pacote de instalação independente.
- **Versão do Agente de Rede**. A propriedade será exibida apenas se o Agente de Rede estiver incluído no pacote de instalação independente.
- **Tamanho**. Tamanho do arquivo em MB.
- **Grupo**. Nome do grupo para o qual o dispositivo cliente é movido após a instalação do Agente de Rede.
- **Criação**. Data e hora da criação do pacote de instalação independente.
- **Modificação**. Data e hora da modificação do pacote de instalação independente.
- **Caminho**. Caminho completo para a pasta em que o pacote de instalação independente está localizado.
- **Endereço da Web**. Endereço da Web do local do pacote de instalação independente.
- **Hash de arquivo**. A propriedade é usada para certificar que o pacote de instalação independente não foi alterado por terceiros e que um usuário tem o mesmo arquivo que você criou e transferiu para o usuário.

Informações sobre tamanho, hash de arquivo e caminho não estão disponíveis na lista de pacotes de instalação do pacote independente do Agente de Rede ou de quaisquer pacotes criados em Servidores de Administração virtuais. Os pacotes autônomos são gerados no momento do download.

Para visualizar a lista de pacotes de instalação independente para um pacote de instalação específico:

Selecione o pacote de instalação na lista e, acima da lista, clique no botão **Exibir a lista de pacotes independentes**.

Na lista de pacotes de instalação independentes, você pode fazer o seguinte:

- Publique um pacote de instalação independente no servidor da Web, clicando no botão **Publicar**. O pacote de instalação independente publicado está disponível para download para usuários aos quais você enviou o link para o pacote de instalação independente.
- Anular publicação de um pacote de instalação independente no Servidor Web clicando no botão **Cancelar a publicação**. O pacote de instalação independente não publicado está disponível para download apenas para você e outros administradores.
- Baixe um pacote de instalação independente para o seu dispositivo clicando no botão **Baixar**.
- Envie um e-mail com o link para um pacote de instalação independente clicando no botão **Enviar por e-mail**.
- Remova um pacote de instalação independente clicando no botão **Remover**.

Instalação do Agente de Rede para Linux

Para gerenciar dispositivos em uma organização, você deve instalar o Agente de Rede em cada um deles. A implementação do Kaspersky Security Center Linux distribuído nos dispositivos corporativos normalmente começa com a instalação do Agente de Rede neles.

Existem os seguintes métodos para instalar inicialmente o Agente de Rede no dispositivo gerenciado Linux:

- Ao se conectar com o dispositivo gerenciado via SSH e que executa a tarefa de instalação remota.
- Ao executar a instalação do pacote no dispositivo gerenciado.

Depois de instalar o Agente de Rede em um dispositivo, você poderá executar a instalação remota de aplicativos da Kaspersky no mesmo dispositivo através deste Agente de Rede. O pacote de distribuição de um aplicativo a ser instalado é transferido através de canais de comunicação entre Agentes de Rede e o Servidor de Administração, junto com as configurações de instalação definidas pelo administrador. Para transferir o pacote de distribuição, é possível usar nós de distribuição de transmissão, ou seja, pontos de distribuição, entrega multicast, etc.

Ao selecionar um método e uma estratégia para a implementação de aplicativos em uma rede gerenciada, é necessário considerar um número de fatores (lista parcial):

- Configuração de rede da organização.
- Número total de dispositivos.
- Presença de dispositivos na rede da organização, que não são membros de nenhum domínio, e de contas uniformes com direitos de administrador nesses dispositivos.
- Capacidade do canal entre o Servidor de Administração e os dispositivos.

- Tipo de comunicação entre Servidor de Administração e as sub-redes remotas e a capacidade dos canais de rede nessas sub-redes.
- Configurações de segurança aplicadas nos dispositivos remotos no início da implementação. Esses parâmetros permitem estabelecer a conexão remota com o dispositivo gerenciado e iniciar a instalação.

Preparação de um dispositivo Linux para a instalação do Agente de Rede

Antes da instalação do Agente de Rede em um dispositivo Linux, você deve executar as etapas de preparação necessárias para qualquer dispositivo Linux.

Para preparar um dispositivo executando no Linux para a instalação remota do Agente de Rede:

1. Verifique e confirme se o dispositivo no qual deseja instalar o Agente de Rede para Linux está executando em uma das distribuições Linux compatíveis.
2. Se você quiser instalar o Agente de Rede no AltOS no modo de ambiente de software fechado, desative este modo até que a instalação seja concluída.
3. Baixe o pacote de instalação do Agente de Rede usando a interface do Web Console ou no site da Kaspersky.

   Se precisar instalar o Agente de Rede em um dispositivo que executa sistema operacional Linux com glibc 2.5, deverá baixar o pacote de instalação do *Kaspersky Network Agent for Linux Legacy* usando a interface do Web Console ou no site da Kaspersky.
4. Certifique-se de que o software a seguir está instalado no dispositivo Linux de destino:
   - Sudo (para Ubuntu 10.04, a versão do Sudo é 1.7.2p1 ou posterior)
   - Intérprete de linguagem Perl versão 5.10 ou posterior
   - utilitário ps
5. Testar a configuração do dispositivo:
   a. Verifique se você pode conectar-se ao dispositivo através de um cliente SSH (como PuTTY).

      Se não for possível se conectar ao dispositivo, abra o arquivo `/etc/ssh/sshd_config` e assegure-se de que as seguintes configurações têm os respectivos valores listados abaixo:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      Não modifique o arquivo /etc/ssh/sshd_config caso possa se conectar ao dispositivo sem problemas. Caso contrário, poderá haver falha de autenticação SSH ao executar uma tarefa de instalação remota.

      Salve o arquivo (se necessário) e reinicie o serviço SSH usando o comando `sudo service ssh restart`.

   b. Assegure-se de que a porta TCP 22 esteja aberta e acessível em um dispositivo não atribuído baseado em Linux.

      A porta TCP 22 deve estar disponível para que a instalação do Agente de Rede para Linux seja bem-sucedida.

c. Desative a senha sudo para a conta do usuário sob a qual o dispositivo deve ser conectado.

d. Use o comando `visudo` no sudo para abrir o arquivo de configuração sudoers.

No arquivo aberto, adicione a seguinte linha ao final do arquivo: `<nome de usuário> ALL = (ALL) NOPASSWD: ALL`. Neste caso, o `<nome de usuário>` é a conta de usuário que deve ser usada para a conexão de dispositivo usando o SSH. Caso esteja usando o sistema operacional Astra Linux, no arquivo /etc/sudoers, adicione a última linha com o seguinte texto: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. Salve o arquivo sudoers e, a seguir, feche-o.

f. Conecte-se novamente ao dispositivo pelo SSH, verifique e confirme se o serviço Sudo não solicita a inserção de uma senha. Será possível fazer isso com o uso do comando `sudo whoami`.

6. Se quiser instalar o Agente de Rede remotamente em dispositivos que executam o sistema operacional com o sistema de inicialização systemd, abra o arquivo `/etc/systemd/logind.conf` e execute uma das seguintes ações:

- Especifique `no` como valor para a configuração de `KillUserProcesses`: `KillUserProcesses=no`.
- Para a configuração de `KillExcludeUsers`, digite o nome de usuário da conta sob a qual a instalação remota será executada, por exemplo `KillExcludeUsers=root`.

Dispositivo de destino Astra Linux

Caso o dispositivo de destino esteja executando o Astra Linux, adicione a string `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` no arquivo `/home/<nome de usuário>/.bashrc`, onde `<nome de usuário>` é a conta de usuário que deve ser usada para a conexão do dispositivo com o uso do SSH.

Dispositivo de destino OSnova

Caso o dispositivo de destino esteja executando o OSnova, faça o seguinte:

a. Abra o arquivo `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` e, em seguida, comente a linha `#KillUserProcess=yes`.

b. Abra o arquivo `/usr/lib/NESS/pam-user-session` e, em seguida, comente a linha `#loginctl terminate-session "$XDG_SESSION_ID"`.

Para aplicar a configuração alterada, reinicie o dispositivo Linux ou execute o comando a seguir:

```
sudo systemctl restart systemd-logind.service
```

7. Caso queira instalar o agente de rede em dispositivos com o sistema operacional SUSE Linux Enterprise Server 15, instale o pacote insserv-compat primeiro para configurar o agente de rede.

8. Caso queira instalar o Agente de Rede em dispositivos com o sistema operacional Astra Linux em execução no modo de ambiente de software fechado, execute as etapas adicionais para preparar os dispositivos Astra Linux.

9. Caso queira instalar o Agente de Rede em dispositivos que executam o Ubuntu Server ou o Ubuntu Desktop versão 10.04, execute as etapas adicionais para preparar esses dispositivos.

10. Se quiser instalar o Agente de Rede em um dispositivo que executa um sistema operacional Linux com glibc 2.5, execute as etapas adicionais para preparar os dispositivos de destino.

11. Se você estiver instalando o Agente de Rede no AltOS no modo de ambiente de software fechado, reative este modo.

12. Se você deseja instalar o Agente de Rede em dispositivos que usam o sistema operacional RED OS 7.3.4 ou posterior ou MSVSPHERE 9.2 ou posterior, instale o pacote libxcrypt-compat para a função correta do Agente de Rede.

O dispositivo Linux está pronto para a instalação do Agente de Rede. É possível fazer a instalação remota do Agente de Rede no modo interativo ou no modo silencioso.

Preparo de um dispositivo executando o SUSE Linux Enterprise Server 15 para instalação do agente de rede

Antes da instalação do Agente de Rede em um dispositivo que executa o SUSE Linux Enterprise Server 15, execute dois procedimentos de preparação: o mencionado nas instruções abaixo e as etapas gerais de preparação para qualquer dispositivo Linux.

Para instalar o agente de rede em um dispositivo com o sistema operacional SUSE Linux Enterprise Server 15:

Antes da instalação do agente de rede, execute o seguinte comando:

```
sudo zypper install insserv-compat
```

Isso permite a instalação do pacote insserv-compat e configure o agente de rede corretamente.

> Execute o comando `rpm -q insserv-compat` para verificar se o pacote já está instalado.

Caso a rede inclua muitos dispositivos executando o SUSE Linux Enterprise Server 15, será possível usar o software especial para configurar e gerenciar a infraestrutura da empresa. Ao usar o software, é possível instalar automaticamente o pacote insserv-compat em todos os dispositivos necessários de uma só vez. Por exemplo, é possível usar Puppet, Ansible, Chef e ainda criar o próprio script. Use qualquer método conveniente para você.

Se o dispositivo não tiver as chaves de assinatura GPG do SUSE Linux Enterprise, você poderá encontrar o seguinte aviso: `Package header is not signed!` Selecione a opção `i` para ignorar a advertência.

Depois de preparar o dispositivo Linux, é possível fazer a instalação remota do Agente de Rede no modo interativo ou no modo silencioso.

Preparar um dispositivo executando o Astra Linux no modo de ambiente de software fechado para a instalação do Agente de Rede

Antes da instalação do Agente de Rede em um dispositivo executando o Astra Linux no modo de ambiente de software fechado, execute dois procedimentos de preparação: o mencionado nas instruções abaixo e as etapas gerais de preparação para qualquer dispositivo Linux.

> Execute os comandos fornecidos nesta instrução em uma conta com privilégios de acesso root.

Para preparar um dispositivo executando o Astra Linux no modo de ambiente de software fechado para a instalação do Agente de Rede:

1. Abra o arquivo `/etc/digsig/digsig_initramfs.conf` e especifique a seguinte configuração:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Na linha de comando, execute o seguinte comando para instalar o pacote de compatibilidade:

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

3. Crie um diretório para a chave do aplicativo:

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

4. Coloque a chave do aplicativo /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg no diretório criado na etapa anterior:

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

   > Se o kit de distribuição do Kaspersky Security Center Linux não incluir a chave do aplicativo kaspersky_astra_pub_key.gpg, você poderá baixá-lo clicando no link: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Atualize os discos RAM:

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

   Reinicialize o sistema.

O dispositivo Linux está pronto para a instalação do Agente de Rede. É possível fazer a instalação remota do Agente de Rede no modo interativo ou no modo silencioso.

Preparação para a instalação do Agente de Rede em um sistema operacional Linux com glibc 2.5 (SO herdado)

Antes de instalar o Agente de Rede em um dispositivo que executa um sistema operacional Linux com glibc 2.5 (SO herdado), execute dois procedimentos de preparação: as etapas gerais de preparação para qualquer dispositivo Linux e o procedimento descrito neste artigo.

Recomendamos o uso do instalador local para instalar o Agente de Rede em um sistema operacional Linux com glibc 2.5 (SO herdado). Caso precise usar uma tarefa de instalação remota para este cenário, será necessário executar etapas adicionais descritas nas instruções abaixo.

> Execute os comandos fornecidos neste procedimento em uma conta com privilégios raiz.

Recomendamos o uso do instalador local para instalar o Agente de Rede em um sistema operacional Linux com glibc 2.5 (SO herdado). Caso precise usar uma tarefa de instalação remota para este cenário, será necessário executar etapas adicionais descritas nas instruções abaixo.

1. No dispositivo executando um sistema operacional Linux com glibc 2.5, execute as etapas de preparação comuns para qualquer dispositivo Linux.

2. No arquivo `/etc/sudoers`, remova a linha `Defaults requiretty`.

3. Desative a lista de permissão de algoritmos de criptografia válidos para conexões SSH para poder instalar o Agente de Rede no dispositivo que executa um sistema operacional Linux com glibc 2.5.

   Para isso, no dispositivo com o Servidor de Administração instalado ou em um dispositivo que atue como um ponto de distribuição cujo escopo inclua o dispositivo de destino, execute o seguinte comando na linha de comando:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

O dispositivo Linux está pronto para a instalação remota do Agente de Rede.

A desativação da lista de permissão de algoritmos de criptografia válidos pode afetar a segurança da conexão SSH. É altamente recomendável reativar a lista de permissão de algoritmos de criptografia válidos imediatamente após a instalação do Agente de Rede. Para reativar a lista de permissão de algoritmos de criptografia válidos, execute o seguinte comando:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Depois de instalar o Agente de Rede e reativar a lista de permissão de algoritmos de criptografia válidos, o dispositivo que executa um sistema operacional Linux com glibc 2.5 (SO herdado) passa a ser gerenciado pelo Servidor de Administração.

Preparação para a instalação do Agente de Rede em um sistema operacional Linux com OpenSSH versão 6.4 (SO herdado)

Antes da instalação do Agente de Rede em um dispositivo que usa o OpenSSH versão 6.4 ou anteriores (SO herdado), é necessário executar dois procedimentos de preparação: as etapas gerais de preparação para qualquer dispositivo Linux e o procedimento descrito neste artigo.

Recomendamos o uso do instalador local para instalar o Agente de Rede em um sistema operacional Linux com glibc 2.5 (SO herdado). Caso precise usar uma tarefa de instalação remota para este cenário, será necessário executar etapas adicionais descritas nas instruções abaixo.

> Execute os comandos fornecidos nesta instrução em uma conta com privilégios de acesso root.

Para preparar um dispositivo que usa o OpenSSH versão 6.4 ou anterior para a instalação do Agente de Rede:

1. No dispositivo que usa o OpenSSH versão 6.4 ou anterior, execute as etapas de preparação comuns para qualquer dispositivo Linux.

2. Desative a lista de permissões de algoritmos de criptografia válidos para conexões SSH para poder instalar o Agente de Rede no dispositivo que usa o OpenSSH versão 6.4 ou anteriores.

   Para isso, no dispositivo com o Servidor de Administração instalado ou em um dispositivo que atue como um ponto de distribuição cujo escopo inclua o dispositivo de destino, execute o seguinte comando na linha de comando:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

O dispositivo Linux está pronto para a instalação remota do Agente de Rede.

A desativação da lista de permissão de algoritmos de criptografia válidos pode afetar a segurança da conexão SSH. É altamente recomendável reativar a lista de permissão de algoritmos de criptografia válidos imediatamente após a instalação do Agente de Rede. Para reativar a lista de permissão de algoritmos de criptografia válidos, execute o seguinte comando:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Depois de instalar o Agente de Rede e reativar a lista de permissão de algoritmos de criptografia válidos, o dispositivo que executa um sistema operacional Linux com glibc 2.5 (SO herdado) passa a ser gerenciado pelo Servidor de Administração.

Instalação remota do Agente de Rede em um dispositivo Linux

Antes de instalar o Agente de Rede em um dispositivo baseado em Linux, você deve concluir as etapas preparatórias gerais que são necessárias para todos os dispositivos baseados em Linux.

Depois de concluir as etapas gerais, você pode seguir as instruções adicionais específicas do seu sistema operacional:

- Preparação de um dispositivo que executa o SUSE Linux Enterprise Server 15
- Preparação de um dispositivo que executa o Astra Linux no modo de ambiente de software fechado
- Preparação de um dispositivo que executa o Ubuntu Server/Desktop versão 10.04 e 16.04
- Preparar um dispositivo que executa um sistema operacional Linux com glibc 2.5

Para instalar o Agente de Rede em dispositivos Linux remotamente:

1. Baixar e criar um pacote de instalação:

   a. Antes da instalação no dispositivo, assegure-se que ele já tenha todas as dependências (programas e bibliotecas) instaladas para este pacote.

   Você pode exibir as dependências para cada pacote por si só, usando utilitários que são específicos para a distribuição Linux na qual o pacote deve ser instalado. Para obter mais detalhes sobre os utilitários, consulte a documentação de seu sistema operacional.

   b. Para criar um pacote de instalação remota, use os seguintes arquivos:

   - klnagent.kpd
   - akinstall.sh
   - Pacote .deb ou .rpm para Agente de Rede

2. Crie uma tarefa de instalação remota com as seguintes configurações:

   - Na página **Configurações** do Assistente para novas tarefas, marque a caixa de seleção **Uso dos recursos do sistema operacional por meio do Servidor de Administração**. Limpar todas as outras caixas de seleção.

   - Na página **Selecionar uma conta para executar a tarefa**, especifique as configurações da conta de usuário usadas para a conexão do dispositivo através de SSH.

3. Executar a tarefa de instalação remota. Use a opção para o comando `su` para preservar o ambiente: `-m, -p, --preserve-environment`.

Instalar o Agente de Rede para Linux no modo silencioso (com um arquivo de resposta)

Você pode instalar o Agente de Rede em dispositivos Linux usando um arquivo de resposta – um arquivo de texto que contém um conjunto personalizado de parâmetros de instalação: variáveis e seus respectivos valores. O uso do arquivo de resposta permite executar a instalação no modo silencioso, ou seja, sem a participação do usuário.

Antes de instalar o Agente de Rede em um dispositivo baseado em Linux, você deve concluir as etapas preparatórias gerais que são necessárias para todos os dispositivos baseados em Linux.

Depois de concluir as etapas gerais, você pode seguir as instruções adicionais específicas do seu sistema operacional:

- Preparação de um dispositivo que executa o SUSE Linux Enterprise Server 15
- Preparação de um dispositivo que executa o Astra Linux no modo de ambiente de software fechado
- Preparação de um dispositivo que executa o Ubuntu Server/Desktop versão 10.04 e 16.04
- Preparar um dispositivo que executa um sistema operacional Linux com glibc 2.5

Para executar a instalação do Agente de Rede para Linux no modo silencioso:

1. Leia o Contrato de Licença do Usuário Final. Siga as etapas abaixo somente se entender e aceitar os termos do Contrato de Licença do Usuário Final.

2. Crie o arquivo de resposta (no formato TXT). Adicione ao arquivo de resposta uma lista de variáveis no formato VARIABLE_NAME = variable_value, cada variável em uma linha separada.

   Para o uso correto do arquivo de resposta, você deve incluir nele um conjunto mínimo das três variáveis necessárias:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Você também pode adicionar quaisquer variáveis opcionais para usar parâmetros mais específicos da sua instalação remota. A tabela a seguir lista todas as variáveis que podem ser incluídas no arquivo de resposta:

   Variáveis do arquivo de resposta usadas como parâmetros de instalação do Agente de Rede para Linux no modo silencioso

Variáveis do arquivo de resposta usadas como parâmetros de instalação do Agente de Rede para Linux no modo silencioso

Nome da variável	Necessário	Descrição	Valores possíveis
KLNAGENT_SERVER	Sim	Contém o nome do Servidor de Administração apresentado como nome de domínio totalmente qualificado (FQDN) ou endereço IP.	Nome DNS ou endereço IP.
KLNAGENT_AUTOINSTALL	Sim	Define se o modo de instalação silenciosa está ativado.	1 – O modo silencioso está ativado; o usuário não é solicitado a executar nenhuma ação durante a instalação. Outro – O modo silencioso está desativado; o usuário pode ser solicitado a executar ações durante a instalação.
EULA_ACCEPTED	Sim	Define se o usuário aceita o Contrato de Licença do Usuário Final (EULA) do Agente de Rede; quando ausente, pode ser interpretado como não aceitação do EULA.	1 – Confirmo que li, entendi e aceito integralmente os termos e condições deste Contrato de Licença do Usuário Final. Outro ou não especificado – Não aceito os termos do Contrato de Licença (a instalação não é executada).
KLNAGENT_PROXY_USE	Não	Define se a conexão com o Servidor de Administração usará configurações de proxy. O valor padrão é 0.	1 – As configurações de proxy são usadas. Outro – As configurações de proxy não são usadas.
KLNAGENT_PROXY_ADDR	Não	Define o endereço do servidor proxy usado para conexão com o Servidor de Administração.	Nome DNS ou endereço IP.
KLNAGENT_PROXY_LOGIN	Não	Define o nome de usuário usado para fazer login no servidor proxy.	Qualquer nome de usuário existente.
KLNAGENT_PROXY_PASSWORD	Não	Define a senha de usuário usada para o login no servidor proxy.	Qualquer conjunto de caracteres alfanuméricos permitido pelo formato de senha no sistema operacional.
KLNAGENT_VM_VDI	Não	Define se o Agente de Rede está instalado em uma imagem para criação de máquinas virtuais dinâmicas.	1 – O Agente de Rede é instalado em uma imagem, usada posteriormente para a criação de máquinas virtuais dinâmicas. Outro – Nenhuma imagem é usada durante a instalação.
KLNAGENT_VM_OPTIMIZE	Não	Define se as configurações do Agente de Rede são ideais para o hypervisor.	1 – As configurações locais padrão do Agente de Rede são modificadas para permitir o uso otimizado no hypervisor.
KLNAGENT_TAGS	Não	Lista as tags atribuídas à instância do Agente de Rede.	Um ou vários nomes de tag separados por ponto e vírgula.
KLNAGENT_UDP_PORT	Não	Define a porta UDP usada pelo Agente de Rede. O valor padrão é 15000.	Qualquer número de porta existente.
KLNAGENT_PORT	Não	Define a porta não TLS usada pelo Agente de Rede. O valor padrão é 14000.	Qualquer número de porta existente.
KLNAGENT_SSLPORT	Não	Define a porta TLS usada pelo Agente de Rede. O valor padrão é 13000.	Qualquer número de porta existente.
KLNAGENT_USESSL	Não	Define se o TLS (Transport Layer Security) é usado para conexão.	1 (padrão) – O TLS é usado. Outro – O TLS não é usado.

KLNAGENT_GW_MODE	Não	Define se o gateway de conexão é usado.	1 (padrão) – As configurações atuais não são modificadas (na primeira chamada, nenhum gateway de conexão é especificado). 2 – Nenhum gateway de conexão é usado. 3 – O gateway de conexão é usado. KLNAGENT_GW_ADDRESS é necessário. 4 – A instância do Agente de Rede é usada como gateway de conexão na zona desmilitarizada (DMZ). O certificado do servidor é necessário.
KLNAGENT_GW_ADDRESS	Não	Define o endereço do gateway de conexão. O valor é aplicável apenas se KLNAGENT_GW_MODE=3.	Nome DNS ou endereço IP.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Não	Permite executar o registro do usuário como um utilitário de proprietário do dispositivo após a instalação do Agente de Rede. Caso esteja desativado, o registro como proprietário do dispositivo não estará disponível para o usuário.	1 – O registro do usuário como um utilitário de proprietário do dispositivo será executado após a instalação do Agente de Rede. Outro – Desativado.
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	Não	Define se as atualizações baixadas para o Agente de Rede com status *Indefinido* devem ser instaladas automaticamente.	true (padrão) - as atualizações são instaladas automaticamente. falso - as atualizações não são instaladas automaticamente.

3. Execute a instalação do Agente de Rede. A variável de ambiente KLAUTOANSWERS, que especifica o caminho para o arquivo de resposta, é fornecida ao comando de instalação. Execute um dos seguintes comandos:

   - Para instalar o Agente de Rede usando um pacote RPM em um sistema operacional de 32 bits, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> yum install ./klnagent-<número da compilação>.i386.rpm`

   - Para instalar o Agente de Rede usando um pacote RPM em um sistema operacional de 64 bits, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> yum install ./klnagent64-<número da compilação>.x86_64.rpm`

   - Para instalar o Agente de Rede usando um pacote RPM em um sistema operacional de 64 bits para arquitetura Arm, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> yum install ./klnagent64-<número da compilação>.aarch64.rpm`

   - Para instalar o Agente de Rede usando um pacote DEB em um sistema operacional de 32 bits, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> apt install ./klnagent_<número da compilação>_i386.deb`

- Para instalar o Agente de Rede usando um pacote DEB em um sistema operacional de 64 bits, execute o seguinte comando:
  `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> apt install ./klnagent64_<número da compilação>_amd64.deb`

- Para instalar o Agente de Rede usando um pacote DEB em um sistema operacional de 64 bits para arquitetura Arm, execute o seguinte comando:
  `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> apt install ./klnagent64_<número da compilação>_arm64.deb`

Dependendo da configuração do sistema operacional, você também pode usar os gerenciadores de pacotes rpm, dpkg ou dnf para instalar o Agente de Rede.

A instalação do Agente de Rede para Linux inicia no modo silencioso; o usuário não é solicitado a executar nenhuma ação durante o processo.

Instalação do Agente de Rede para Linux no modo interativo

Este artigo descreve passo a passo como instalar o Agente de Rede, ao especificar os parâmetros de instalação em dispositivos Linux no modo interativo. Como alternativa, é possível usar um arquivo de resposta, um arquivo de texto que contém um conjunto personalizado de parâmetros de instalação: variáveis e seus respectivos valores. O uso do arquivo de resposta permite executar a instalação no modo silencioso, ou seja, sem a participação do usuário.

Antes de instalar o Agente de Rede em um dispositivo baseado em Linux, você deve concluir as etapas preparatórias gerais que são necessárias para todos os dispositivos baseados em Linux.

Depois de concluir as etapas gerais, você pode seguir as instruções adicionais específicas do seu sistema operacional:

- Preparação de um dispositivo que executa o SUSE Linux Enterprise Server 15
- Preparação de um dispositivo que executa o Astra Linux no modo de ambiente de software fechado
- Preparação de um dispositivo que executa o Ubuntu Server/Desktop versão 10.04 e 16.04
- Preparar um dispositivo que executa um sistema operacional Linux com glibc 2.5

Para instalar o Agente de Rede no modo interativo:

1. Execute a instalação do Agente de Rede. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:

   - Para instalar o Agente de Rede com um pacote RPM para um sistema operacional de 32 bits:
     `# yum -i klnagent-<número da compilação>.i386.rpm`

   - Para instalar o Agente de Rede com um pacote RPM para um sistema operacional de 64 bits:
     `# yum -i klnagent64-<número da compilação>.x86_64.rpm`

   - Para instalar o Agente de Rede com um pacote RPM para um sistema operacional de 64 bits para a arquitetura Arm:
     `# yum -i klnagent64-<número da compilação>.aarch64.rpm`

- Para instalar o Agente de Rede com um pacote DEB para um sistema operacional de 32 bits:

  `# apt install ./klnagent_<número da compilação>_i386.deb`

- Para instalar o Agente de Rede com um pacote DEB para um sistema operacional de 64 bits:

  `# apt install ./klnagent64_<número da compilação>_amd64.deb`

- Para instalar o Agente de Rede com um pacote DEB para um sistema operacional de 64 bits para a arquitetura Arm:

  `# apt install ./klnagent64_<número da compilação>_arm64.deb`

2. Execute a configuração do Agente de Rede:

   `# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`

3. Leia o Contrato de Licença do Usuário Final. O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite um dos seguintes valores:

   - Digite `y` (sim), se você entende e aceita integralmente os termos do EULA.
   - Digite `n` (não) se você não aceita os termos do EULA. Para usar o Agente de Rede, é necessário aceitar os termos do EULA.
   - Insira `r` para mostrar o EULA novamente.

4. Digite o nome DNS do Servidor de Administração ou o endereço IP.

5. Digite o número da porta do Servidor de Administração. O número da porta padrão é 14000.

6. Digite o número da porta SSL do Servidor de Administração. O número da porta padrão é 13000.

7. Insira `y` caso queira usar a criptografia SSL para o tráfego entre o Agente de Rede e o Servidor de Administração. Caso contrário, insira `n`.

8. Selecione uma das seguintes opções para configurar o Agente de Rede:

   - `[1] – Keep current connection gateway settings`.

     As configurações do gateway de conexão são preservadas durante as atualizações. Na instalação inicial, o gateway de conexão não é configurado.

   - `[2] – Do not use connection gateway.`

     Seu dispositivo não se conectará com o Servidor de Administração por meio de um gateway de conexão.

   - `[3] –Connect to server using connection gateway`.

     Seu dispositivo se conectará com o Servidor de Administração por meio de um gateway de conexão.

   - `[4] – Use as connection gateway`.

     Seu dispositivo atuará como um gateway de conexão.

O Agente de Rede está instalado em um dispositivo Linux.

O suporte do sistema de arquivos reverte para dispositivos com o Agente de Rede

O Kaspersky Security Center Linux é um aplicativo distribuído. Reverter o sistema de arquivos a um estado anterior em um dispositivo com o Agente de Rede instalado resultará na dessincronização e no funcionamento impróprio do Kaspersky Security Center Linux.

O sistema de arquivos (ou uma parte dele) pode ser revertido nos seguintes casos:

- Ao copiar uma imagem do disco rígido.
- Ao restaurar um estado da máquina virtual por meio da infraestrutura virtual.
- Ao restaurar os dados de uma cópia de backup ou de um ponto de recuperação.

Cenários em que software de terceiros em dispositivos com o Agente de Rede instalado afetam o diretório /var/opt/kaspersky/klnagent são apenas cenários críticos para o Kaspersky Security Center Linux. Portanto, você sempre deve excluir esta pasta do procedimento de recuperação, se possível.

Como as regras do local de trabalho de algumas organizações oferecem a possibilidade para a reversão do sistema de arquivos em dispositivos, o suporte para a reversão do sistema de arquivos em dispositivos com o Agente de Rede instalado foi adicionado ao Kaspersky Security Center Linux, começando com a versão 10 Maintenance Release 1 (o Servidor de Administração e os Agentes de Rede devem ser da versão 10 Maintenance Release 1 ou posterior). Quando detectado, estes dispositivos são automaticamente reconectados ao Servidor de Administração com a total limpeza dos dados e a total sincronização.

Por padrão, o suporte à detecção de reversão do sistema de arquivos está ativado no Kaspersky Security Center Linux.

Sempre que possível, evite reverter o diretório /var/opt/kaspersky/klnagent em dispositivos com o Agente de Rede instalado, porque a ressincronização completa de dados exige uma grande quantidade de recursos.

A reversão do estado de sistema não é absolutamente permitida em um dispositivo com o Servidor de Administração instalado. A reversão do banco de dados também não é usada pelo Servidor de Administração.

Você pode restaurar um estado do Servidor de Administração a partir de uma cópia de backup somente com o utilitário klbackup padrão.

Instalação do Agente de Rede para Windows

Você também pode instalar o Agente de Rede em dispositivos Windows de uma organização para gerenciá-los usando o Servidor de Administração.

No Microsoft Windows XP, o Agente de Rede pode não executar as seguintes operações corretamente: baixar atualizações diretamente dos servidores da Kaspersky (como um ponto de distribuição); funcionar como servidor proxy da KSN (como um ponto de distribuição); e detectar vulnerabilidades de terceiros (caso o Gerenciamento de patches e vulnerabilidades seja usado).

Antes de instalar o Agente de Rede em um dispositivo executando o Microsoft Windows on Arm, assegure-se de que nenhum Agente de Rede para Microsoft Windows x86-64 já esteja instalado. Caso contrário, a instalação falhará.

Existem os seguintes métodos para instalar inicialmente o Agente de Rede no dispositivo gerenciado pelo Windows:

- Ao executar a tarefa de instalação remota pelo ponto de distribuição do Windows.

  Antes de executar uma instalação remota em um dispositivo Windows não atribuído, um ponto de distribuição baseado em Windows verifica automaticamente a porta UDP 137 para determinar o tipo do sistema operacional do dispositivo de destino. Se a porta UDP 137 estiver indisponível, o ponto de distribuição tentará se conectar à porta TCP 445 no dispositivo de destino, necessária para executar a instalação.

- Ao usar o pacote de instalação do Windows (MSI) para o Agente de Rede, com ferramentas de terceiros instalar aplicativos de maneira remota.

- Ao executar o instalador do aplicativo no dispositivo gerenciado.

- Com o envio de links para os usuários de dispositivo para o acesso aos pacotes independentes pelo Kaspersky Security Center Linux. Os pacotes independentes são módulos executáveis que contêm os pacotes de distribuição de aplicativos selecionados com as suas configurações definidas.

Instalando o Agente de Rede para Windows no modo interativo

Para instalar o Agente de Rede em um dispositivo localmente:

1. No dispositivo, execute o arquivo ksc_<número da versão>.<número da compilação>_full_<idioma de localização>.exe do pacote de distribuição baixado da Internet.

   Uma janela é exibida, solicitando que você selecione os aplicativos Kaspersky para instalar.

2. Na janela de seleção do aplicativo, clique no link **Instalar somente o Agente de Rede do Kaspersky Security Center** para iniciar o assistente de instalação do Agente de Rede. Siga as etapas do Assistente.

   Enquanto o Assistente de instalação estiver sendo executado, você pode especificar as configurações avançadas do Agente de Rede (consulte embaixo).

3. Se você desejar usar seu dispositivo como um gateway de conexão para um grupo de administração específico, na janela **Gateway de conexão** do Assistente de instalação, selecione **Usar o Agente de Rede como um gateway de conexão na DMZ** como um gateway de conexão na DMZ.

4. Para configurar o Agente de Rede durante a instalação em uma máquina virtual:

   a. Se você plane criar máquinas virtuais dinâmicas a partir da imagem da máquina virtual, ative o modo dinâmico do Agente de Rede para a Virtual Desktop Infrastructure (VDI). Para isso, na janela **Configurações avançadas** do Assistente de instalação, selecione a opção **Ativar modo dinâmico para VDI**.

      Ignore esta etapa se você não planeja criar máquinas virtuais dinâmicas a partir da imagem da máquina virtual.

   b. Otimizar a operação do Agente de Rede para VDI. Para isso, na janela **Configurações avançadas** do assistente de instalação, selecione a opção **Otimizar as configurações para VM**.

      A verificação de arquivos executáveis quanto à existência de vulnerabilidades ao inicializar será desativada. Também, isto desativa o envio de informações sobre os seguintes objetos ao Servidor de Administração:

      - Registro de hardware
      - Aplicativos instalados no dispositivo
      - Atualizações ao Microsoft Windows que devem ser instaladas no dispositivo cliente local
      - Vulnerabilidades de software detectadas no dispositivo local

      Além disso, você será capaz de ativar o envio destas informações nas propriedades do Agente de Rede ou nas configurações de política do Agente de Rede.

Quando o Assistente de instalação for concluído, o Agente de Rede será instalado no dispositivo.

É possível visualizar as propriedades do serviço do Agente de Rede. Ainda é possível iniciar, interromper e monitorar a atividade do Agente de Rede através de ferramentas padrão do Microsoft Windows: Gerenciamento do computador\Serviços.

Instalar o Agente de Rede para Windows no modo silencioso

O Agente de Rede pode ser instalado no modo silencioso, ou seja, sem a inserção interativa dos parâmetros de instalação. A instalação silenciosa usa um pacote do Windows Installer (MSI) para o Agente de Rede. O arquivo MSI está localizado no pacote de distribuição do Kaspersky Security Center Linux, na pasta Packages\NetAgent\exec.

A instalação do Agente de Rede a partir do pacote MSI só é possível no modo silencioso, pois não é possível realizar a instalação interativa a partir do pacote MSI.

Para instalar o Agente de Rede em um dispositivo local no modo silencioso:

1. Leia o Contrato de Licença do Usuário Final. Use o comando abaixo somente entende e aceita os termos do Contrato de Licença do Usuário Final.

2. Execute o comando

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

onde `setup_parameters` corresponde a uma lista de parâmetros e seus valores respectivos separados por um espaço (`PROP1=PROP1VAL PROP2=PROP2VAL`).

Na lista de parâmetros, é preciso incluir `EULA=1`. Caso contrário, o Agente de Rede não será instalado.

Caso esteja usando as configurações de conexão padrão do Kaspersky Security Center e do Agente de Rede em dispositivos remotos, execute o comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` é a chave para gravar registros. O log é criado durante a instalação do Agente de Rede e salvo em C:\windows\temp\nag_inst.log.

Além do nag_inst.log, o aplicativo cria o arquivo $klssinstlib.log, que contém o log de instalação. Esse arquivo está armazenado na pasta %windir%\temp ou %temp%. Para fins de solução de problemas, você ou um especialista do Suporte Técnico da Kaspersky podem precisar dos dois arquivos de log – nag_inst.log e $klssinstlib.log.

Se você precisar especificar adicionalmente a porta para a conexão ao Servidor de Administração, execute o comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

O parâmetro `SERVERPORT` corresponde ao número da porta para conexão ao Servidor de Administração.

Os nomes e os valores possíveis de parâmetros que podem ser usados quando o Agente de Rede for instalado no modo silencioso são listados na seção Parâmetros de instalação do Agente de Rede.

Se você quiser atualizar o Agente de Rede usando o Windows Installer, execute o seguinte comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Implementação ao capturar e copiar a imagem de um dispositivo

Caso necessite instalar o Agente de Rede em dispositivos nos quais um sistema operacional e outro software também devem ser instalados (ou reinstalados), será possível usar o mecanismo de captura e copiar a imagem daquele dispositivo.

Para realizar a implementação capturando e copiando um disco rígido:

1. Crie um dispositivo de referência com um sistema operacional e o software relevante instalado, incluindo o Agente de Rede e um aplicativo de segurança.

2. Capture a imagem de referência no dispositivo e distribua essa imagem nos novos dispositivos através da tarefa dedicada do Kaspersky Security Center Linux.

   Para capturar e instalar imagens de disco, use as ferramentas de terceiros disponíveis na organização.

Copiar uma imagem do disco com ferramentas de terceiros

Ao aplicar ferramentas de terceiros para capturar a imagem de um dispositivo com o Agente de Rede instalado, use um dos seguintes métodos:

- No dispositivo de referência, pare o serviço Agente de Rede e execute o utilitário klmover com a chave `-dupfix`. O utilitário klmover está incluído no pacote de instalação do Agente de Rede. Evite qualquer execuções subsequentes do serviço Agente de Rede até que a operação de captura da imagem seja concluída.
- Certifique-se de que o utilitário klmover seja executado com a chave `-dupfix` antes da primeira execução do serviço Agente de Rede nos dispositivos de destino. Esse é um requisito obrigatório e deve ser feito na primeira inicialização do sistema operacional após a implementação da imagem. O utilitário klmover está incluído no pacote de instalação do Agente de Rede.
- Use o modo de clonagem do disco do Agente de Rede.

Caso a imagem da unidade de disco rígido tenha sido copiada incorretamente, é possível solucionar o problema.

Também é possível capturar a imagem de um dispositivo sem que o Agente de Rede esteja instalado. Para fazer isso, execute a implementação de imagem em dispositivos de destino e, a seguir, implemente o Agente de Rede. Caso esteja usando esse método, forneça acesso à pasta de rede com os pacotes de instalação independentes a partir de um dispositivo.

Modo de clonagem do disco do Agente de Rede

Clonar o disco rígido de um dispositivo de referência é um método popular de instalação de software em novos dispositivo. Se o Agente de Rede estiver sendo executado no modo padrão no disco rígido do dispositivo de referência, o seguinte problema surge:

Após a imagem do disco de referência com o Agente de Rede ter sido implementada em novos dispositivos, eles serão exibidos no Kaspersky Security Center Web Console como um único dispositivo. Este problema surge porque o procedimento de clonagem faz com que os novos dispositivos mantenham os dados internos idênticos. Isso permite ao Servidor de Administração associar um dispositivo com o seu próprio registro no Kaspersky Security Center Web Console.

O *Modo de clonagem do disco do Agente de Rede* especial permite evitar os problemas com uma exibição incorreta de novos dispositivos no Kaspersky Security Center Web Console após a clonagem. Use este modo ao implementar o software (com o Agente de Rede) em novos dispositivos clonando o disco.

No modo de clonagem do disco, o Agente de Rede continua a ser executado, mas ele não se conecta ao Servidor de Administração. Ao sair do modo de clonagem, o Agente de Rede exclui os dados internos que fazem com que o Servidor de Administração associe múltiplos dispositivos com um registro único no Kaspersky Security Center Web Console. Para concluir a clonagem da imagem do dispositivo de referência, os novos dispositivos são exibidos corretamente no Kaspersky Security Center Web Console (com registros individuais).

Cenário de uso do modo de clonagem do disco do Agente de Rede

1. O administrador instala o Agente de Rede no dispositivo de referência.
2. O administrador verifica a conexão do Agente de Rede com o Servidor de Administração usando o utilitário klnagchk.
3. O administrador ativa o modo de clonagem do disco do Agente de rede.
4. O administrador instala software e os patches no dispositivo, e reinicia-o quantas vezes for necessário.
5. O administrador clona o disco rígido do dispositivo de referência em qualquer número de dispositivos.
6. Cada cópia clonada deve atender as seguintes condições:
   a. O nome do dispositivo precisa ser alterado.
   b. O dispositivo deve ser reiniciado.
   c. O modo de clonagem de disco deve ser desativado.

Ativar e desativar o modo de clonagem do disco usando o utilitário klmover

Para ativar ou desativar o modo de clonagem do disco do Agente de rede:

1. Execute o utilitário klmover no dispositivo com o Agente de Rede instalado que você precisar clonar.
   O utilitário klmover está localizado na pasta Instalação do Agente de Rede.
2. Para ativar o modo de clonagem do disco, insira o seguinte comando no shell de comando do Linux:
   `./klmover -cloningmode 1`
   O Agente de Rede alterna para o modo de clonagem do disco.
3. Para solicitar o status atual do modo de clonagem do disco, insira o seguinte comando no prompt de comando:
   `./klmover -cloningmode`
   A janela do utilitário mostra se o modo de clonagem do disco está ou não ativado.
4. Para desativar o modo de clonagem do disco, insira o seguinte comando na linha de comando do utilitário:
   `./klmover -cloningmode 0`

Parâmetros de instalação do Agente de Rede

A tabela abaixo descreve as propriedades MSI que você pode configurar ao instalar o Agente de Rede. Todos os parâmetros são opcionais, exceto para o EULA e SERVERADDRESS.

Propriedade de MSI	Descrição	Valores disponíveis
EULA	Aceitação dos termos do Contrato de Licença	• 1 – Confirmo que li, entendi e aceito totalmente os termos e condições deste Contrato de Licença de Usuário Final. • 0 – Eu não aceito os termos do Contrato de Licença (a instalação não é executada). • Nenhum valor – Eu não aceito os termos do Contrato de Licença (a instalação não é executada).
DONT_USE_ANSWER_FILE	Ler as configurações de instalação a partir do arquivo de resposta	• 1 – Não usar. • Outro valor ou sem valor – Leitura.
INSTALLDIR	Caminho para a pasta de instalação do Agente de Rede	Valor da sequência de caracteres.
SERVERADDRESS	Endereço do Servidor de Administração (necessário)	Valor da sequência de caracteres.
SERVERPORT	Número de uma porta para conexão ao Servidor de Administração	Valor numérico.
SERVERSSLPORT	Número da porta para a conexão criptografada ao Servidor de Administração usando protocolo SSL	Valor numérico.
USESSL	Decida se deseja usar uma conexão SSL	• 1 – Usar. • Outro valor ou sem valor – Não usar.
OPENUDPPORT	Decida se deseja abrir uma porta UDP	• 1 – Abrir. • Outro valor ou sem valor – Não abrir.
UDPPORT	Número da porta UDP	Valor numérico.
USEPROXY	Se um servidor proxy deve ser usado.	• 1 – Usar. • Outro valor ou sem valor – Não usar.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Endereços de proxy e número de uma porta para conexão ao servidor de proxy	Valor da sequência de caracteres.
PROXYLOGIN	Conta para a conexão ao servidor proxy	Valor da sequência de caracteres.
PROXYPASSWORD	Senha da conta para conexão ao servidor proxy (Não especifique nenhum detalhe de contas privilegiadas nos parâmetros dos pacotes de instalação.)	Valor da sequência de caracteres.
GATEWAYMODE	Modo de uso do gateway de conexão	• 0 – Não usar gateway de conexão. • 1 – Usar este Agente de Rede como gateway de conexão. • 2 – Conectar-se ao Servidor de Administração usando o gateway de conexão.
GATEWAYADDRESS	Endereço gateway-conexão	Valor da sequência de caracteres.
CERTSELECTION	Método para receber um certificado	• GetOnFirstConnection – Receber um certificado a partir do Servidor de Administração. • GetExistent – Especificar um certificado existente. Caso essa opção seja selecionada, a propriedade CERTFILE deve ser definida.
CERTFILE	Caminho para o arquivo do certificado	Valor da sequência de caracteres.
VMVDI	Ativar o modo dinâmico para a Virtual Desktop Infrastructure (VDI)	• 1 – Ativar. • 0 - Não ativar. • Sem valor – Não ativar.
LAUNCHPROGRAM	Decida se deseja iniciar o serviço Agente de Rede após a instalação. O parâmetro é ignorado se VMVDI=1	• 1 – Iniciar. • Outro valor ou sem valor – Não iniciar.
NAGENTTAGS	Tag para o Agente de Rede (tem prioridade sobre a tag fornecida no arquivo de resposta)	Valor da sequência de caracteres.

Instalação de aplicativos usando a tarefa de instalação remota

O Kaspersky Security Center Linux permite instalar aplicativos em dispositivos remotamente, usando tarefas de instalação remotas. Essas tarefas são criadas e atribuídas aos dispositivos por um assistente dedicado. Para atribuir uma tarefa com mais rapidez e facilidade, é possível especificar dispositivos (até mil) na janela do assistente de uma das seguintes formas:

- **Atribuir tarefa a um grupo de administração**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em um grupo de administração anteriormente criado.
- **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**. Você pode especificar nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.
- **Atribuir tarefa a uma seleção de dispositivos**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em uma seleção anteriormente criada. Você pode especificar a seleção padrão ou uma personalizada que você criou. Só é possível selecionar até mil dispositivos.

Para evitar problemas que podem ocorrer durante a instalação do aplicativo em um dispositivo cliente no qual o Agente de Rede não foi instalado, será necessário prosseguir conforme o descrito em implementação forçada por meio da tarefa de instalação remota do Kaspersky Security Center Linux.

Sobre as tarefas de instalação remotas no Kaspersky Security Center Linux

O Kaspersky Security Center Linux fornece vários mecanismos para a instalação remota de aplicativos, que são implementados como tarefas de instalação remotas (instalação forçada, instalação por meio de cópia de uma imagem de disco rígido, instalação por meio de políticas de grupo do Microsoft Windows). É possível criar uma tarefa de instalação remota para um grupo de administração especificado e para dispositivos específicos ou para uma seleção de dispositivos (essas tarefas são exibidas no Kaspersky Security Center Web Console, na pasta **Tarefas**). Ao criar uma tarefa, você pode selecionar pacotes de instalação (aqueles do Agente de Rede e / ou outro aplicativo) a ser instalado dentro desta tarefa, assim como especificar determinadas configurações que definem o método da instalação remota. Além disso, você pode usar o Assistente de instalação remota, que tem base na criação de uma tarefa de instalação remota e no monitoramento dos resultados.

As tarefas para grupos de administração afetam ambos os dispositivos incluídos em um grupo especificado e todos os dispositivos em todos os subgrupos dentro daquele grupo de administração. Uma tarefa cobre dispositivos de Servidores de Administração secundários incluídos em um grupo ou algum dos seus subgrupos se a configuração correspondente estiver ativada na tarefa.

As tarefas para dispositivos específicos atualizam a lista de dispositivos cliente em cada execução de acordo com o conteúdo da seleção no momento em que a tarefa é iniciada. Se uma seleção incluir dispositivos que foram conectados aos Servidores de Administração secundários, a tarefa também será executada naqueles dispositivos. Para obter detalhes sobre aquelas configurações e métodos de instalação, consulte abaixo nesta seção.

Para certificar-se do sucesso de uma tarefa de instalação remota nos dispositivos conectados aos Servidores de Administração secundários, você deve usar a tarefa de encaminhamento para encaminhar os pacotes de instalação usados por sua tarefa aos Servidores de Administração secundários correspondentes com antecedência.

Instalar um aplicativo remotamente

Esta seção contém informações sobre como instalar um aplicativo nos dispositivos em um grupo de administração, dispositivos com endereços específicos ou uma seleção de dispositivos gerenciados.

Para instalar um aplicativo nos dispositivos específicos:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.
3. No campo **Tipo de tarefa**, selecione **Instalar o aplicativo remotamente**.
4. Escolha uma das seguintes opções:

   Atribuir tarefa a um grupo de administração

   A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

   Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

   Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

   Especificar endereços de dispositivos manualmente ou importar endereços de uma lista

   Você pode especificar nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

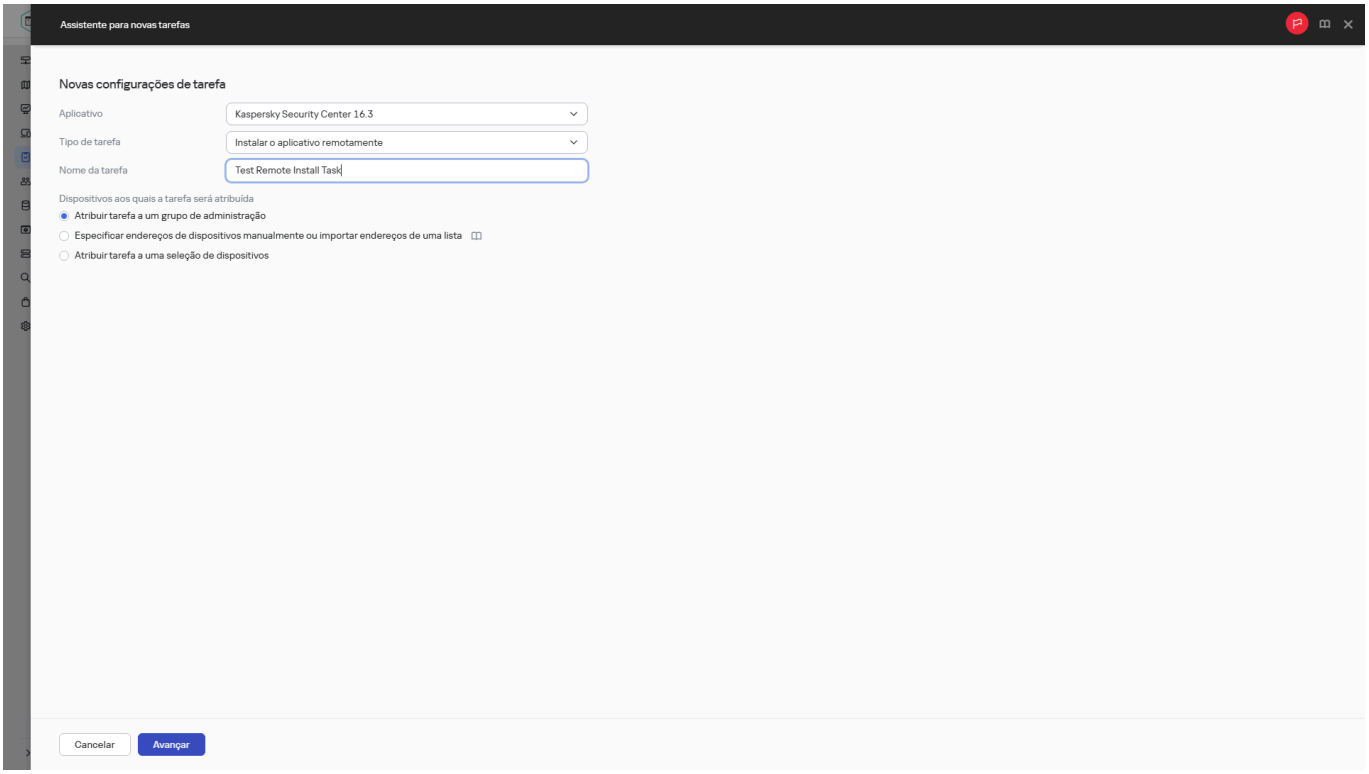
   Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

   Atribuir tarefa a uma seleção de dispositivos

   A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

   Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

A tarefa *Instalar aplicativo remotamente* é criada para os dispositivos especificados. Se você selecionou a opção **Atribuir tarefa a um grupo de administração**, a tarefa será de grupo.



Criação da tarefa Instalar o aplicativo remotamente

5. Na etapa **Escopo da tarefa**, especifique um grupo de administração, dispositivos com endereços específicos ou uma seleção de dispositivos gerenciados.

   As configurações disponíveis dependem da opção selecionada na etapa anterior.

6. Na etapa **Pacotes de instalação**, especifique as seguintes configurações:

   - No campo **Selecione o pacote de instalação**, selecione o pacote de instalação de um aplicativo que deseja instalar.

   - No grupo de configurações **Forçar download do pacote de instalação**, especifique como os arquivos que são necessários para instalar um aplicativo são distribuídos nos dispositivos cliente:

     Usando o Agente de Rede

     Se esta opção de seleção estiver ativada, os pacotes de instalação são entregues aos dispositivos clientes pelo Agente de Rede instalado neles.

     Caso esta opção estiver desativada, os pacotes de instalação serão entregues usando as ferramentas do sistema operacional dos dispositivos clientes.

     Recomendamos que você ative esta opção se a tarefa tiver sido atribuída a dispositivos com o Agente de Rede instalado.

     Por padrão, esta opção está ativada.

     Usando recursos do sistema operacional através de pontos de distribuição

     Se a caixa de seleção estiver marcada, os pacotes de instalação serão entregues aos dispositivos clientes usando os mecanismos do sistema operacional por meio de um ponto de distribuição. Você pode selecionar esta opção se houver, no mínimo, um ponto de distribuição na rede.

     Se opção **Uso do Agente de Rede** estiver ativada, os arquivos serão entregues pelas ferramentas do sistema operacional, apenas se os recursos do Agente de Rede estiverem indisponíveis.

Por padrão, esta opção está ativada para as tarefas de instalação remotas que são criadas em um Servidor de Administração virtual.

A única maneira de instalar um aplicativo para Windows (inclusive o Agente de Rede para Windows) em um dispositivo que não tenha o Agente de Rede instalado é usando um ponto de distribuição baseado no Windows. Portanto, ao instalar um aplicativo do Windows:

- Selecione esta opção.
- Verifique e confirme se um ponto de distribuição foi atribuído aos dispositivos clientes de destino.
- Verifique se o ponto de distribuição é baseado em Windows.

Usando recursos do sistema operacional através do Servidor de Administração

Caso esta opção esteja ativada, os arquivos serão transmitidos para os dispositivos clientes usando as ferramentas do sistema operacional pelo Servidor de Administração. Você pode ativar esta opção se nenhum Agente de Rede estiver instalado no dispositivo cliente, mas esse está na mesma rede que o Servidor de Administração.

Por padrão, esta opção está ativada.

- No campo **Número máximo de downloads concomitantes**, especifique o número máximo permitido de dispositivos clientes para os quais o Servidor de Administração pode transmitir os arquivos simultaneamente.
- No campo **Número máximo de tentativas de instalação**, especifique o número máximo permitido de execuções do instalador.

  Caso o número de tentativas especificado no parâmetro seja excedido, o Kaspersky Security Center Linux não iniciará mais o instalador no dispositivo. Para reiniciar a tarefa *Instalar aplicativo remotamente*, aumente o valor do parâmetro **Número máximo de tentativas de instalação** e inicie a tarefa. Alternativamente, é possível criar uma nova tarefa de *Instalação remota de aplicativo*.
- Caso migre de um aplicativo da Kaspersky para outro e seu aplicativo atual esteja protegido por senha, insira a senha no campo **Senha para desinstalar o aplicativo da Kaspersky atual**. Observe que, durante a migração, o aplicativo atual da Kaspersky será desinstalado.

  O campo **Senha para desinstalar o aplicativo da Kaspersky atual** só estará disponível se a opção **Usando o Agente de Rede** tiver sido selecionada no grupo de configurações **Forçar download do pacote de instalação**.

  Você pode usar a senha de desinstalação somente para o cenário de migração do Kaspersky Security for Windows Server para o Kaspersky Endpoint Security for Windows ao instalar o Kaspersky Endpoint Security for Windows usando a tarefa Instalar aplicativo remotamente. Usar a senha de desinstalação ao instalar outros componentes pode causar erros de instalação.

  Para concluir o cenário de migração com êxito, certifique-se de que os seguintes pré-requisitos sejam atendidos:

  - Você está usando o Agente de Rede do Kaspersky Security Center 14.2 for Windows ou posterior.
  - Você está instalando o aplicativo em dispositivos que executam o Windows.
- Defina as configurações adicionais:

Não reinstalar o aplicativo se ele já estiver instalado

Se esta opção estiver ativada, o aplicativo selecionado não será reinstalado se já estiver instalado neste dispositivo cliente.

Se esta opção não estiver ativada, o aplicativo será instalado de qualquer forma.

Por padrão, esta opção está ativada.

Verificar o tipo do sistema operacional antes de baixar

Antes de transmitir os arquivos para dispositivos clientes, o Kaspersky Security Center Linux verifica se as configurações do utilitário de instalação são aplicáveis ao sistema operacional do dispositivo cliente. Caso as configurações não sejam aplicáveis, o Kaspersky Security Center Linux não transmitirá os arquivos e não tentará instalar o aplicativo. Por exemplo, para instalar algum aplicativo em dispositivos de um grupo de administração que inclui dispositivos que executam vários sistemas operacionais, é possível atribuir a tarefa de instalação ao grupo de administração e então ativar essa opção para ignorar os dispositivos que executem um sistema operacional diferente do requerido.

Quando você faz a instalação remota do Agente de Rede em dispositivos não atribuídos, o Kaspersky Security Center Linux ou um ponto de distribuição determina automaticamente o tipo do sistema operacional do dispositivo, sem considerar a configuração **Verificar o tipo do sistema operacional antes de baixar**.

Atribuir a instalação do pacote em políticas de grupo do Active Directory

Se esta opção estiver ativada, é instalado um pacote de instalação, usando as políticas de grupo do Active Directory.

Essa opção fica disponível se o pacote de instalação do Agente de Rede estiver selecionado.

Por padrão, esta opção está desativada.

Solicitar aos usuários o fechamento de aplicativos em execução

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

- Selecione em quais dispositivos deseja instalar o aplicativo:

  Instalar em todos os dispositivos

  O aplicativo será instalado até mesmo nos dispositivos gerenciados por outros Servidores de Administração.

  Esta opção está marcada por padrão. Não é preciso alterar essa configuração se houver somente um Servidor de Administração na rede.

  Instalar somente em dispositivos gerenciados por este Servidor de Administração

  O aplicativo será instalado somente nos dispositivos gerenciados por este Servidor de Administração. Selecione esta opção se você tiver mais de um Servidor de Administração na rede e deseja evitar conflitos entre eles.

- Especifique se os dispositivos devem ser movidos para um grupo de administração depois da instalação:

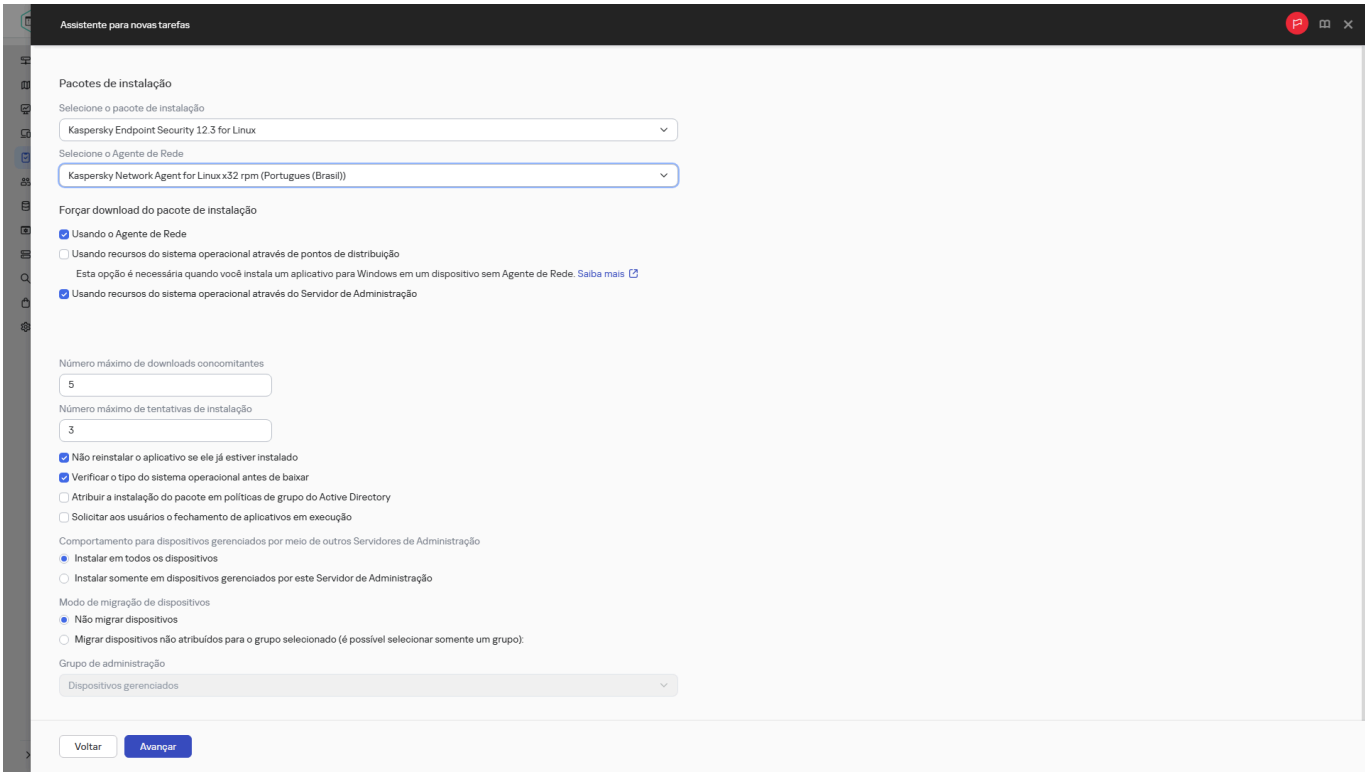
Não migrar dispositivos

Os dispositivos permanecem nos grupos nos quais eles estão atualmente localizados. Os dispositivos que não foram colocados em nenhum grupo continuam não atribuídos.

Migrar dispositivos não atribuídos para o grupo selecionado (é possível selecionar somente um grupo)

Os dispositivos são movidos para o grupo de administração selecionado.

A opção **Não migrar dispositivos** está marcada por padrão. Por motivos de segurança, você pode desejar mover os dispositivos manualmente.



Especificação das configurações da tarefa

7. Nesta etapa do assistente, especifique se os dispositivos devem ser reiniciados durante a instalação de aplicativos:

   Não reiniciar o dispositivo

   Se esta opção for selecionada, o dispositivo não será reiniciado após a instalação do aplicativo de segurança.

   Reiniciar o dispositivo

   Se esta opção for selecionada, o dispositivo será reiniciado após a instalação do aplicativo de segurança.

8. Caso necessário, na etapa **Selecionar contas para acessar os dispositivos**, adicione as contas que serão usadas para iniciar a tarefa *Instalar aplicativo remotamente*:

   Nenhuma conta necessária (Agente de Rede instalado)

   Se essa caixa de seleção estiver selecionada, você não precisará especificar uma conta sob a qual o instalador do aplicativo será executado. A tarefa será executada sob a conta sob a qual o serviço do Servidor de Administração está sendo executado.

   Se o Agente de Rede não tiver sido instalado em dispositivos clientes, esta opção não estará disponível.

   Conta necessária (Agente de Rede não é usado)

Selecione esta opção se o Agente de Rede não estiver instalado nos dispositivos aos quais você atribui a tarefa de instalação remota. Neste caso, é possível especificar uma conta de usuário ou um certificado SSH para instalar o aplicativo.

- **Conta local ou de domínio**. Se essa opção estiver selecionada, especifique a conta de usuário sob a qual o instalador do aplicativo será executado. Clique no botão **Adicionar**, selecione **Conta local ou de domínio** e, então, especifique as credenciais da conta do usuário.

  É possível especificar várias contas de usuário se, por exemplo, nenhuma delas tiver todos os direitos necessários em todos os dispositivos para os quais você atribui a tarefa. Nesse caso, todas as contas adicionadas são usadas para executar a tarefa, em ordem consecutiva, de cima para baixo.

- **Certificado SSH**. Se quiser instalar um aplicativo em um dispositivo cliente baseado em Linux, poderá especificar um certificado SSH em vez de uma conta de usuário. Clique no botão **Adicionar**, selecione **Certificado SSH** e, então, especifique as chaves privada e pública do certificado.

  Para gerar uma chave privada, você pode usar o utilitário ssh-keygen. Observe que o Kaspersky Security Center Linux é compatível com o formato PEM de chaves privadas, mas o utilitário ssh-keygen gera chaves SSH no formato OPENSSH por padrão. O formato OPENSSH não é compatível com o Kaspersky Security Center Linux. Para criar uma chave privada no formato PEM compatível, adicione a opção -m PEM no comando ssh-keygen. Por exemplo:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "< e-mail do usuário >"
  ```

9. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

   Se você ativou a opção **Abrir detalhes da tarefa quando a criação for concluída**, a janela de configurações da tarefa é aberta. Nesta janela, é possível verificar os parâmetros da tarefa, modificá-los ou configurar um cronograma de início da tarefa, caso necessário.

10. Na lista de tarefas, selecione a tarefa criada e clique em **Começar**.

    Como alternativa, aguarde que a tarefa seja inicializada de acordo com o agendamento especificado nas configurações da tarefa.

Quando a tarefa de instalação remota for concluída, o aplicativo selecionado será instalado nos dispositivos específicos.

Instalação remota de aplicativos em dispositivos macOS

Para instalar aplicativos em dispositivos com macOS usando uma tarefa de instalação remota:

1. Crie um arquivo compactado contendo um pacote de instalação e um script de instalação .sh.

2. Desative a opção **Verificar o tipo do sistema operacional antes de baixar** no Assistente para novas tarefas.

Como alternativa, você pode usar a tarefa **Executar scripts remotamente**. O artigo a seguir descreve como configurar arquivos para esta tarefa: Instalar aplicativos remotamente em dispositivos usando a tarefa Executar scripts remotamente.

Instalando aplicativos nos Servidores de Administração secundários

Se a versão do Servidor de Administração for 15.4 ou posterior, você poderá instalar aplicativos em um Servidor de Administração secundário somente se sua versão for 15.4 ou posterior.

Para instalar um aplicativo em Servidores de Administração secundários:

1. Estabeleça uma conexão ao Servidor de Administração que controla os Servidores de Administração secundários relevantes.

2. Certifique-se de que o pacote de instalação corresponde ao aplicativo sendo instalado em cada um dos Servidores de Administração secundários selecionados. Se você não encontrar o pacote de instalação em nenhum dos Servidores secundários, distribua-o. Para este efeito, crie uma tarefa com o tipo de tarefa **Distribuir pacote de instalação**.

3. Crie uma tarefa para uma instalação de aplicativo remoto em Servidores de Administração secundários. Selecione o tipo de tarefa **Instalar o aplicativo no Servidor de Administração secundário remotamente**.

   O Assistente para novas tarefas cria uma tarefa para instalação remota do aplicativo selecionado no assistente em Servidores de Administração secundários específicos.

4. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que especificou nas configurações da tarefa.

Quando a tarefa de instalação remota for concluída, o aplicativo selecionado será instalado nos Servidores de Administração secundários.

Instalação remota de aplicativos em dispositivos com o Agente de Rede instalado

Se um Agente de Rede operável conectado ao Servidor de Administração principal (ou a algum dos seus Servidores secundários) for instalado em um dispositivo, você poderá fazer um upgrade do Agente de Rede neste dispositivo, assim como instalar, atualizar ou remover qualquer aplicativo compatível através do Agente de Rede.

Você pode ativar a opção **Usando o Agente de Rede** nas propriedades da tarefa de instalação remota.

Se esta opção estiver selecionada, os pacotes de instalação com configurações de instalação definidas pelo administrador serão transferidos para os dispositivos alvo através dos canais de comunicação entre o Agente de Rede e o Servidor de Administração.

Para otimizar a carga do Servidor de Administração e minimizar o tráfego entre o Servidor de Administração e os dispositivos, é útil atribuir pontos de distribuição em cada rede remota ou em cada domínio emissor (consulte as seções "Sobre os pontos de distribuição" e "Criar uma estrutura de grupos de administração e atribuir pontos de distribuição"). Neste caso, os pacotes de instalação e as configurações do instalador são distribuídos a partir do Servidor de Administração para os dispositivos alvo através de pontos de distribuição.

Além disso, você pode usar pontos de distribuição para transmitir (multicast) a entrega de pacotes de instalação, que permite reduzir significativamente o tráfego de rede ao implementar aplicativos.

Ao transferir pacotes de instalação para dispositivos alvo usando os canais de comunicação entre os Agentes de Rede e o Servidor de Administração, todos os pacotes de instalação que tenham sido preparados para transferência, também serão colocados em cache na pasta /var/opt/kaspersky/klnagent_srv/1093/.working. Ao usar múltiplos grandes pacotes de instalação de vários tipos e ao envolver um grande número de pontos de distribuição, o tamanho desta pasta pode aumentar drasticamente.

Os arquivos não podem ser excluídos da pasta FTServer manualmente. Quando os pacotes de instalação originais forem excluídos, os dados correspondentes serão automaticamente excluídos da pasta FTServer.

Os dados recebidos pelos pontos de distribuição são salvos na pasta /var/opt/kaspersky/klnagent_srv/1103/.

Os arquivos não podem ser excluídos da pasta de $FTCITmp manualmente. Quando as tarefas usando dados desta pasta forem concluídas, o conteúdo desta pasta será automaticamente excluído.

Como os pacotes de instalação são distribuídos sobre os canais de comunicação entre o Servidor de Administração e os Agentes de Rede a partir de um repositório intermediário em um formato otimizado para transferências na rede, nenhuma modificação é permitida nos pacotes de instalação armazenados na pasta original de cada pacote de instalação. Estas modificações não serão automaticamente registradas pelo Servidor de Administração. Caso seja necessário modificar manualmente os arquivos de pacotes de instalação (embora seja recomendado evitar esse cenário), será necessário editar as configurações necessárias de um pacote de instalação no Kaspersky Security Center Web Console. Editar as configurações de um pacote de instalação no Kaspersky Security Center Web Console faz com que o Servidor de Administração atualize a imagem do pacote na memória no cache que foi preparado para a transferência aos dispositivos de destino.

O servidor envia solicitações de eco ICMP (o mesmo que o comando ping) para o dispositivo alvo durante a instalação remota.

O gerenciamento do dispositivo reinicia na tarefa de instalação remota

Os dispositivos muitas vezes precisam de um reinício para concluir a instalação remota de aplicativos (em particular no Windows).

Caso a tarefa de instalação remota do Kaspersky Security Center Linux seja usada, no assistente para novas tarefas ou na janela de propriedades da tarefa que foi criada (seção **Operating system restart**), será possível selecionar a ação a ser executada quando o dispositivo Windows precisar ser reiniciado:

- **Não reiniciar o dispositivo**. Neste caso, nenhum reinício automático será executado. Para concluir a instalação, você deve reiniciar o dispositivo (por exemplo, manualmente ou através da tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário serão salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas de instalação em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**. Neste caso, o dispositivo sempre é reiniciado automaticamente se um reinício for necessário para a conclusão da instalação. Esta opção é útil para tarefas de instalação em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**. O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). A opção **Perguntar ao usuário o que fazer** é a mais adequada para estações de trabalho onde os usuários precisam da possibilidade de selecionar a hora mais conveniente para um reinício.

Implementação forçada usando a tarefa de instalação remota do Kaspersky Security Center Linux

Para a implementação inicial do Agente de Rede ou de outros aplicativos, é possível forçar a instalação de pacotes selecionados usando a tarefa de instalação remota do Kaspersky Security Center Linux, desde que cada dispositivo tenha pelo menos uma conta de usuário com direitos de administrador local.

A instalação forçada também pode ser aplicada se os dispositivos não puderem ser diretamente acessados pelo Servidor de Administração: por exemplo, os dispositivos estão em redes isoladas ou estão em uma rede local, enquanto o item Servidor de Administração está na DMZ.

No caso de implementação inicial, o Agente de Rede não é instalado. Portanto, nas configurações da tarefa de instalação remota, não é possível selecionar a distribuição dos arquivos necessários para a instalação do aplicativo com o uso do Agente de Rede. Você só pode optar por distribuir arquivos usando recursos do sistema operacional por meio do Servidor de Administração ou pontos de distribuição.

O serviço do Servidor de Administração deve ser executado em uma conta que tenha privilégios administrativos nos dispositivos de destino. Como alternativa, é possível especificar uma conta que tenha acesso ao compartilhamento admin$ nas configurações da tarefa de instalação remota.

Por padrão, a tarefa de instalação remota é aplicada aos dispositivos usando as credenciais da conta sob a qual o Servidor de Administração está sendo executado. É importante esclarecer que esta é a conta usada para acessar o compartilhamento admin$, e não a conta na qual a tarefa de instalação remota é executada. A instalação será realizada na conta LocalSystem.

É possível especificar dispositivos de destino explicitamente (com uma lista) ao selecionar o grupo de administração do Kaspersky Security Center Linux ao qual eles pertencem; ou ao criar uma seleção de dispositivos de acordo com um critério específico. A hora início da instalação é definida pelo agendamento da tarefa. Caso a configuração **Executar tarefas ignoradas** esteja ativada nas propriedades da tarefa, a tarefa poderá ser executada imediatamente após os dispositivos de destino serem ligados ou quando eles forem movidos para o grupo de administração de destino.

A instalação forçada consiste em entregar pacotes de instalação aos dispositivos de destino, cópia subsequente de arquivos para o recurso admin$ em cada um dos dispositivos de destino e registro remoto de serviços de suporte nesses dispositivos. A entrega de pacotes de instalação aos dispositivos de destino é realizada por meio de um recurso do Kaspersky Security Center Linux que garante a interação de rede. As seguintes condições devem ser atendidas neste caso:

- Os dispositivos de destino podem ser acessados no lado do Servidor de Administração ou no lado do ponto de distribuição.
- A resolução de nomes para dispositivos de destino funciona corretamente na rede.
- Os compartilhamentos administrativos (admin$) permanecem ativados nos dispositivos-alvo.
- Os seguintes serviços do sistema estão em execução nos dispositivos de destino:
  - Server (LanmanServer)

    Por padrão, este serviço está em execução.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- A porta TCP 445 está aberta nos dispositivos de destino para permitir acesso remoto por meio do Instrumentação de Gerenciamento do Windows (WMI).

  > Os protocolos TCP 139, UDP 137 e UDP 138 são usados por protocolos mais antigos e não são mais necessários para aplicativos atuais.

  Portas de acesso de saída dinâmicas devem ser permitidas no firewall para conexões do Servidor de Administração e pontos de distribuição para dispositivos de destino.
- As configurações de segurança da política de domínio do Active Directory têm permissão para fornecer a operação do protocolo NTLM durante a implementação do Agente de Rede.
- Em dispositivos-alvo que executam o Microsoft Windows XP, o modo Compartilhamento Simples de Arquivo está desativado.
- Nos dispositivos de destino, o compartilhamento de acesso e o modelo de segurança são definidos como *Clássico: os usuários locais se autenticam como eles mesmos*. Ele não pode de forma alguma ser *apenas Visitante: os usuários locais são autenticados como Visitantes*.
- Os dispositivos-alvo são membros do domínio, ou as contas uniformes com direitos de administrador são criadas nos dispositivos-alvo com antecedência.

Para implementar com sucesso o Agente de Rede ou outros aplicativos em um dispositivo que não esteja associado a um domínio do Active Directory do Windows Server 2003 ou posterior, é necessário desativar o UAC remoto nesse dispositivo. O UAC remoto é um dos motivos que impedem que contas administrativas locais acessem admin$, o que é necessário para a implementação forçada do Agente de Rede ou de outros aplicativos. A desativação do UAC remoto não afeta o UAC local.

Durante a instalação em novos dispositivos que ainda não foram alocados em nenhum dos grupos de administração do Kaspersky Security Center Linux, é possível abrir as propriedades da tarefa de instalação remota e especificar o grupo de administração para o qual os dispositivos serão movidos após a instalação do Agente de Rede.

Ao criar uma tarefa de grupo, tenha em mente que cada tarefa de grupo afeta todos os dispositivos em todos os grupos aninhados dentro de um grupo selecionado. Portanto, você deve evitar duplicar tarefas de instalação em subgrupos.

Uma maneira simplificada de criar tarefas para a instalação forçada de aplicativos é a instalação automática. Para fazer isso, você deve abrir as propriedades do grupo de administração, abrir a lista de pacotes de instalação e selecionar aqueles que devem ser instalados nos dispositivos deste grupo. Como resultado, os pacotes de instalação selecionados serão automaticamente instalados em todos os dispositivos neste grupo e em todos os seus subgrupos. O intervalo de tempo sobre o qual os pacotes serão instalados depende da produtividade da rede e o número total de dispositivos na rede.

Para reduzir a carga no Servidor de Administração durante a entrega de pacotes de instalação a dispositivos-alvo, é possível selecionar a instalação por meio dos pontos de distribuição na tarefa de instalação. Observe que este método de instalação coloca uma carga significativa nos dispositivos que atuam como pontos de distribuição. Portanto, é recomendável selecionar os dispositivos que atendam aos requisitos para pontos de distribuição. Se você usar pontos de distribuição, precisará garantir que eles estejam presentes em cada uma das sub-redes isoladas que hospedam os dispositivos de destino.

Usando pontos de distribuição como centros de instalação locais também pode ser útil ao executar a instalação em dispositivos em sub-redes comunicadas com o Servidor de Administração através de um canal de baixa potência enquanto um canal mais amplo esteja disponível entre os dispositivos na mesma sub-rede.

O espaço livre em disco na partição com a pasta /var/opt/kaspersky/KSC_Backups* deve exceder muitas vezes o tamanho total dos pacotes de distribuição dos aplicativos instalados.

Instalando aplicativos no modo silencioso

Para instalar o aplicativo em modo silencioso:

1. No menu principal, vá para **Gerenciamento de software** → **Pacotes de instalação**.
2. Marque a caixa de seleção ao lado do pacote de instalação do aplicativo necessário ou crie um novo pacote para esse aplicativo.

   O pacote de instalação será armazenado no Servidor de Administração na pasta Serviço de pacotes que está dentro da pasta compartilhada. Uma subpasta separada corresponde a cada pacote de instalação.

3. Abra a pasta que armazena o pacote de instalação requerido de uma das seguintes formas:

   - Copiando a pasta correspondente para o pacote de instalação relevante do Servidor de Administração ao dispositivo cliente. Então abra a pasta copiada no dispositivo cliente.
   - Abrindo a partir do dispositivo cliente a pasta compartilhada que corresponde ao pacote de instalação requerido no Servidor de Administração.

Se a pasta compartilhada estiver localizada em um dispositivo com o sistema operacional Microsoft Windows Vista, selecione o valor **Desativado** para a configuração **Controle de conta do usuário: executar todos os administradores no modo de aprovação do administrador** (**Iniciar** → **Painel de Controle** → **Administração** → **Política de segurança local** → **Configurações de segurança**).

4. Dependendo do aplicativo selecionado, faça o seguinte:

   - Para Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers e Kaspersky Security Center, navegue até à subpasta exec e execute o arquivo executável (o arquivo com a extensão .exe) com uma tecla /s.

   - Para outro aplicativo da Kaspersky, rode o arquivo executável (um arquivo com a extensão .exe) com a tecla /s a partir da pasta aberta.

Executar o arquivo executável com o `EULA=1` e chaves `PRIVACYPOLICY=1` significa que você aceita os termos do Contrato de Licença e da Política de Privacidade, respectivamente. Você também está ciente de que seus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade. O texto do Contrato de Licença e da Política de Privacidade está incluído no kit de distribuição do Kaspersky Security Center Linux. Aceitar os termos do Contrato de Licença e da Política de Privacidade é necessário para instalar o aplicativo ou atualizar uma versão anterior do aplicativo.

Preparar um dispositivo macOS para a instalação remota do Agente de Rede

Existem os seguintes métodos para instalar inicialmente o Agente de Rede no dispositivo gerenciado macOS:

- Ao executar a tarefa de instalação remota no ponto de distribuição do macOS.

- Com o envio de links para os usuários de dispositivo para o acesso aos pacotes independentes pelo Kaspersky Security Center Linux. Os pacotes independentes são módulos executáveis que contêm os pacotes de distribuição de aplicativos selecionados com as suas configurações definidas.

Para preparar um dispositivo executando no macOS para a instalação remota do Agente de Rede:

1. Certifique-se de que o sudo esteja instalado no dispositivo macOS de destino.

2. Testar a configuração do dispositivo:

   a. Certifique-se de que a porta 22 esteja aberta no dispositivo cliente. Para fazer isso, nas **Preferências do Sistema**, abra o painel de **Compartilhamento** e, em seguida, verifique se a caixa de seleção **Login Remoto** está marcada.

   Você pode se conectar ao dispositivo cliente via Secure Shell (SSH) somente pela porta 22. Você não pode alterar o número da porta.

   Você pode usar o comando `ssh <nome_do_dispositivo>` para fazer login no dispositivo macOS remotamente. No painel **Compartilhamento**, você pode usar a opção **Permitir acesso para** definir o escopo dos usuários que têm acesso permitido ao dispositivo macOS.

b. Desative a senha sudo para a conta do usuário sob a qual o dispositivo deve ser conectado.

Use o comando `sudo visudo` no terminal para abrir o arquivo de configuração sudoers. No arquivo que você abriu, na entrada `User privilege specification`, especifique o seguinte: `username ALL = (ALL) NOPASSWD: ALL`. Neste caso, o campo `username` corresponde à conta de usuário, que deve ser usada para a conexão de dispositivo usando o SSH.

c. Salve o arquivo sudoers e, a seguir, feche-o.

d. Conecte-se novamente ao dispositivo pelo SSH, verifique e confirme se o serviço Sudo não solicita a inserção de uma senha. Será possível fazer isso com o uso do comando `sudo whoami`.

3. Baixar e criar um pacote de instalação:

a. Baixe o pacote de instalação do Agente de Rede usando um dos seguintes métodos:

- Através da interface do aplicativo.
- Baixando a versão relevante do Agente de Rede no site de Suporte Técnico em https://support.kaspersky.com/.
- Solicitando o pacote de instalação aos especialistas do Suporte Técnico

b. Para criar um pacote de instalação remota, use os seguintes arquivos:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. Criar uma tarefa de instalação remota com as seguintes configurações:

- Na página **Configurações** do Assistente para novas tarefas, marque a caixa de seleção **Usando recursos do sistema operacional através do Servidor de Administração**. Limpar todas as outras caixas de seleção.
- Na página **Selecionar uma conta para executar a tarefa**, para executar a tarefa, especifique as configurações da conta de usuário que são usadas para a conexão do dispositivo por meio de SSH.

O dispositivo cliente está pronto para a instalação remota do Agente de Rede por meio da tarefa correspondente que foi criada.

Infraestrutura virtual

O Kaspersky Security Center Linux é compatível com o uso de máquinas virtuais. Você pode instalar o Agente de Rede e do aplicativo de segurança em cada máquina virtual, assim como a proteção de máquinas virtuais em nível de hipervisor. No primeiro caso, você pode usar o aplicativo de segurança padrão ou o Kaspersky Security for Virtualization Light Agent para proteger suas máquinas virtuais. No segundo caso, você pode usar o Kaspersky Security for Virtualization Agentless.

O Kaspersky Security Center Linux é compatível com as reversões de máquinas virtuais ao estado anterior.

Dicas sobre como reduzir a carga em máquinas virtuais

Ao instalar o Agente de Rede em uma máquina virtual, é aconselhável considerar a desativação de alguns recursos do Kaspersky Security Center Linux que parecem ser pouco usados pelas máquinas virtuais.

Ao instalar o Agente de Rede em uma máquina virtual ou em um modelo destinado para a geração de máquinas virtuais, recomendamos executar as seguintes ações:

- Se estiver executando uma instalação remota, na janela Propriedades do pacote de instalação do Agente de Rede na seção **Avançado**, selecione a opção **Otimizar as configurações para VDI**.
- Se você estiver executando uma instalação interativa por meio de um assistente, na janela assistente, selecione a opção **Otimizar as configurações do Agente de Rede para a infraestrutura virtual**.

Selecionar essas opções alterará as configurações do Agente de Rede para que os seguintes recursos permaneçam desativados por padrão (antes da política ser aplicada):

- Recuperar informações sobre o software instalado
- Recuperar informações sobre o hardware
- Recuperar informações sobre as vulnerabilidades detectadas
- Recuperar informações sobre as atualizações necessárias

Normalmente, aqueles recursos não são necessários em máquinas virtuais porque elas usam o software uniforme e o hardware virtual.

A desativação dos recursos é irreversível. Se algum dos recursos desativados for necessário, você pode ativá-lo através da política do Agente de Rede ou através das configurações locais do Agente de Rede. As configurações locais do Agente de Rede estão disponíveis no menu de contexto do dispositivo pertinente no Kaspersky Security Center Web Console.

Suporte de máquinas virtuais dinâmicas

O Kaspersky Security Center Linux é compatível com as máquinas virtuais dinâmicas. Se uma infraestrutura virtual tiver sido implementada na rede da organização, as máquinas virtuais dinâmicas (temporárias) podem ser usadas em determinados casos. As VMs dinâmicas são criadas sob nomes únicos com base em um modelo que foi preparado pelo administrador. O usuário trabalha em uma VM durante algum tempo, então, depois ser desligada, esta máquina virtual será removida da infraestrutura virtual. Caso o Kaspersky Security Center Linux tenha sido implementado na rede da organização, uma máquina virtual com o Agente de Rede instalado será adicionada ao banco de dados do Servidor de Administração. Depois que você desliga uma máquina virtual, a entrada correspondente também deve ser removida do banco de dados do Servidor de Administração.

Para tornar funcional o recurso de remoção automática de entradas em máquinas virtuais, ao instalar o Agente de Rede em um modelo para máquinas virtuais dinâmicas, selecione a opção **Ativar modo dinâmico para VDI**:

- Para a instalação remota - na janela de propriedades do pacote de instalação do Agente de Rede (seção Avançado)
- Para a instalação interativa – No Assistente de instalação de Agente de Rede

Evite selecionar a opção **Ativar modo dinâmico para VDI** ao instalar o Agente de Rede em dispositivos físicos.

Se desejar que os eventos das máquinas virtuais dinâmicas sejam armazenados no Servidor de Administração durante algum tempo após essas máquinas virtuais serem removidas, então, na janela Propriedades do Servidor de Administração, na seção **Repositório de eventos**, selecione a opção **Armazenar eventos após a exclusão dos dispositivos** e especifique o período máximo de armazenamento para eventos (em dias).

Não recomendamos ativar a criptografia de unidade em máquinas virtuais dinâmicas.

Suporte para copiar máquinas virtuais

Copiar uma máquina virtual com o Agente de Rede instalado ou criar um a partir de um modelo com o Agente de Rede instalado, é idêntico a implementação de Agentes de Rede ao capturar e copiar uma imagem do disco rígido. Deste modo, no caso geral, ao copiar máquinas virtuais, você tem de executar as mesmas ações feitas ao implementar o Agente de Rede copiando uma imagem do disco.

No entanto, as duas caixas descritas abaixo apresentam o Agente de Rede que detecta a cópia automaticamente. Devido aos motivos acima, você não tem que executar as operações sofisticadas descritas sob "Implementar ao capturar e copiar o disco rígido de um dispositivo":

- A opção **Ativar modo dinâmico para VDI** foi selecionada durante a instalação do Agente de Rede. Após cada reinicialização do sistema operacional, esta máquina virtual será reconhecida como um novo dispositivo, independentemente de ter sido copiada ou não.
- Um dos seguintes hypervisors está em uso: VMware™, HyperV®, ou Xen®: o Agente de Rede detecta a cópia da máquina virtual através das IDs alteradas do hardware virtual.

A análise das modificações no hardware virtual não é absolutamente confiável. Antes de aplicar este método amplamente, você deve testá-lo em um pequeno conjunto de máquinas virtuais da versão do hypervisor atualmente usado na sua organização.

Especificando configurações para instalação remota em dispositivos Unix

Ao instalar um aplicativo em um dispositivo Unix usando uma tarefa de instalação remota, você pode especificar configurações específicas do Unix para a tarefa. Essas configurações estão disponíveis nas propriedades da tarefa depois da tarefa ser criada.

Para especificar configurações específicas do Unix para uma tarefa de instalação remota:

1. No menu principal, vá para **Tarefas**.
2. Clique no nome da tarefa de instalação remota para a qual deseja especificar as configurações específicas do Unix.

   A janela de propriedades da tarefa é aberta.
3. Acesse **Configurações do aplicativo → Configurações Unix específicas**.
4. Especificar as seguintes configurações:

   Definir uma senha para a conta raiz (apenas para implementação via SSH)

   Se o comando `sudo` não puder ser usado no dispositivo de destino sem especificar a senha, selecione esta opção e, em seguida, especifique a senha para a conta raiz. O Kaspersky Security Center Linux transmite a senha de forma criptografada para o dispositivo de destino, descriptografa a senha e inicia o procedimento de instalação em nome da conta raiz com a senha especificada.

   > O Kaspersky Security Center Linux não usa a conta ou a senha especificada para criar uma conexão SSH.

   Especificar o caminho para uma pasta temporária com permissões de Execução no dispositivo de destino (apenas para implementação via SSH)

   Se o diretório/tmp no dispositivo de destino não tiver permissão de execução, selecione esta opção e, a seguir, especifique o caminho para o diretório com a permissão de execução. O Kaspersky Security Center Linux usa o diretório especificado como um diretório temporário para acessar por meio do SSH. O aplicativo coloca o pacote de instalação no diretório e executa o procedimento de instalação.
5. Clique no botão **Salvar**.

As configurações de tarefa especificadas são salvas.

Monitorar a implementação

Para monitorar a implementação do Kaspersky Security Center Linux e ter a garantia de que um aplicativo de segurança e o Agente de Rede estejam instalados nos dispositivos gerenciados, use o recurso de monitoramento e relatório:

- Use o widget de implementação do painel para monitorar a implementação em tempo real.
- Use relatórios para obter as informações detalhadas.

Início e interrupção de aplicativos da Kaspersky

É possível usar a tarefa *Iniciar ou interromper aplicativo* para iniciar e interromper os aplicativos da Kaspersky em dispositivos gerenciados.

Para criar a tarefa Iniciar ou interromper aplicativo:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na lista suspensa **Aplicativo**, selecione o aplicativo ao qual se deseja criar uma tarefa.

   Os aplicativos da Kaspersky serão exibidos na lista caso você tenha anteriormente adicionado os plug-ins de gerenciamento da web para esses aplicativos.
4. Na lista **Tipo de tarefa**, selecione a tarefa **Ativação do aplicativo**.
5. No campo **Nome da tarefa**, especifique o nome da nova tarefa.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).
6. Selecione os dispositivos aos quais a tarefa será atribuída.
7. Na janela **Aplicativos**, faça o seguinte:

   - Marque as caixas de seleção ao lado dos nomes dos aplicativos para os quais se deseja criar a tarefa.
   - Selecione a opção **Iniciar aplicativo** ou **Parar aplicativo**.
8. Caso queira modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na etapa **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode alterar as configurações padrão depois, a qualquer momento.
9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.
10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.
11. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades e, em seguida, salve-as.

A tarefa é criada e configurada.

Caso queira executar a tarefa, basta selecioná-la na lista de tarefas e, então, clicar no botão **Iniciar**.

Substituição de aplicativos de segurança de terceiros

A instalação de aplicativos de segurança da Kaspersky por meio do Kaspersky Security Center Linux pode exigir a remoção de software de terceiros incompatível com o aplicativo sendo instalado. O Kaspersky Security Center Linux fornece vários modos de remover os aplicativos de terceiros.

Remoção de aplicativos incompatíveis ao configurar a instalação remota de um aplicativo

É possível ativar a opção **Desinstalar automaticamente aplicativos incompatíveis** ao configurar a instalação remota de um aplicativo de segurança no Assistente de implementação da proteção. Quando esta opção está ativada, o Kaspersky Security Center Linux remove aplicativos incompatíveis antes de instalar um aplicativo de segurança em um dispositivo gerenciado.

Remover aplicativos incompatíveis através de uma tarefa dedicada

Para remover aplicativos incompatíveis através de uma tarefa, use a tarefa *Desinstalar aplicativo remotamente*. Esta tarefa deve ser executada nos dispositivos antes da execução da tarefa de instalação do aplicativo de segurança. Por exemplo, na tarefa de instalação, você pode selecionar **Na conclusão de outra tarefa** como tipo de agendamento em que a outra tarefa é *Desinstalar aplicativo remotamente*.

Este método da desinstalação é útil quando o instalador do aplicativo de segurança não puder remover apropriadamente um aplicativo incompatível.

Remover aplicativos ou atualizações de software remotamente

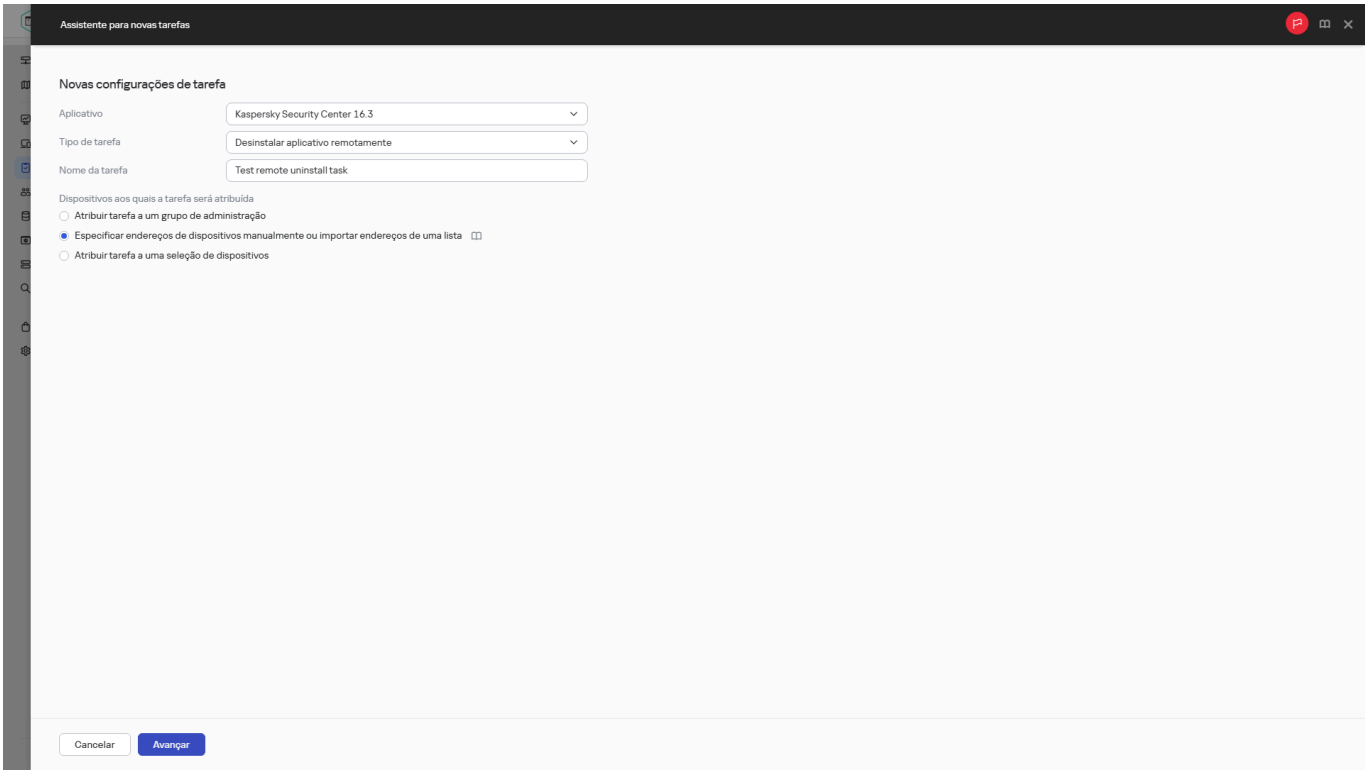
Você pode remover aplicativos ou atualizações de software em dispositivos gerenciados que executam o Linux remotamente apenas usando o Agente de Rede.

Para remover aplicativos ou atualizações de software remotamente de dispositivos selecionados:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na lista suspensa **Aplicativo**, selecione Kaspersky Security Center Linux.
4. Na lista **Tipo de tarefa**, selecione o tipo de tarefa **Desinstalar aplicativo remotamente**.
5. No campo **Nome da tarefa**, especifique o nome da nova tarefa.

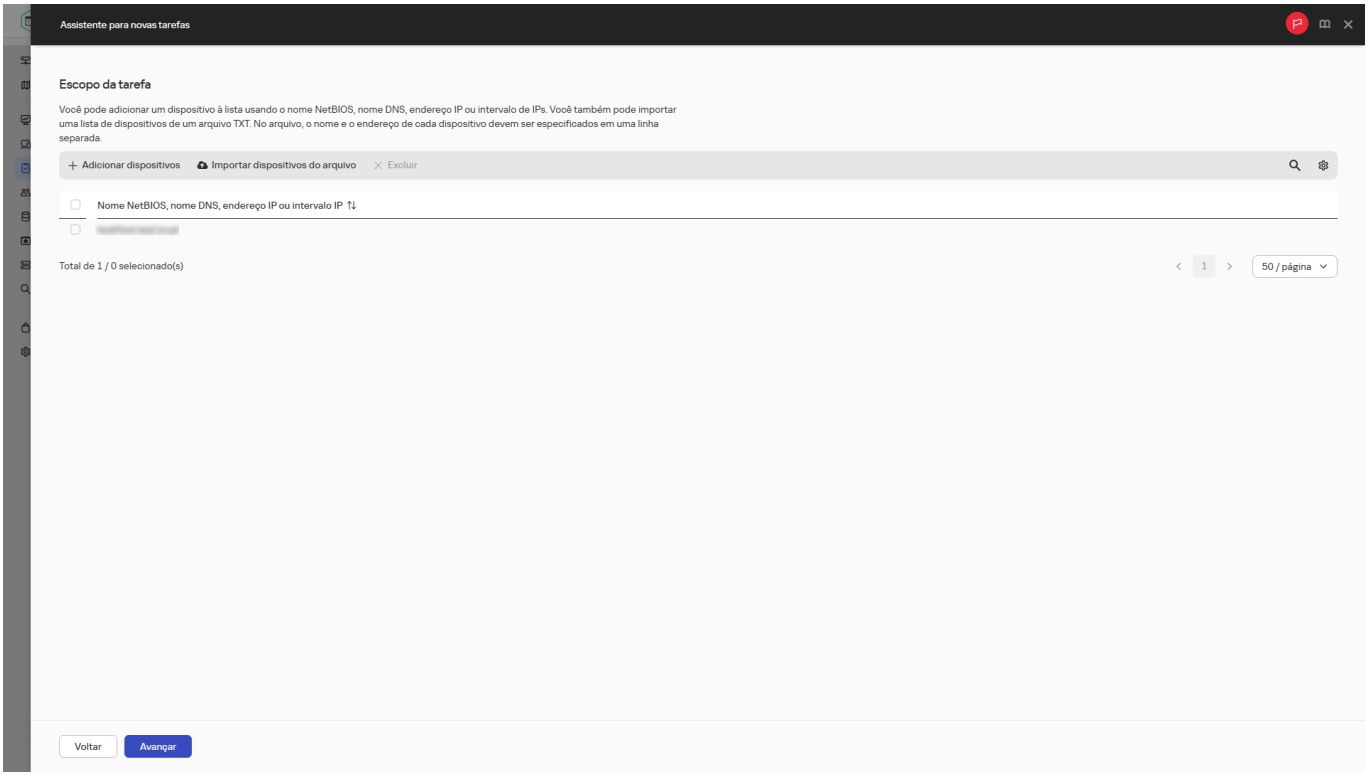
O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).



Criação da tarefa Desinstalar aplicativo remotamente

6. Selecione os dispositivos aos quais a tarefa será atribuída.

   Vá para a próxima etapa do assistente.



Especificação do escopo da tarefa

7. Selecione o tipo de software que deseja remover e, em seguida, selecione os aplicativos, atualizações ou patches específicos que deseja remover:

   Desinstalar o aplicativo gerenciado

Uma lista de aplicativos da Kaspersky é exibida. Selecione o aplicativo que deseja remover.

Desinstalar aplicativo incompatível

Uma lista de aplicativos incompatíveis com os aplicativos de segurança da Kaspersky ou o Kaspersky Security Center Linux é exibida. Marque as caixas de seleção ao lado dos aplicativos que deseja remover.

Desinstalar aplicativo do registro de aplicativos

Por padrão, os Agentes de Rede enviam ao Servidor de Administração informações sobre os aplicativos instalados nos dispositivos gerenciados. A lista de aplicativos instalados é armazenada no registro de aplicativos.

Para selecionar um aplicativo no registro de aplicativos:

a. Clique no campo **Aplicativo a ser desinstalado** e selecione o aplicativo que deseja remover.

Se você selecionar o Agente de Rede do Kaspersky Security Center, ao executar a tarefa, o status *Concluído com êxito* mostra que o processo de remoção foi iniciado. Se o Agente de Rede do Kaspersky Security Center for removido, o status não será alterado. Se a tarefa falhar, o status será alterado para *Falha.*

b. Especifique as opções de desinstalação:

- **Modo de desinstalação**

  Selecione como deseja remover o aplicativo:

  - **Definir o comando de desinstalação automaticamente**

    Se o aplicativo tiver um comando de desinstalação definido pelo fornecedor do aplicativo, o Kaspersky Security Center Linux usa esse comando. Recomendamos que você selecione esta opção.

  - **Especificar o comando de desinstalação**

    Selecione esta opção se desejar especificar seu próprio comando para a desinstalação do aplicativo.

    Recomendamos que você primeiro tente remover o aplicativo usando a opção **Definir o comando de desinstalação automaticamente**. Se a desinstalação por meio do comando definido automaticamente falhar, use seu próprio comando.

    Digite um comando de instalação no campo e especifique a seguinte opção:

    Usar este comando para desinstalação apenas se o comando padrão não tiver sido detectado automaticamente

    O Kaspersky Security Center Linux verifica se o aplicativo selecionado tem ou não um comando de desinstalação definido pelo fornecedor do aplicativo. Se o comando for encontrado, o Kaspersky Security Center Linux o usará em vez do comando especificado no campo **Comando para desinstalação de aplicativos**.

    Recomendamos que você ative esta opção.

- **Reinicializar após a desinstalação bem-sucedida do aplicativo**

  Se o aplicativo exigir que o sistema operacional seja reiniciado no dispositivo gerenciado após a desinstalação bem-sucedida, o sistema operacional será reiniciado automaticamente.

Desinstalar a atualização, patch ou o aplicativo de terceiro especificado

Uma lista de atualizações, patches e aplicativos de terceiros é exibida. Selecione o item que deseja remover.

A lista exibida é uma lista geral de aplicativos e atualizações e não corresponde aos aplicativos e atualizações instalados nos dispositivos gerenciados. Antes de selecionar um item, recomendamos que você verifique se o aplicativo ou a atualização está instalada nos dispositivos definidos no escopo da tarefa. Você pode visualizar a lista de dispositivos nos quais o aplicativo ou a atualização está instalada por meio da janela de propriedades.

Para visualizar a lista de dispositivos:

a. Clique no nome do aplicativo ou da atualização.

   A janela de propriedades é exibida.

b. Abra a seção **Dispositivos**.

   Você também pode visualizar a lista de aplicativos e atualizações instalados na janela de propriedades do dispositivo.

8. Especifique como os dispositivos clientes farão o download do utilitário de desinstalação:

Usando o Agente de Rede

Os arquivos são entregues aos dispositivos clientes pelo Agente de Rede instalado nesses dispositivos.

Se esta opção estiver desativada, os arquivos serão entregues usando as ferramentas do sistema operacional Linux.

Recomendamos que você ative esta opção se a tarefa tiver sido atribuída a dispositivos com o Agente de Rede instalado.

Usando recursos do sistema operacional através do Servidor de Administração

A opção está obsoleta. Em vez disso, use a opção **Usando o Agente de Rede** ou **Usando recursos do sistema operacional através de pontos de distribuição**.

Os arquivos são transmitidos para dispositivos clientes usando as ferramentas do sistema operacional do Servidor de Administração. Você pode ativar esta opção se nenhum Agente de Rede estiver instalado no dispositivo cliente, mas esse está na mesma rede que o Servidor de Administração.

Usando recursos do sistema operacional através de pontos de distribuição

Os arquivos são transmitidos para dispositivos clientes usando ferramentas do sistema operacional por meio de pontos de distribuição. Você pode ativar esta opção se houver, no mínimo, um ponto de distribuição na rede.

Se a opção **Usando o Agente de Rede** estiver marcada, os arquivos serão entregues por meio das ferramentas do sistema operacional somente se os recursos do Agente de Rede estiverem indisponíveis.

Número máximo de downloads concomitantes

O número máximo permitido de dispositivos clientes para os quais o Servidor de Administração pode transmitir os arquivos simultaneamente. Quanto maior esse número, mais rápido o aplicativo será desinstalado, mas a carga no Servidor de Administração será maior.

Número máximo de tentativas de desinstalação

Se, ao executar a tarefa *Desinstalar aplicativo remotamente*, o Kaspersky Security Center Linux falhar em desinstalar o aplicativo em um dispositivo gerenciado dentro do número de execuções do instalador especificado pelo parâmetro, o Kaspersky Security Center Linux interrompe a entrega do utilitário de desinstalação a esse dispositivo gerenciado e não inicia mais o instalador no dispositivo.

O parâmetro **Número máximo de tentativas de desinstalação** permite salvar os recursos do dispositivo gerenciado, assim como reduzir o tráfego (desinstalação, execução do arquivo MSI e mensagens de erro).

As tentativas recorrentes de início de tarefas podem indicar um problema no dispositivo e que impede a desinstalação. O administrador deve resolver o problema dentro do número especificado de tentativas de desinstalação e, em seguida, reiniciar a tarefa (manualmente ou por programação).

Se a desinstalação não for realizada eventualmente, o problema será considerado não solucionável e quaisquer tarefas adicionais serão consideradas como custosas em temos de consumo desnecessário de recursos e tráfego.

Quando a tarefa for criada, o contador de tentativas é definido como `0`. Cada execução do instalador retorna um erro no dispositivo e incrementa a leitura do contador.

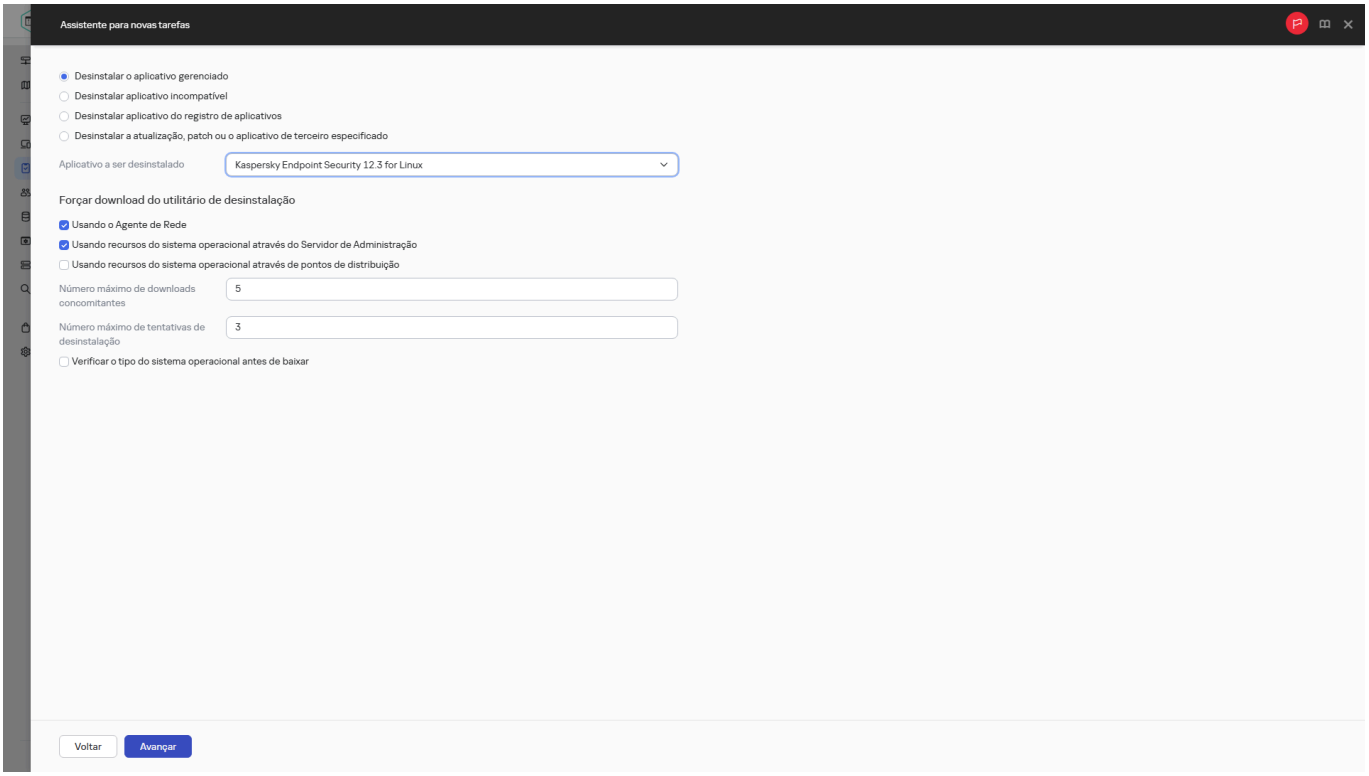
Se o número de tentativas especificado no parâmetro tiver sido excedido e o dispositivo estiver pronto para a desinstalação do aplicativo, você poderá aumentar o valor do parâmetro **Número máximo de tentativas de desinstalação** e iniciar a tarefa para desinstalar o aplicativo. Alternativamente, você pode criar uma nova tarefa *Desinstalar aplicativo remotamente*.

Verificar o tipo do sistema operacional antes de baixar

Antes de transmitir os arquivos para dispositivos clientes, o Kaspersky Security Center Linux verifica se as configurações do utilitário de instalação são aplicáveis ao sistema operacional do dispositivo cliente. Caso as configurações não sejam aplicáveis, o Kaspersky Security Center Linux não transmitirá os arquivos e não tentará instalar o aplicativo. Por exemplo, para instalar algum aplicativo em dispositivos de um grupo de administração que inclui dispositivos que executam vários sistemas operacionais, é possível atribuir a tarefa de instalação ao grupo de administração e então ativar essa opção para ignorar os dispositivos que executem um sistema operacional diferente do requerido.

Quando você faz a instalação remota do Agente de Rede em dispositivos não atribuídos, o Kaspersky Security Center Linux ou um ponto de distribuição determina automaticamente o tipo do sistema operacional do dispositivo, sem considerar a configuração **Verificar o tipo do sistema operacional antes de baixar**.

Vá para a próxima etapa do assistente.



Especificação das configurações da tarefa

9. Especifique as configurações para reiniciar o sistema operacional:

Não reiniciar o dispositivo

Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

Reiniciar o dispositivo

Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

Perguntar ao usuário o que fazer

O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min)**
- **Reiniciar após (min)**

Forçar fechamento de aplicativos em sessões bloqueadas

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

Vá para a próxima etapa do assistente.

10. Se necessário, adicione as contas que serão usadas para iniciar a tarefa de desinstalação remota:

Nenhuma conta necessária (Agente de Rede instalado)

Se essa caixa de seleção estiver selecionada, você não precisará especificar uma conta sob a qual o instalador do aplicativo será executado. A tarefa será executada sob a conta sob a qual o serviço do Servidor de Administração está sendo executado.

Se o Agente de Rede não tiver sido instalado em dispositivos clientes, esta opção não estará disponível.

Conta necessária (Agente de Rede não é usado)

Selecione esta opção se o Agente de Rede não estiver instalado nos dispositivos aos quais você atribui a tarefa de *Desinstalar aplicativo remotamente*. Nesse caso, é possível especificar uma conta de usuário ou um certificado SSH para desinstalar o aplicativo.

- **Conta local ou de domínio**. Se essa opção estiver selecionada, especifique a conta de usuário sob a qual o instalador do aplicativo será executado. Clique no botão **Adicionar**, selecione **Conta local ou de domínio** e, então, especifique as credenciais da conta do usuário.

  É possível especificar várias contas de usuário se, por exemplo, nenhuma delas tiver todos os direitos necessários em todos os dispositivos para os quais você atribui a tarefa. Nesse caso, todas as contas adicionadas são usadas para executar a tarefa, em ordem consecutiva, de cima para baixo.

- **Certificado SSH**. Se quiser desinstalar um aplicativo de um dispositivo cliente baseado em Linux, é possível especificar um certificado SSH em vez de uma conta de usuário. Clique no botão **Adicionar**, selecione **Certificado SSH** e, então, especifique as chaves privada e pública do certificado.

  Para gerar uma chave privada, você pode usar o utilitário ssh-keygen. Observe que o Kaspersky Security Center Linux é compatível com o formato PEM de chaves privadas, mas o utilitário ssh-keygen gera chaves SSH no formato OPENSSH por padrão. O formato OPENSSH não é compatível com o Kaspersky Security Center Linux. Para criar uma chave privada no formato PEM compatível, adicione a opção -m PEM no comando ssh-keygen.

  Por exemplo:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail do usuário>"
  ```

11. Se, na etapa **Concluir a criação da tarefa** do assistente, você ativar a opção **Abrir detalhes da tarefa quando a criação for concluída**, poderá editar as configurações padrão da tarefa.

    Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois.

12. Clique no botão **Concluir**.

    O assistente cria a tarefa. Caso a opção **Abrir detalhes da tarefa quando a criação for concluída** tenha sido ativada, a janela de propriedades da tarefa abrirá automaticamente. Nesta janela, você pode especificar as configurações gerais da tarefa e, se necessário, alterar as configurações especificadas durante a criação da tarefa.

    > Você também pode abrir a respectiva janela de propriedades clicando no nome da tarefa criada na lista de tarefas.

    A tarefa é criada, configurada e exibida na lista de tarefas em **Tarefas**.

13. Para executar a tarefa, selecione-a na lista de tarefas e, então, clique no botão **Iniciar**.

    Você também pode definir um agendamento de início de tarefa na guia **Agendamento** da janela de propriedades da tarefa.

    Para obter uma descrição detalhada das configurações de início agendado, consulte as configurações gerais da tarefa.

Depois que a tarefa for concluída, o aplicativo selecionado é removido nos dispositivos selecionados.

Problemas na desinstalação remota

Às vezes, a desinstalação remota de aplicativos de terceiros pode terminar com a seguinte advertência: "A desinstalação remota foi concluída neste dispositivo com avisos: o aplicativo para remoção não está instalado". Esse problema ocorre quando o aplicativo em questão já foi desinstalado ou foi instalado apenas para um usuário individual. Os aplicativos instalados para um usuário individual (também chamados de aplicativos por usuário) ficam invisíveis e não podem ser desinstalados remotamente se o usuário não estiver conectado.

Esse comportamento se diferencia de aplicativos destinados ao uso por vários usuários no mesmo dispositivo (também chamados de aplicativos por dispositivo). Os aplicativos por dispositivo ficam visíveis e acessíveis a todos os usuários do dispositivo.

Portanto, os aplicativos por usuário devem ser desinstalados somente quando o usuário estiver conectado.

Fonte de informação sobre os aplicativos instalados

O Agente de Rede recupera informações sobre software instalado em dispositivos Windows das seguintes chaves de registro:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para todos os usuários.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para todos os usuários.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para o usuário atual.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para usuários específicos.

Preparação de um dispositivo Windows para instalação remota

A instalação remota do aplicativo no dispositivo cliente poderá retornar um erro devido aos seguintes motivos:

- A tarefa já foi executada com êxito neste dispositivo.

  Nesse caso, a tarefa não tem de ser executada novamente.

- Quando a tarefa foi iniciada, o dispositivo foi desligado.

  Nesse caso, ligue o dispositivo, e em seguida, reinicie a tarefa.

- Não há conexão entre o Servidor de Administração e o Agente de Rede instalados no dispositivo cliente.

  Para determinar a causa do problema, use o utilitário projetado para o diagnóstico remoto nos dispositivos clientes (klactgui).

- Se o Agente de Rede não estiver instalado no dispositivo, podem ocorrer os seguintes problemas durante a instalação remota:
  - O dispositivo cliente tem a opção **Desativar compartilhamento simples de arquivo** ativada.
  - O serviço do servidor não está sendo executado no dispositivo cliente.
  - As portas relevantes estão fechadas no dispositivo cliente.
  - A conta de usuário que é usada para executar a tarefa possui privilégios insuficientes.

  Para evitar problemas que podem ocorrer durante a instalação do aplicativo em um dispositivo cliente no qual o Agente de Rede não foi instalado, será necessário prosseguir conforme o descrito em implementação forçada por meio da tarefa de instalação remota do Kaspersky Security Center Linux.

Anteriormente, o utilitário riprep foi usado para preparar um dispositivo para instalação remota. Agora, o procedimento é considerado um método desatualizado para configurar sistemas operacionais. O utilitário riprep não é recomendado para uso em sistemas operacionais mais recentes que Windows XP e Windows Server 2003 R2.

Criar a tarefa Executar scripts remotamente

Você pode criar uma tarefa *Executar scripts remotamente* para executar um pacote de instalação em um dispositivo cliente e para instalar remotamente um aplicativo.

Um pacote de instalação contém um arquivo ZIP com um conjunto de scripts para execução em dispositivos cliente, bem como um arquivo manifest.json. Saiba mais sobre como criar esse tipo de pacote de instalação neste artigo.

Essa tarefa deve ser iniciada somente em dispositivos com o Agente de Rede para Linux.

Para iniciar uma tarefa Executar scripts remotamente:

1. Acesse o **Assistente para novas tarefas** e selecione o tipo de tarefa **Executar scripts remotamente**.
2. Insira o nome da tarefa e selecione os dispositivos aos quais a tarefa será atribuída. Clique em **Avançar**.
3. Selecione um pacote de instalação baseado em um arquivo ZIP com um arquivo manifest.json para execução remota.

   Se não quiser executar novamente a tarefa em dispositivos onde ela já foi concluída, ative a opção **Não iniciar esta tarefa em dispositivos em que ela já tenha sido concluída**.
4. Selecione uma conta para executar a tarefa.

   Se você selecionar a conta padrão, a tarefa será executada pelo Agente de Rede (conta raiz).

   Quando a tarefa *Executar scripts remotamente* é iniciada, você não pode alterar a conta à qual ela está atribuída. Para alterar a conta para a qual a tarefa está atribuída, interrompa a tarefa nas configurações da tarefa e crie-a novamente com os detalhes de conta corretos.

5. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode alterar as configurações padrão depois, a qualquer momento.

6. Clique no botão **Concluir**.

   A tarefa *Executar scripts remotamente* é criada e aparece na lista de tarefas.

Depois de receber dados da tarefa *Executar scripts remotamente*, o Agente de Rede restringe o acesso aos dados recebidos para todos os usuários, exceto o administrador e o usuário especificado nas configurações da tarefa.

Criar um pacote de instalação com base em um arquivo de manifesto

Para criar um pacote de instalação com base em um arquivo de manifesto:

1. No menu principal, vá para **Gerenciamento de software → Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Clique em **Adicionar**.

   O Assistente de novo pacote inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Selecione **Crie um pacote de instalação para a tarefa Executar scripts remotamente com base em um arquivo ZIP com o arquivo manifest.json**.

4. Especifique o nome do pacote e clique no botão **Procurar**.

   Na janela exibida, escolha um arquivo para criar o pacote de instalação.

5. Selecione um arquivo morto localizado nos discos disponíveis. Saiba como preparar um arquivo compactado para esta tarefa neste artigo.

   O arquivo começa a ser carregado no Servidor de Administração Kaspersky Security Center Linux.

   O processo para criar o pacote de instalação é iniciado.

   O assistente informa quando o processo é concluído.

   Se o pacote de instalação não for criado, a mensagem apropriada será exibida.

6. Clique no botão **Concluir** para fechar o assistente.

O pacote de instalação que você criou é baixado na subpasta Packages da pasta compartilhada do Servidor de Administração. Após o download, o pacote de instalação aparece na lista de pacotes de instalação.

Na lista de pacotes de instalação disponíveis no Servidor de Administração, clicando no link com o nome de um pacote de instalação personalizado, você pode:

- Visualize as seguintes propriedades de um pacote de instalação:
  - **Nome.** Nome do pacote de instalação personalizada.
  - **Origem.** Nome do fornecedor do aplicativo.

- **Versão.** Versão do aplicativo.
- **Criação.** Data de criação do pacote de instalação.
- **Modificação.** Data de modificação do pacote de instalação.
- **Caminho.** Caminho para o pacote de instalação personalizada no Servidor de Administração.

- Altere o nome do pacote e os parâmetros da linha de comandos. Este recurso está disponível apenas para pacotes que não são criados baseados nos aplicativos Kaspersky.

Preparar um arquivo para a tarefa Executar scripts remotamente

Um arquivo para a tarefa *Executar scripts remotamente* com base em um arquivo manifest.json deve atender aos seguintes requisitos:

- Formato do arquivo: ZIP.
- Tamanho total: não mais que 1 GB.
- O número de arquivos e pastas no arquivo compactado é ilimitado.
- O arquivo de manifesto do arquivo compactado deve corresponder ao esquema abaixo e deve ser denominado manifest.json. O esquema é validado somente durante a execução da tarefa em um dispositivo.

  Esquema JSON do arquivo de manifesto e descrição das matrizes

  Esquema JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
```

```
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Exemplo do arquivo de manifesto

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
```

```
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- O arquivo deve ser estruturado da seguinte forma:

```
manifest.json
<file1>
<file2>
<folder1>/<file3>
<folder2>/<folder3>/<file4>
...
<fileX>
```

`manifest.json` é o arquivo de manifesto da tarefa.

`<file1>`, ..., `<fileX>` é o conjunto de arquivos com scripts a serem executados.

Instalar aplicativos remotamente em dispositivos usando a tarefa Executar scripts remotamente

A tarefa *Executar scripts remotamente* pode ser usada para instalar remotamente um aplicativo em um dispositivo cliente criando um pacote de instalação personalizado.

Saiba como preparar um arquivo compactado para esta tarefa neste artigo.

Para criar um pacote de instalação para a instalação remota de um aplicativo em um dispositivo cliente, os seguintes arquivos devem ser incluídos no arquivo compactado que você deseja carregar para esta tarefa:

- `<nome do pacote>`.deb
- **install.sh**

  ```
  sudo apt-get install <nome do pacote>.deb
  ```

- **manifest.json**

Esquema JSON para a instalação remota de um aplicativo

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<inserir os argumentos, se necessário>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

Descrição dos conjuntos

1. `version` – versão do arquivo de manifesto e da tarefa.

   Atualmente, o único valor aceitável é 1.

2. Os elementos do conjunto de `actions` determinam a composição e a ordem dos scripts que são executados na tarefa.

   A ordem de execução do script corresponde ao índice de um elemento (local) na matriz.

3. Para cada elemento da matriz `actions`, os seguintes elementos são definidos.

   a. `type` – tipo de comando executável dos scripts. Atualmente, o valor é sempre `execute`.

   b. `path` – caminho para o arquivo de script no arquivo compactado.

   c. `args` – argumentos que são passados para o script como parte do comando executável.

   d. `results` – matriz que define outras ações, dependendo do resultado da tarefa.

      1. `code` – valor que retorna um script.

      2. `next` – ação a ser concluída em seguida. A ação `continue` prossegue com a execução do próximo script (elemento da matriz `actions`). A ação `break` interrompe a tarefa.

   e. `default_next` – ação se um script retornar um valor que não está contido em `results`.

Quando a tarefa *Executar scripts remotamente* for iniciada, o Agente de Rede carregará o pacote de instalação com o aplicativo para o dispositivo cliente. Quando o dispositivo cliente recebe o pacote de instalação, o Agente de Rede neste dispositivo analisa o arquivo manifest.json e define a ordem de execução de scripts e ações dependendo do resultado e, em seguida, inicia a execução.

Quando a tarefa *Executar scripts remotamente* for concluída, o aplicativo será instalado no dispositivo cliente.

Configurar notificações e monitoramento para a tarefa Executar scripts remotamente

Você pode configurar o monitoramento, o comportamento de salvar eventos e as notificações para a tarefa *Executar scripts remotamente*.

Para visualizar o status de Executar scripts remotamente:

1. No menu principal, vá para **Tarefas**.

   A lista de tarefas é exibida.

2. Selecione a tarefa e clique em **Histórico do dispositivo**.

   O progresso da tarefa é exibido.

Para configurar o comportamento de salvamento de eventos:

1. Na lista de tarefas, clique na tarefa e vá para a guia **Configurações**.
2. Na seção **Notificações**, clique no botão **Configurações**.
3. Selecione uma das seguintes opções para como o aplicativo se comportará após a conclusão da tarefa:

   - **Salvar todos os eventos**.
   - **Salvar eventos relacionados ao progresso da tarefa**.
   - **Salvar apenas os resultados da execução da tarefa**.

     Os eventos são salvos no **Histórico do dispositivo** e no **Repositório de eventos**.

     Por padrão, somente os resultados da execução da tarefa são salvos.

     > Se você selecionar **Salvar todos os eventos**, somente os resultados da execução da tarefa serão salvos.

4. Se desejar manter os eventos no banco de dados do Servidor de Administração, no log de eventos do Servidor de Administração ou no dispositivo, ative a opção correspondente.

Saiba mais sobre como configurar notificações neste artigo.

Licenciamento

Esta seção fornece as seguintes informações:

- Conceitos gerais relacionados ao licenciamento do Kaspersky Security Center Linux
- Instruções sobre o gerenciamento de licenças de aplicativos Kaspersky gerenciados

Licenciamento da Kaspersky Security Center Linux

Esta seção descreve os conceitos gerais relacionados ao licenciamento do Kaspersky Security Center Linux.

Sobre o Contrato de Licença do Usuário Final

O Contrato de Licença do Usuário Final (Contrato de Licença ou EULA) é um contrato vinculativo entre você e a AO Kaspersky Lab que estipula os termos nos quais você pode usar o aplicativo.

Leia com atenção o seguinte Contrato de Licença antes de começar a usar o aplicativo.

O Kaspersky Security Center Linux e seus componentes, por exemplo, Agente de Rede, têm seu próprio EULA.

Você pode visualizar os termos do Contrato de Licença do Usuário Final para o Kaspersky Security Center Linux usando os seguintes métodos:

- Durante a instalação do Kaspersky Security Center.
- Lendo o documento license.txt incluído no kit de distribuição do Kaspersky Security Center.
- Lendo o documento license.txt presente na pasta de instalação do Kaspersky Security Center.
- Ao baixar o arquivo license.txt do site da Kaspersky.

Você pode visualizar os termos do Contrato de Licença do Usuário Final para o Agente de Rede para Linux usando os seguintes métodos:

- Durante o download do pacote de distribuição do Agente de Rede dos servidores da web Kaspersky.
- Durante a instalação do Agente de Rede para Linux.
- Lendo o documento license.txt incluído no pacote de distribuição do Agente de Rede para Linux.
- Lendo o documento license.txt constante na pasta de instalação do Agente de Rede para Linux.
- Ao baixar o arquivo license.txt do site da Kaspersky.

Você aceita os termos do Contrato de Licença do Usuário Final confirmando que concorda com o Contrato de Licença do Usuário Final ao instalar o aplicativo. Se você não aceitar os termos do Contrato de Licença, cancele instalação do aplicativo e não o utilize.

Sobre a licença

Uma *licença* é um direito com período de validade limitado para uso do Kaspersky Security Center, concedido nos termos do Contrato de Licença (Contrato de Licença de Usuário Final).

O escopo dos serviços e o período de validade dependem da licença sob a qual o aplicativo é utilizado.

São fornecidos os seguintes tipos de licença:

- *Avaliação*

  Uma licença gratuita concebida para experimentar o aplicativo. Uma licença de avaliação normalmente tem um prazo de validade curto.

  Quando a licença de avaliação expira, todos os recursos do Kaspersky Security Center Linux são desativados. Para continuar usando o aplicativo, é necessário comprar a licença comercial.

  Você pode usar o aplicativo com uma licença de avaliação por apenas um período de avaliação.

- *Comercial*

  Uma licença paga.

  Quando uma licença comercial expira, os principais recursos do aplicativo são desativados. Para manter o Kaspersky Security Center funcionando, é necessário renovar sua licença comercial. Depois que a licença expirar, você não poderá mais usar o aplicativo e deverá excluí-lo do dispositivo.

  Recomendamos a renovação da sua licença antes que ela expire para garantir a máxima proteção contra todas as ameaças à segurança.

Sobre o certificado de licença

Um *certificado de licença* é um documento fornecido a você juntamente com um arquivo de chave ou um código de ativação.

O certificado de licença contém as seguintes informações sobre a licença concedida:

- ID da licença ou número do pedido
- Informações sobre o usuário ao qual é concedida a licença
- Informações sobre o aplicativo que pode ser ativado com a licença fornecida
- Limite do número de unidades de licenciamento (por exemplo, dispositivos nos quais o aplicativo pode ser usado com uma licença fornecida)
- Data de início do período da licença
- Data de expiração da licença ou período da licença
- Tipo de licença

Sobre a chave de licença

Chave de licença é a sequência de bits que você pode aplicar para ativar e usar o aplicativo de acordo com os termos do Contrato de Licença do Usuário Final. As chaves de licença são geradas pelos especialistas da Kaspersky.

Você pode adicionar uma chave de licença ao aplicativo usando um dos seguintes métodos: aplicando um *arquivo de chave* ou inserindo um *código de ativação*. A chave de licença é exibida na interface do aplicativo como uma sequência alfanumérica única após você a adicionar ao aplicativo.

A chave de licença pode estar bloqueada pela Kaspersky caso os termos do Contrato de Licença tenham sido violados. Se a chave de licença tiver sido bloqueada, você deve adicionar outra se desejar usar o aplicativo.

Uma chave de licença pode ser ativa ou adicional (ou reserva).

Uma *chave de licença ativa* é uma chave de licença que é atualmente usada pelo aplicativo. Uma chave de licença ativa pode ser adicionada para uma licença de avaliação ou comercial. O aplicativo não pode ter mais de uma chave de licença ativa.

Uma *chave de licença adicional (ou reserva)* é uma chave de licença que permite ao usuário utilizar o aplicativo, mas que não se encontra atualmente em uso. A chave de licença adicional torna-se automaticamente ativa quando a licença associada à chave atual expira. Uma chave de licença adicional pode ser adicionada somente se uma chave de licença atual tiver sido adicionada.

Uma chave de licença para uma licença de avaliação pode ser adicionada somente como um chave de licença atual. Uma chave de licença para uma licença de avaliação não pode ser adicionada como uma chave de licença adicional.

Ler a Política de Privacidade

A Política de Privacidade está disponível online em https://www.kaspersky.com/products-and-services-privacy-policy.

A Política de Privacidade também está disponível off-line:

- É possível ler a Política de Privacidade antes de instalar o Kaspersky Security Center Linux.
- O texto da Política de Privacidade está incluído no arquivo license.txt, na pasta de instalação do Kaspersky Security Center Linux.
- O arquivo privacy_policy.txt está disponível em um dispositivo gerenciado, na pasta de instalação do Agente de Rede.
- Você pode descompactar o arquivo privacy_policy.txt do pacote de distribuição do Agente de Rede.

Opções de licença do Kaspersky Security Center

O Kaspersky Security Center pode funcionar nos seguintes modos:

- **Funcionalidade básica do Console de Administração**

  O Kaspersky Security Center funciona nesse modo antes que o aplicativo seja ativado ou após a licença comercial expirar. O Kaspersky Security Center com suporte para a funcionalidade básica do Console de Administração é fornecido como parte dos aplicativos da Kaspersky para proteção de redes corporativas. Também pode baixá-lo pelo site da Kaspersky.

- **Licença comercial**

  Caso necessite de uma funcionalidade adicional não incluída na funcionalidade básica do Console de Administração, será necessário comprar uma licença comercial.

  Ao adicionar uma chave de licença na janela de propriedades do Servidor de Administração, verifique e confirme se uma chave de licença foi adicionada para permitir o uso do Kaspersky Security Center Linux. Você pode encontrar essas informações no site da Kaspersky. Cada página da web da solução contém a lista de aplicativos incluídos nela. O Servidor de Administração pode aceitar chaves de licença não compatíveis, por exemplo, uma chave de licença do Kaspersky Endpoint Security Cloud, mas essas chaves de licença não fornecem novos recursos além da funcionalidade básica do Console de Administração.

Recurso ou propriedade	Modo de operação do Kaspersky Security Center Linux	
	A licença está ausente	Licença comercial
Funcionalidade básica do Console de Administração As seguintes funções estão disponíveis: • Criação de Servidores de Administração virtuais para gerenciar uma rede de escritórios remotos ou organizações clientes • Criação de uma hierarquia de grupos de administração para gerenciar dispositivos específicos como uma entidade única • Instalação remota de aplicativos • Configuração centralizada de aplicativos instalados em dispositivos cliente • Controle do status de segurança antivírus de uma organização • Gerenciamento de funções do usuário • Estatísticas e relatórios sobre a operação do aplicativo assim como notificações sobre eventos críticos • Operações centralizadas com arquivos que foram movidos para a Quarentena e Backup e arquivos cujo processamento foi adiado • Criptografia e gerenciamento de proteção de dados • Visualização e edição manual da lista de componentes de hardware detectados pela sondagem da rede • Visualização da lista de imagens do sistema operacional disponíveis para instalação remota	✓	✓

Recurso ou propriedade	Modo de operação do Kaspersky Security Center Linux	
	A licença está ausente	Licença comercial
Gerenciamento de patches e vulnerabilidades: funcionalidade básica As seguintes tarefas não exigem uma licença comercial: • A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* Por meio dessa tarefa, o Kaspersky Security Center Linux recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para o software de terceiros instalado nos dispositivos gerenciados. • A tarefa *Corrigir vulnerabilidades* A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para softwares de terceiros. Para usar essa tarefa, é necessário especificar manualmente as correções do usuário para vulnerabilidades nas configurações da tarefa.	✓	✓
Gerenciamento de patches e vulnerabilidades: funcionalidade avançada Você pode definir as regras para a instalação remota automática de atualizações de software e a correção de vulnerabilidades automaticamente.	—	✓
Gerenciamento do sistema As seguintes funções estão disponíveis: • Permissão remota de conexão aos dispositivos cliente através de um componente do Microsoft® Windows® denominado Remote Desktop Connection. • Conexão remota aos dispositivos cliente através do Windows Desktop Sharing.	—	✓
Exportando eventos para sistemas SIEM: uso do protocolo Syslog Usando o protocolo Syslog, você pode encaminhar qualquer evento que ocorre no Servidor de Administração do Kaspersky Security Center e em aplicativos Kaspersky que são instalados em dispositivos gerenciados. O protocolo Syslog é um protocolo de registro de mensagem padrão. É possível usá-lo para exportar os eventos para qualquer sistema SIEM.	✓	✓
Agregação de alertas e execução de ações de resposta por meio do Active Directory, do KASAP e do Kaspersky TIP Sandbox	—	✓

Sobre o arquivo de chave

Um *arquivo de chave* é um arquivo com a extensão .key fornecido a você pela Kaspersky. Os arquivos de chave se destinam a ativar o aplicativo adicionando uma chave de licença.

Você recebe o arquivo de chave pelo endereço de e-mail que especificou após comprar o Kaspersky Security Center, ou que utilizou para solicitar a versão de avaliação do Kaspersky Security Center.

Você não precisa se conectar aos servidores de ativação da Kaspersky para ativar o aplicativo com um arquivo de chave.

Se o arquivo de chave tiver sido excluído acidentalmente, você poderá restaurá-lo. Você pode precisar de um arquivo de chave, por exemplo, para se registrar no Kaspersky CompanyAccount.

Para restaurar o arquivo de chave, execute uma das seguintes ações:

- Entre em contato com o vendedor da licença.
- Obtenha um arquivo de chave no site da Kaspersky com base no código de ativação disponível.

Sobre a coleta de dados

Dados fornecidos a terceiros

Ao usar a funcionalidade de Gerenciamento de Dispositivos Móveis do Software, com o objetivo de fornecer em tempo hábil os comandos para os dispositivos que executam o sistema operacional Android por meio do sistema de notificação push, o serviço Google Firebase Cloud Messaging será usado. Se o Usuário tiver configurado o uso do serviço Google Firebase Cloud Messaging, o Usuário concordará em fornecer as seguintes informações ao serviço Google Firebase Cloud Messaging no modo automático:

- ID da instância
- ID do software no serviço Google Firebase Cloud Messaging
- Versão do software instalado
- Versão completa do software
- Versão do Google Play
- Nome do pacote de distribuição do software
- Versão do esquema para os dados fornecidos
- Operating system version
- ID do software

Para bloquear a troca de informações com o serviço Google Firebase Cloud Messaging, o Usuário deve reverter as configurações de uso do serviço Google Firebase Cloud Messaging para seus valores de fábrica.

Ao usar a funcionalidade de Gerenciamento de Dispositivos Móveis do Software, com o objetivo de fornecer em tempo hábil os comandos para dispositivos que executam o sistema operacional iOS por meio do sistema de notificação push, o Apple Push Notification Service (APNs) será usado. Se o Usuário instalou um certificado de APNs em um servidor de MDM do iOS, criou um perfil de MDM do iOS com um conjunto de configurações para conexão dos dispositivos móveis iOS para o Software, e instalou este nos dispositivos móveis, o Usuário concorda em fornecer as seguintes informações para as APNs no modo automático:

- Token – Push token do dispositivo. O servidor usa este token quando está mandando notificações de push para o dispositivo.
- PushMagic – Um string que precisa ser incluído quando mandar notificações. O valor do string é gerado pelo dispositivo.

Dados transferidos para AO Kaspersky Lab

Caso a funcionalidade Kaspersky Extended Detection and Response Optimum esteja disponível para o usuário, o Kaspersky Security Center Linux transferirá dados nos seguintes casos:

- Para atribuir um curso de treinamento a um profissional, o Kaspersky Security Center Linux transfere os seguintes dados para a Kaspersky Automated Security Awareness Platform (KASAP): e-mail do usuário, e-mail alternativo do usuário (se disponível), ID do usuário no KASAP, ID do grupo de treinamento.

- Para executar automaticamente um arquivo usando o Kaspersky Cloud Sandbox, o aplicativo gerenciado transfere os arquivos em quarentena do Servidor de Administração por meio do Agente de Rede e, em seguida, por meio do Kaspersky Security Center Web Console, para o Kaspersky Cloud Sandbox. O Kaspersky Cloud Sandbox analisa o arquivo e quaisquer arquivos que possam ser criados durante a execução dele.

Dados processados localmente

O Kaspersky Security Center Linux foi projetado para a execução centralizada de administração básica e tarefas de manutenção em uma rede corporativa. O Kaspersky Security Center Linux fornece ao administrador o acesso a informações detalhadas sobre o nível de segurança da rede corporativa. O Kaspersky Security Center Linux permite ao administrador configurar todos os componentes de proteção criados com base nos aplicativos Kaspersky. O Kaspersky Security Center Linux executa as seguintes funções principais:

- Detecção de dispositivos e seus usuários na rede da organização
- Criação de uma hierarquia de grupos administrativos para gerenciamento de dispositivos
- Instalação de aplicativos do Kaspersky nos dispositivos
- Gerenciamento de configurações e tarefas dos aplicativos instalados
- Gerenciamento de atualizações do Kaspersky e aplicativos de terceiros, busca e correções de vulnerabilidades
- Ativação de aplicativos Kaspersky nos dispositivos
- Como gerenciar contas de usuário
- Visualizando informações sobre a operação dos aplicativos do Kaspersky nos dispositivos
- Visualização de relatórios
- Ativação da integração com os serviços da Kaspersky

Para desempenhar sua função principal, o Kaspersky Security Center Linux pode receber, armazenar e processar as seguintes informações:

- Informações sobre os dispositivos na rede da organização recebidas por meio da verificação dos controladores de domínio (Active Directory, Samba, FreeIPA e ALD Pro) ou por meio da verificação de intervalos IP. O Servidor de Administração obtém dados de forma independente ou recebe dados do Agente de Rede.

- Informações dos controladores de domínio (Active Directory, Samba, FreeIPA e ALD Pro) sobre unidades organizacionais, domínios, usuários e grupos. O Servidor de Administração obtém dados sozinho ou recebe dados do Agente de Rede atribuído para funcionar como um ponto de distribuição.

- Detalhes dos dispositivos gerenciados. O Agente de Rede transfere os dados listados abaixo do dispositivo para o Servidor de Administração. O usuário digita o nome de exibição e a descrição do dispositivo na interface do Kaspersky Security Center Web Console:

    - Especificações técnicas dos dispositivos gerenciados e seus componentes requeridos para identificação do dispositivo: nome de exibição e descrição do dispositivo, nome e tipo do domínio do Windows (para os dispositivos que pertençam a um domínio do Windows), nome do dispositivo no ambiente do Windows (para dispositivos que pertençam a um domínio do Windows), domínio DNS e nome DNS, endereço IPv4, endereço IPv6, localização da rede, endereço MAC, número de série, tipo de sistema operacional, se o dispositivo é uma máquina virtual com tipo de hipervisor e se o dispositivo é uma máquina virtual dinâmica como parte de uma VDI.

    - Outras especificações de dispositivos gerenciados e os componentes necessários para auditoria de dispositivos gerenciados e para tomada de decisões sobre se os patches específicos e as atualizações são aplicáveis: arquitetura do sistema operacional, fornecedor do sistema operacional, número da compilação do sistema operacional, ID da versão do sistema operacional, pasta de localização do sistema operacional; se o dispositivo é uma máquina virtual, o tipo de máquina virtual, o nome do Servidor de Administração virtual que gerencia o dispositivo.

    - Detalhes de ações em dispositivos gerenciados: data e hora da ultima atualização, hora em que o dispositivo esteve visível na rede pela última vez, status de espera de reinício e hora em que o dispositivo foi ligado.

    - Detalhes das contas de usuário do dispositivo e as suas sessões.

- Dados recebidos ao executar o diagnóstico remoto em um dispositivo gerenciado: arquivos de rastreamento, informações do sistema, detalhes dos aplicativos da Kaspersky instalados no dispositivo, arquivos de despejo, logs de eventos, os resultados da execução dos scripts de diagnóstico recebidos do Suporte técnico da Kaspersky.

- Estatísticas de operação do ponto de distribuição se o dispositivo for um ponto de distribuição. O Agente de Rede transfere os dados do dispositivo para o Servidor de Administração.

- Configurações do ponto de distribuição inseridas pelo usuário no Kaspersky Security Center Web Console.

- Dados necessários para a conexão de dispositivos móveis ao Servidor de Administração: certificado, porta de conexão móvel, endereço de conexão do Servidor de Administração. O usuário insere os dados no Kaspersky Security Center Web Console.

- Detalhes dos dispositivos móveis transferidos usando o uso do protocolo móvel. Os dados listados abaixo são transferidos do dispositivo móvel para o Servidor de Administração:

  - Informações sobre o aplicativo: nome do aplicativo, versão completa do aplicativo, data e hora de instalação do aplicativo, status da proteção em tempo real do dispositivo e ID da sessão.

  - Informações sobre as chaves de licença usadas pelo aplicativo: número de série da chave de licença e tipo de licença, status da chave de licença, período de validade da chave de licença em dias, datas de geração e expiração da chave de licença, nome da empresa para a qual a licença foi fornecida, informações adicionais no caso de uma assinatura ser usada (sinalizador de assinatura, data de expiração e número de dias disponíveis para renovação da assinatura, endereço da Web do provedor de assinatura, status atual da assinatura e causa para obter esse status), data e hora em que o aplicativo foi ativado no dispositivo, data e quando a licença no dispositivo expirar.

  - Informações sobre o dispositivo gerenciado: nome do dispositivo, ID do dispositivo, tipo de dispositivo, IMEI do dispositivo (caso esteja disponível), número de série do dispositivo (caso esteja disponível), fabricante do dispositivo, nome da família de CPU do dispositivo, impressão digital do certificado do proprietário do dispositivo, tipo de SO, versão do SO, nome do SO, espaço total em disco no dispositivo, nome do servidor ao qual o dispositivo pertence, endereço IP do dispositivo, nome do grupo de dispositivos, nome distinto do usuário, nome distinto do domínio, senha única ou senha de domínio.

  - Informações sobre o resultado da execução de comandos personalizados: ID do comando, status de execução do comando, resultado da execução do comando; para o comando de localização do dispositivo: latitude, longitude, altitude e velocidade de movimento do dispositivo; para o comando de retrato: fotos tiradas pela câmera frontal do dispositivo móvel ao tentar desbloquear.

  - Informações sobre a verificação de dispositivos: data e hora da última verificação de dispositivo, caminho completo no sistema de arquivos a partir do qual a verificação foi iniciada, número de objetos verificados, número de objetos maliciosos detectados, número de objetos bloqueados, excluídos e desinfectados, número de objetos que não puderam ser desinfectados, número de erros de validação, número de processos encerrados.

  - Informações sobre o funcionamento de cada componente do aplicativo e sobre o desempenho de cada tarefa, apresentadas como eventos:

    - ID do evento.

    - Gravidade

    - Nome e tipo de evento.

    - Descrição da causa do evento.

    - Data e hora de em que o evento ocorreu.

    - Informações sobre eventos da operação Antirroubo (código de desbloqueio do dispositivo, coordenadas do dispositivo, método de entrega do comando, lista de dados excluídos).

    - Resultados do processamento de um objeto detectado ou ação (nome do arquivo no dispositivo; nome do aplicativo; nome da ameaça; tipo de ameaça; tipo de ação executada com o arquivo; resultado da ação; código de erro, em caso de ocorrência).

    - Informações sobre a regra de conformidade acionada (critério da regra; ação aplicada; descrição do erro ao aplicar a ação, em caso de ocorrência).

    - Informações sobre o erro de operação do aplicativo (versão do aplicativo, versão do SO, nome do dispositivo, descrição do erro).

- Informações sobre o erro do Samsung KNOX (código de erro, URL do qual o arquivo não pôde ser baixado).
- Informações sobre as permissões concedidas ao aplicativo.
- Informações sobre cada um dos aplicativos instalados no dispositivo gerenciado (nome do aplicativo, status da instalação).
- Informações sobre a aceitação global do Contrato de Licença de Usuário Final (EULA): ID do EULA, carimbo de data e hora do EULA, texto do EULA.
- Configurações do Google Firebase Cloud Messaging: ID do remetente, ID de registro do dispositivo.

- Informações sobre o endereço IP público do dispositivo.
- Valores das configurações do usuário. O administrador gerencia as configurações no Kaspersky Security Center Web Console, enquanto o usuário gerencia essas configurações no aplicativo móvel.

- Detalhes dos dispositivos móveis transferidos usando o protocolo MDM do iOS. Os dados listados abaixo são transferidos do dispositivo móvel para o Servidor de Administração:
  - Especificações técnicas do dispositivo móvel e seus componentes necessários para identificação do dispositivo: nome do dispositivo, modelo, nome, versão e número de compilação do sistema operacional, número do modelo do dispositivo, IMEI, número de telefone, UDID, MEID, número de série, quantidade de memória total e disponível, versão do firmware do modem, endereço MAC do Bluetooth, endereço MAC do Wi-Fi e detalhes do cartão SIM (ICCID como parte do ID do cartão SIM).
  - Detalhes da rede móvel usada pelo dispositivo gerenciado: tipo de rede móvel, nome da rede móvel utilizada atualmente, nome da rede móvel doméstica, versão das configurações da operadora de rede móvel, status de roaming de voz, status de roaming de dados, código do país da rede doméstica, código do país de residência, código da rede atualmente em uso e nível de criptografia.
  - Configurações de segurança do dispositivo móvel: uso de uma senha e sua conformidade com as configurações da política, lista de certificados instalados, aplicativos e perfis de configuração.
  - Data e hora da última sincronização com o Servidor de Administração e status de gerenciamento de dispositivos.
- Informações dos dados do dispositivo móvel transferidos usando o protocolo WebRTC: imagem da tela do dispositivo.
- Detalhes de arquivos especificados para transferência para dispositivos móveis. O usuário insere dados na interface do Kaspersky Security Center Web Console.
- Detalhes dos aplicativos da Kaspersky instalados no dispositivo. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede:
  - Configurações dos aplicativos da Kaspersky instalados no dispositivo gerenciado: nome e versão do aplicativo Kaspersky, status, status da proteção em tempo real, data e hora da última verificação do dispositivo, número de ameaças detectadas, número de objetos com falha na desinfecção, disponibilidade e status dos componentes do aplicativo, detalhes sobre as configurações e tarefas do aplicativo da Kaspersky, informações sobre chaves de licença ativa e adicional, data e ID de instalação.
  - Estatística da operação de aplicativo: eventos relacionados a alterações no status dos componentes do aplicativo da Kaspersky no dispositivo gerenciado e desempenho de tarefas iniciadas pelos componentes de software.

- Status do dispositivo definido pelo aplicativo do Kaspersky.
- Marcações feitas por o aplicativo do Kaspersky.

- Dados contidos em eventos dos componentes do Kaspersky Security Center Linux e aplicativos gerenciados Kaspersky. O Agente de Rede transfere os dados do dispositivo para o Servidor de Administração.
- Dados necessários para a integração do Kaspersky Security Center Linux com um sistema SIEM para exportação de eventos. O usuário insere os dados no Kaspersky Security Center Web Console.
- Dados necessários para integrar o Kaspersky Security Center Linux com os controladores de domínio (Active Directory, Samba, FreeIPA e ALD Pro). O usuário insere os dados no Kaspersky Security Center Web Console.
- Arquivos Keytab para conectar com a Conexão única do Kerberos (SSO). O usuário insere os dados no Kaspersky Security Center Web Console.
- Dados necessários para configurar a conexão com o servidor proxy para conexão com a Internet. O usuário insere os dados no Kaspersky Security Center Web Console.
- Configurações dos componentes do Kaspersky Security Center Linux e Kaspersky gerenciados estão disponíveis nas políticas e nos perfis das políticas. O usuário insere dados na interface do Kaspersky Security Center Web Console.
- Configurações de tarefas dos componentes do Kaspersky Security Center Linux e aplicativos gerenciados Kaspersky. O usuário insere dados na interface do Kaspersky Security Center Web Console.
- Dados processados pelo recurso de gerenciamento do sistema. O Agente de Rede transfere do dispositivo para o Servidor de Administração as seguintes informações:
  - Informações sobre hardware detectado em dispositivos gerenciados (Registro de Aplicativos).

    Caso o Agente de Rede esteja instalado em um dispositivo que execute o Windows, ele enviará ao Servidor de Administração as seguintes informações sobre o hardware do dispositivo:

    - RAM
    - Dispositivos de armazenamento em massa
    - Placa-mãe
    - CPU
    - Adaptadores de rede
    - Monitores
    - Adaptador de vídeo
    - Placa de som

    Se o Agente de Rede estiver instalado em um dispositivo com Linux ou macOS, ele enviará ao Servidor de Administração as seguintes informações sobre o hardware, caso o sistema operacional as forneça:

    - Volume total de RAM
    - Volume total de dispositivos de armazenamento em massa

- Placa-mãe
- CPU
- Adaptadores de rede

- Detalhes sobre aplicativos e patches instalados nos dispositivos gerenciados (Registro de aplicativos). O software pode ser comparado com as informações sobre os arquivos executáveis detectados nos dispositivos pela função Controle de Aplicativos.
- Detalhes sobre vulnerabilidades em aplicativos de terceiros nos dispositivos gerenciados.
- Detalhes sobre atualizações de aplicativos de terceiros instalados em dispositivos gerenciados.

- Dados necessários para baixar atualizações no Servidor de Administração isolado para corrigir vulnerabilidades de softwares de terceiros em dispositivos gerenciados. O usuário insere e transmite dados usando o utilitário klscflag do Servidor de Administração.
- Categorias de usuários de aplicativos. O usuário insere dados na interface do Kaspersky Security Center Web Console.
- Detalhes de arquivos executáveis detectados em dispositivos gerenciados pelo recurso de Controle de Aplicativos. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Detalhes sobre arquivos colocados em Backup. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Detalhes sobre arquivos colocados em quarentena. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Detalhes dos arquivos solicitados pelos especialistas da Kaspersky para análise detalhada. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Detalhes sobre status e ativação de Controle de regras das Anomalias Adaptivas. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Detalhes sobre dispositivos externos (unidades de memória, ferramentas de transferência de informações, ferramentas cópia impressa de informações e conexões de buses) instalados ou conectados ao dispositivo gerenciado e detectados pelo recurso de Controle de Dispositivos. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.
- Informações sobre dispositivos Windows criptografados e o status da criptografia. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede.
- Informações sobre os erros de criptografia de dados nos dispositivos. A criptografia é executada pela função Dados de criptografia dos aplicativos Kaspersky. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Lista de controladores lógicos programáveis (PLCs) gerenciados. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Dados necessários para a criação de uma cadeia de desenvolvimento de ameaças. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Informações sobre tentativas dos funcionários de uma organização de acessar os serviços em nuvem. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Dados necessários para a integração do Kaspersky Security Center ao serviço Kaspersky Managed Detection and Response (o plugin dedicado deve ser instalado para o Kaspersky Security Center Web Console): token de iniciação de integração, token de integração e token de sessão do usuário. O Usuário insere os dados na interface do Kaspersky Security Center Web Console. O serviço Kaspersky MDR transfere o token de integração e o token de sessão do usuário por meio do plugin dedicado.

- Dados necessários para integrar o Kaspersky Security Center Linux com o Kaspersky Cloud Sandbox e o Kaspersky Threat Intelligence Portal (requer a instalação do plug-in adequado para o Kaspersky Security Center Web Console): um token de integração, um token de autorização. O usuário insere um token para integração na interface do Kaspersky Security Center Web Console. O Kaspersky Security Center Web Console transfere um token de autorização em uma solicitação para a API do Kaspersky Cloud Sandbox.

- Dados necessários para integrar o Kaspersky Security Center Linux com o serviço Kaspersky Automated Security Awareness Platform (KASAP): token de API para acessar o KASAP Open API, URL (um link para acessar o KASAP por meio do Open API).

- Detalhes dos códigos de ativação e arquivos de chave. O usuário insere dados na interface do Kaspersky Security Center Web Console.

- Contas de usuário: nome, descrição, nome completo, endereço de e-mail, número de telefone principal, senha, chave secreta gerada pelo Servidor de Administração e senha única para autenticação de dois fatores. O usuário insere dados na interface do Kaspersky Security Center Web Console.

- Revisão de histórico de objetos gerenciados excluídos. O usuário insere dados na interface do Kaspersky Security Center Web Console.

- Endereço IP do dispositivo no qual um usuário criou uma revisão. O endereço IP é definido pelo Servidor de Administração automaticamente.

- Registro de objetos gerenciados excluídos. O usuário insere dados na interface do Kaspersky Security Center Web Console.

- Pacotes de instalação criados dos arquivos e configurações de instalações. O usuário insere dados na interface do Kaspersky Security Center Web Console.

- Dados necessários para a exibição de informativos da Kaspersky no Kaspersky Security Center Web Console. O usuário insere dados na interface do Kaspersky Security Center Web Console.

- Dados necessários para o funcionamento de plugins de aplicativos gerenciados no Kaspersky Security Center Web Console e salvos pelos plugins no banco de dados do Servidor de Administração durante sua operação de rotina. A descrição e formas de fornecer os dados são fornecidas nos arquivos de Ajuda do aplicativo correspondente.

- Configurações de usuário do Kaspersky Security Center Web Console: idioma de localização e tema da interface, configurações de exibição do painel de monitoramento, informações sobre o status das notificações (Já lidas/Ainda não lidas), status das colunas nas planilhas (Mostrar/Ocultar), Modo de treinamento progresso. O usuário insere dados na interface do Kaspersky Security Center Web Console.

- Certificados de comunicação segura dos dispositivos gerenciados e componentes do Kaspersky Security Center Linux. O usuário insere e transmite dados usando o utilitário klsetsrvcert do Servidor de Administração.

- Certificados para estabelecer confiança nos recursos da Web internos da organização. O usuário insere dados na interface do Kaspersky Security Center Web Console.

- Informações sobre a aceitação, pelo usuário, dos termos e condições dos acordos legais com a Kaspersky.

- Os dados do Servidor de Administração que o usuário insere no Kaspersky Security Center Web Console ou na interface do programa Kaspersky Security Center OpenAPI.

- Quaisquer dados inseridos pelo usuário na interface do Kaspersky Security Center Web Console.

Os dados listados acima podem estar presentes no Kaspersky Security Center Linux se um dos seguintes métodos for aplicado:

- O usuário insere dados na interface do Kaspersky Security Center Web Console.

- O Agente de Rede automaticamente recebe dados do dispositivo e os transfere para o Servidor de Administração.

- O Agente de Rede recebe extração de dados por o aplicativo gerenciado do Kaspersky e transfere para o Servidor de Administração. A lista de dados processados por aplicativos gerenciados do Kaspersky são providenciados nos arquivos de Ajuda para os aplicativos correspondentes.

- O Servidor de Administração obtém as informações sobre os dispositivos em rede por si só ou recebe os dados do Agente de Rede atribuídos para funcionar como um ponto de distribuição.

- Os dados são transferidos do dispositivo móvel para o Servidor de Administração com o uso do protocolo MDM do iOS ou do protocolo móvel.

Os dados são armazenados no banco de dados do Servidor de Administração. Os hashes de senha são armazenados em formato criptografado.

Todos os dados processados localmente podem ser transferidos para a Kaspersky apenas através de arquivos de dumping, arquivos de rastreamento ou arquivos de log dos componentes do Kaspersky Security Center Linux, incluindo arquivos de log criados por instaladores e utilitários.

Os arquivos de dump, rastreamento ou log dos componentes do Kaspersky Security Center Linux contêm dados arbitrários do Servidor de Administração, Agente de Rede e Kaspersky Security Center Web Console. Os arquivos podem conter dados pessoais ou confidenciais. Os arquivos de dump, rastreamento e log são armazenados no dispositivo de forma não criptografada. Os arquivos de dump, rastreamento ou log não são transferidos para a Kaspersky automaticamente; contudo, um administrador pode transferir dados para a Kaspersky manualmente, mediante solicitação do Suporte Técnico, para resolver problemas na operação do Kaspersky Security Center Linux.

As informações obtidas são protegidas pela Kaspersky Lab de acordo com os requisitos estabelecidos por lei e as normas vigentes da Kaspersky Lab. Os dados são transmitidos por canais de comunicação seguros.

Seguindo os links no Kaspersky Security Center Web Console, o usuário concorda com a transferência automática dos seguintes dados:

- Código do Kaspersky Security Center Linux
- Versão do Kaspersky Security Center Linux
- Localização do Kaspersky Security Center Linux
- ID da licença
- Tipo de licença
- Se a licença foi adquirida por meio de um parceiro

A lista de dados fornecida via cada link depende da finalidade e da localização do link.

A Kaspersky usa os dados coletados de forma anônima e somente para fins estatísticos gerais. As estatísticas sumarizadas são geradas automaticamente a partir dos dados brutos recebidos e não contêm informações pessoais ou outras informações confidenciais. À medida que novos dados são acumulados, os dados mais antigos são apagados (uma vez por ano). As estatísticas sumarizadas são armazenadas por tempo indeterminado.

Sobre a assinatura

A *Assinatura para o Kaspersky Security Center Linux* é um pedido para uso do aplicativo sob as configurações selecionadas (data de expiração da assinatura, número de dispositivos protegidos). Você pode registrar sua assinatura do Kaspersky Security Center Linux com seu provedor de serviços (por exemplo, seu provedor de Internet). Uma assinatura pode ser renovada manualmente ou no modo automático; você também pode cancelá-la.

Uma assinatura pode ser limitada (por exemplo, um ano) ou ilimitada (sem uma data de expiração). Para continuar a usar o Kaspersky Security Center após uma assinatura limitada expirar, você precisa renová-la. Uma assinatura ilimitada é automaticamente renovada, caso tenha sido pré-paga ao provedor de serviços nas datas devidas.

Quando uma assinatura limitada expirar, um período adicional poderá lhe ser fornecido para efetuar a renovação durante o qual o aplicativo continua a funcionar. A disponibilidade e a duração do período de carência é definida pelo provedor de serviços.

Para usar o Kaspersky Security Center Linux sob a assinatura, você precisa aplicar o código de ativação recebido do provedor de serviços.

Você pode aplicar um código de ativação diferente para o Kaspersky Security Center Linux somente após sua assinatura expirar ou quando a cancelar.

Dependendo do provedor de serviços, o conjunto de ações possíveis para o gerenciamento da assinatura pode variar. O Provedor de Serviços não pode conceder nenhum período de carência para a renovação da assinatura, portanto o aplicativo perde sua funcionalidade.

Os códigos de ativação comprados sob a assinatura não podem ser usados para ativar versões anteriores do Kaspersky Security Center.

Ao usar o aplicativo sob a assinatura, o Kaspersky Security Center Linux automaticamente tenta acessar o servidor de ativação em intervalos de tempo especificados até que a assinatura expire. Caso não seja possível acessar o servidor usando o DNS do sistema, o aplicativo usará os servidores DNS públicos. Você pode renovar sua assinatura no site do provedor de serviços.

Ativação do Kaspersky Security Center Linux

Você pode ativar o Kaspersky Security Center Linux para usar sua funcionalidade adicional. Há duas maneiras de realizar esta tarefa: use o assistente de início rápido do Servidor de Administração ou as propriedades do Servidor de Administração.

Para ativar o Kaspersky Security Center Linux:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Chaves de licença**.

3. Em **Licença atual**, clique no botão **Selecionar**.

4. Na janela exibida, selecione a chave de licença que deseja usar para ativar o Kaspersky Security Center Linux. Caso a chave de licença não esteja listada, clique no botão **Adicionar nova chave de licença** e especifique uma nova chave de licença.

5. Caso seja necessário, também será possível adicionar uma chave de licença reserva. Para fazer isso, em **Chave de licença reserva**, clique no botão **Selecionar** e selecione uma chave de licença existente ou adicione uma nova. Observe que não é possível adicionar uma chave de licença reserva caso não haja nenhuma chave de licença ativa.

6. Clique no botão **Salvar**.

Licenciamento de aplicativos gerenciados da Kaspersky

Esta seção descreve os recursos do Kaspersky Security Center relacionados ao trabalho com chaves de licença de aplicativos gerenciados da Kaspersky.

O Kaspersky Security Center Linux lhe permite realizar a distribuição centralizada de chaves de licença para os aplicativos Kaspersky em dispositivos clientes, monitorar seu uso e renovar licenças.

Ao adicionar uma chave de licença usando o Kaspersky Security Center, as configurações da chave de licença são salvas no Servidor de Administração. Com base nestas informações, o aplicativo gera um relatório sobre o uso das chaves de licença e notifica o administrador sobre a expiração das licenças e sobre a violação das restrições de licença que estão definidas nas propriedades das chaves de licença. Você pode configurar as notificações do uso de chaves de licença dentro das configurações do Servidor de Administração.

Licenciamento de aplicativos gerenciados

Os aplicativos Kaspersky instalados em dispositivos gerenciados devem ser licenciados com a aplicação de um arquivo de chave ou um código de ativação à cada um dos aplicativos. Um arquivo de licença ou um código de ativação pode ser implementado nas seguintes formas:

- Implementação automática
- O pacote de instalação de um aplicativo gerenciado
- A tarefa de adicionar uma chave de licença para um aplicativo gerenciado
- Ativação manual de um aplicativo gerenciado

É possível adicionar uma nova chave de licença ativa ou reserva por qualquer um dos métodos listados acima. Um aplicativo da Kaspersky usa uma chave ativa no momento e armazena uma chave reserva para aplicar após a expiração da chave ativa. O aplicativo ao qual a chave de licença é adicionada define se a chave é ativa ou reserva. A definição da chave não depende do método usado para adicionar uma nova chave de licença.

Implementação automática

Se você usar aplicativos gerenciados diferentes e precisa implementar um arquivo de chave ou código de ativação específico para dispositivos, opte por outras formas de implementar aquele código de ativação ou arquivo de chave.

O Kaspersky Security Center lhe permite implementar automaticamente as chaves de licença disponíveis nos dispositivos. Por exemplo, três chaves de licença são armazenadas no repositório do Servidor de Administração. Você ativou a opção **Chave de licença automaticamente distribuída** para as três chaves de licença. Um aplicativo de segurança da Kaspersky – por exemplo, Kaspersky Endpoint Security for Linux – é instalado nos dispositivos da organização. Um novo dispositivo é descoberto, no qual uma chave de licença deve ser implementada. O aplicativo determina, por exemplo, que duas das chaves de licença do repositório podem ser aplicadas ao dispositivo: a chave de licença denominada *Key_1*e chave de licença denominada *Key_2*. Uma destas chaves de licença é implementada no dispositivo. Neste caso, não pode ser previsto qual das duas chaves de licença será implementada no dispositivo, porque a implementação automática de chaves de licença não é fornecida para nenhuma atividade do administrador.

Quando uma chave de licença é implementada, os dispositivos são recontados para aquela chave de licença. Você deve assegurar-se de que o número de dispositivos nos quais a chave de licença foi implementada não excede o limite da licença. Se o número de dispositivos exceder o limite de licença, todos os dispositivos que não foram cobertos pela licença serão terão o status *Crítico* atribuído.

Antes da implementação, o arquivo de chave ou o código de ativação deve ser adicionado ao repositório do Servidor de Administração.

Instruções de como proceder:

- Adição de uma chave de licença ao repositório do Servidor de Administração
- Distribuição automática de uma chave de licença

Observe que uma chave de licença distribuída automaticamente pode não ser exibida no repositório do Servidor de Administração virtual nos seguintes casos:

- A chave de licença não é válida para o aplicativo.
- O Servidor de Administração virtual não tem dispositivos gerenciados.
- A chave de licença já foi usada para dispositivos gerenciados por outro Servidor de Administração virtual e o limite no número de dispositivos foi atingido.

Adicionando um arquivo de chave ou código de ativação ao pacote de instalação de um aplicativo gerenciado

Por motivos de segurança, esta opção não é recomendada. Um arquivo de licença ou um código de ativação adicionado a um pacote de instalação pode se tornar comprometido.

Se você instalar um aplicativo gerenciado usando um pacote de instalação, poderá especificar um código de ativação ou um arquivo de chave neste pacote de instalação ou na política do aplicativo. A chave de licença será implementada nos dispositivos gerenciados no momento da próxima sincronização do dispositivo com o Servidor de Administração.

Instruções: Adicionando uma chave de licença a um pacote de instalação

Implementação através da tarefa de adicionar uma chave de licença para um aplicativo gerenciado

Se você optar por usar a tarefa Adicionar chave de licença para um aplicativo gerenciado, poderá selecionar a chave de licença a ser implementada nos dispositivos e selecionar os dispositivos da maneira mais conveniente, por exemplo, selecionando um grupo de administração ou uma seleção de dispositivos.

Antes da implementação, o arquivo de chave ou o código de ativação deve ser adicionado ao repositório do Servidor de Administração.

Instruções de como proceder:

- Adição de uma chave de licença ao repositório do Servidor de Administração
- Implementação de uma chave de licença para dispositivos clientes

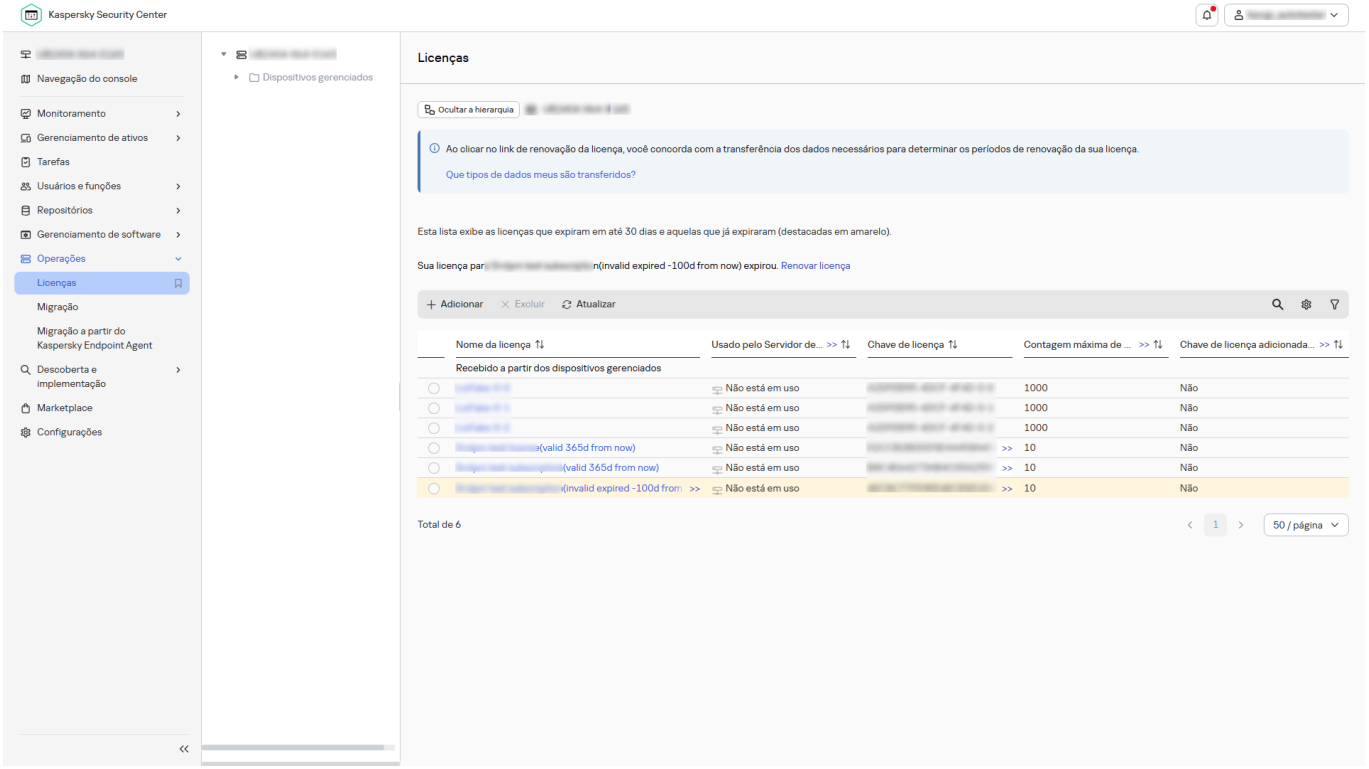
Adicionar um código de ativação ou um arquivo de chave manualmente nos dispositivos

Você pode ativar o aplicativo da Kaspersky instalado localmente usando as ferramentas fornecidas na interface do aplicativo. Consulte a documentação do aplicativo instalado.

Adição de uma chave de licença ao repositório do Servidor de Administração

Adicionar uma chave de licença ao repositório do Servidor de Administração:

1. No menu principal, vá para **Operações** → **Licenças**.



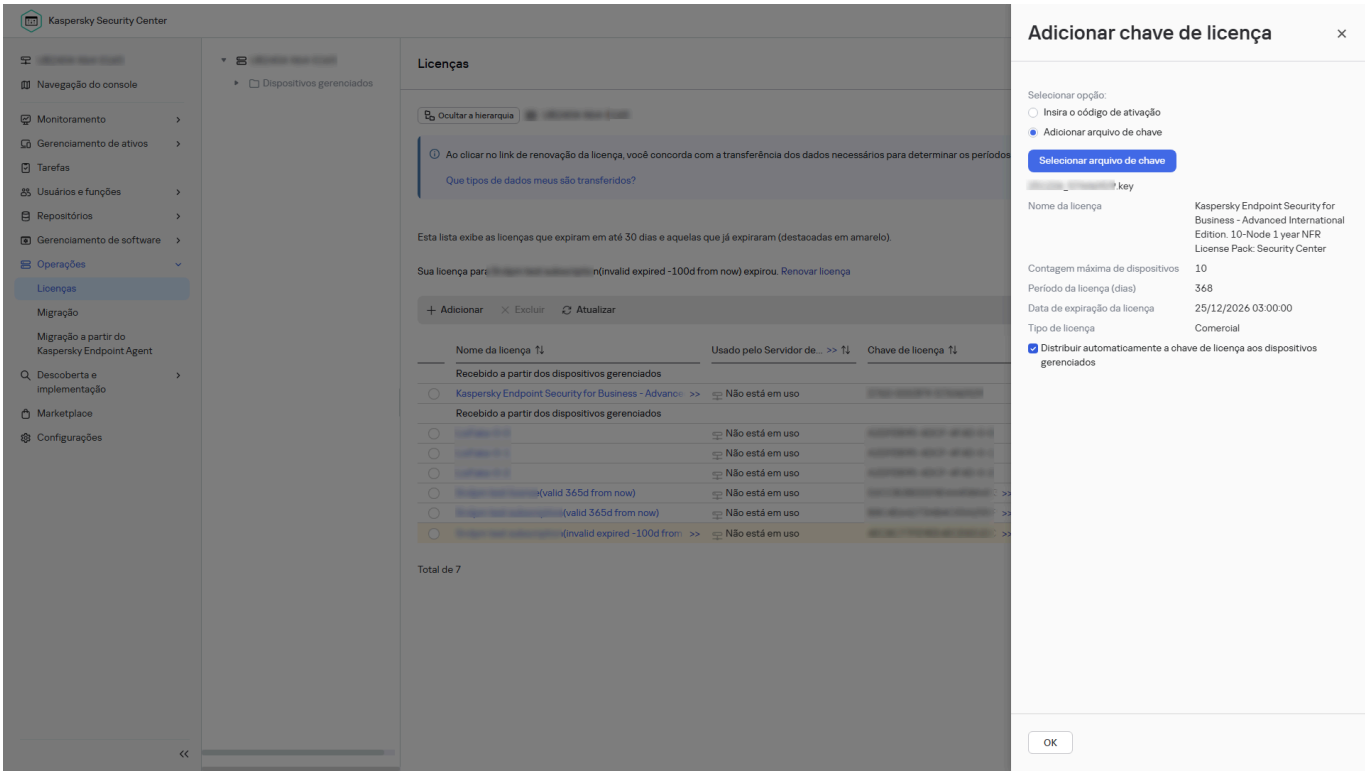
Lista das chaves de licença da Kaspersky adicionadas

2. Clique em **Adicionar**.

3. Selecione o que você quer adicionar:

- **Adicionar arquivo de chave**

  Clique no botão **Selecionar arquivo de chave** e navegue até o arquivo .key que deseja adicionar.



Adicionar uma chave de licença por meio da aplicação de um arquivo de chave

- **Insira o código de ativação**

  Especifique o código de ativação no campo de texto e clique no botão **Enviar**.

4. Clique no botão **Fechar**.

A chave de licença ou várias chaves de licença são adicionadas ao repositório do Servidor de Administração.

Implementando uma chave de licença para dispositivos clientes

O Kaspersky Security Center Web Console permite distribuir uma chave de licença para dispositivos clientes automaticamente ou por meio da tarefa de **Ativação do aplicativo**. É possível usar a tarefa para distribuir chaves para um grupo específico de dispositivos. Durante a distribuição de uma chave de licença por meio da tarefa, o limite do licenciamento em relação ao número de dispositivos não é levado em consideração. Use a distribuição automática de chaves para interromper a distribuição de uma chave de licença automaticamente quando o limite do licenciamento for atingido.

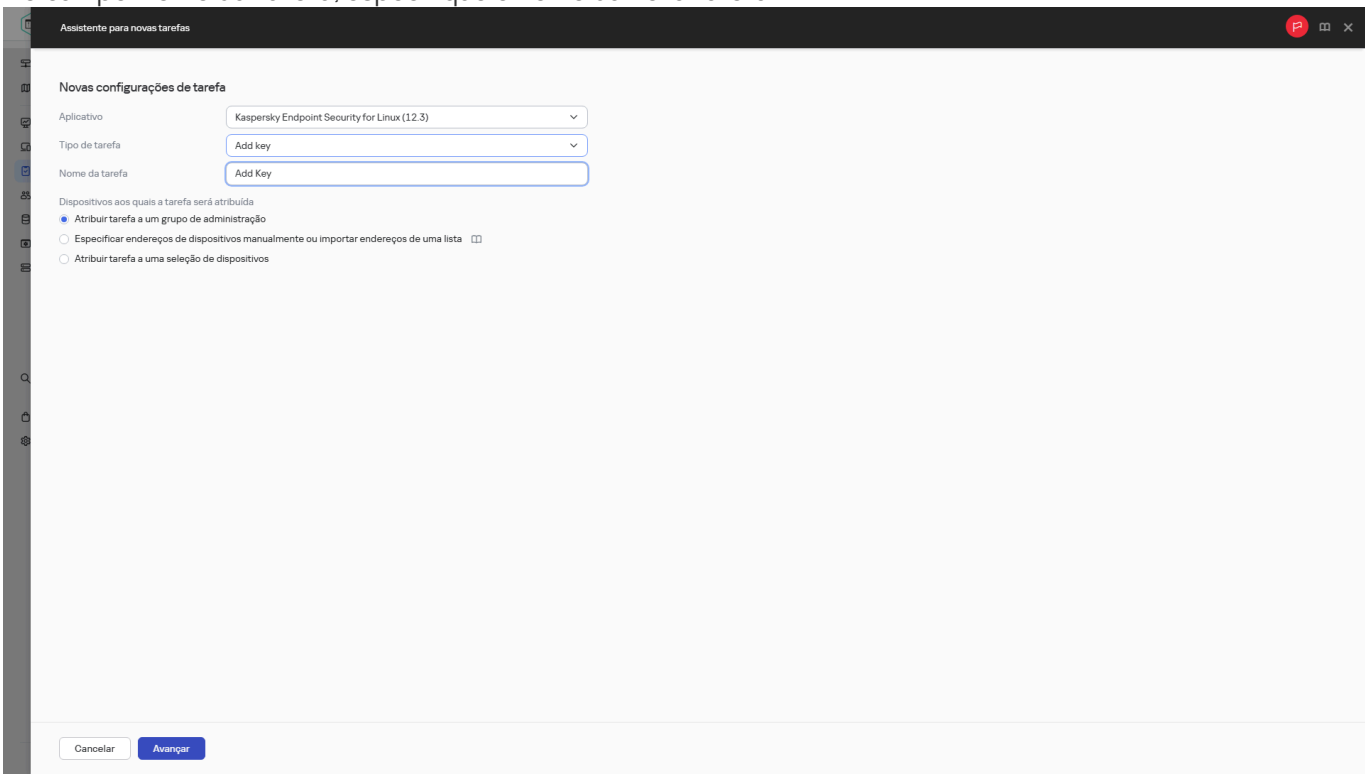
Caso a distribuição automática de uma chave de licença seja ativada, não crie uma tarefa de **Ativação do aplicativo** para distribuir essa chave aos dispositivos clientes. Caso contrário, a carga no Servidor de Administração aumentará devido à sincronização frequente.

Antes da implementação, adicione uma chave de licença ao repositório do Servidor de Administração.

*Para distribuir uma chave de licença para dispositivos clientes por meio da tarefa de **Ativação do aplicativo**:*

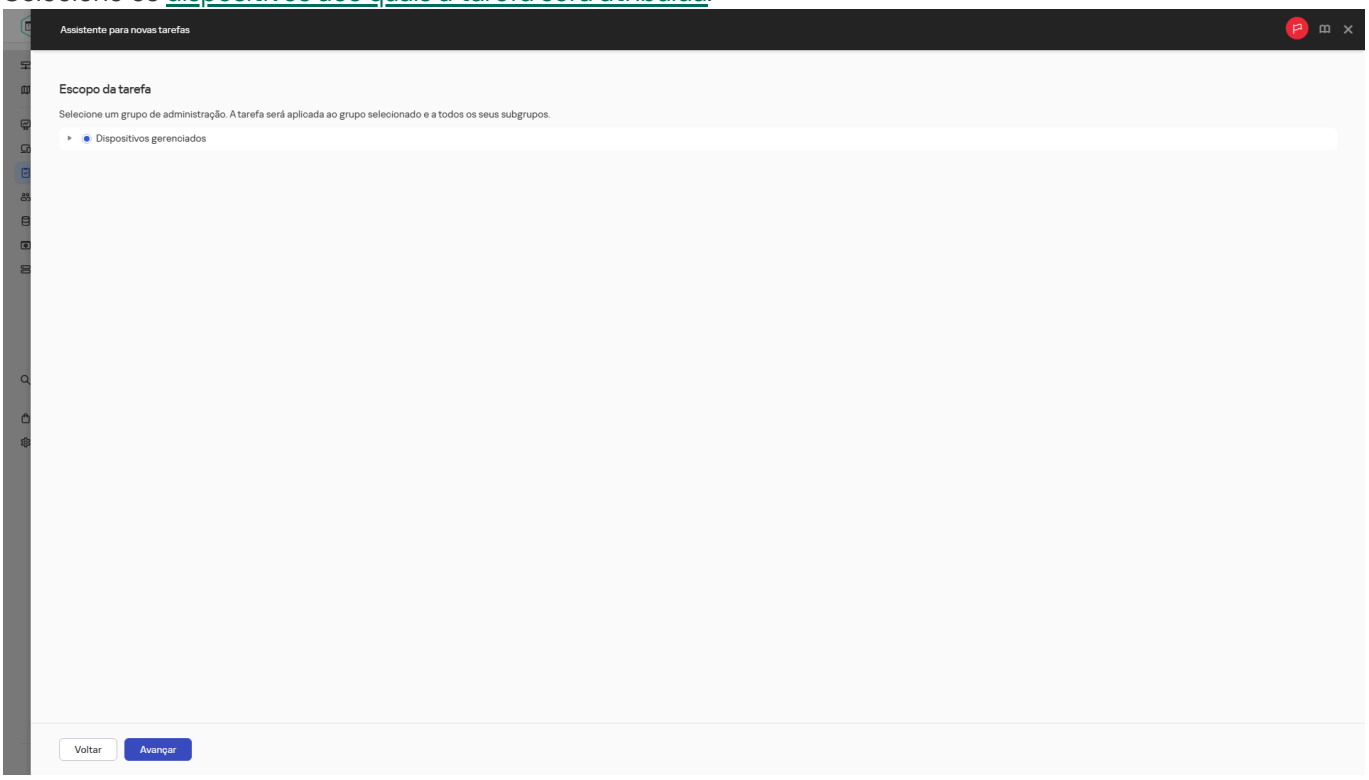
1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O **Assistente para novas tarefas** inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na lista suspensa **Aplicativo**, selecione o aplicativo ao qual você deseja adicionar uma chave de licença.
4. Na lista **Tipo de tarefa**, selecione a tarefa **Ativação do aplicativo**.
5. No campo **Nome da tarefa**, especifique o nome da nova tarefa.



Criação de uma tarefa Adicionar chave

6. Selecione os dispositivos aos quais a tarefa será atribuída.



Especificação do escopo da tarefa

7. Na etapa **Selecionando uma chave de licença** do assistente, clique no link **Adicionar chave** para adicionar a chave de licença.

8. No painel de adição de chave, adicione a chave de licença usando uma das seguintes opções:

> É necessário adicionar a chave de licença somente se ela não tiver sido adicionada ao repositório do Servidor de Administração antes da criação da tarefa de **Ativação do aplicativo**.

- Selecione a opção **Insira o código de ativação** para inserir um código de ativação e, então, faça o seguinte:

  a. Especifique o código de ativação e, então, clique no botão **Enviar**.

  As informações sobre a chave de licença são exibidas no painel de adição de chave.

  b. Clique no botão **Salvar**.

  > Se você quiser distribuir automaticamente a chave de licença para dispositivos gerenciados, ative a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

  O painel de adição de chave é fechado.

- Selecione a opção **Adicionar arquivo de chave** para adicionar um arquivo de chave e, em seguida:

  a. Clique no botão **Selecionar arquivo de chave**.

  b. Na janela exibida, selecione um arquivo de chave e, então, clique no botão **Abrir**.

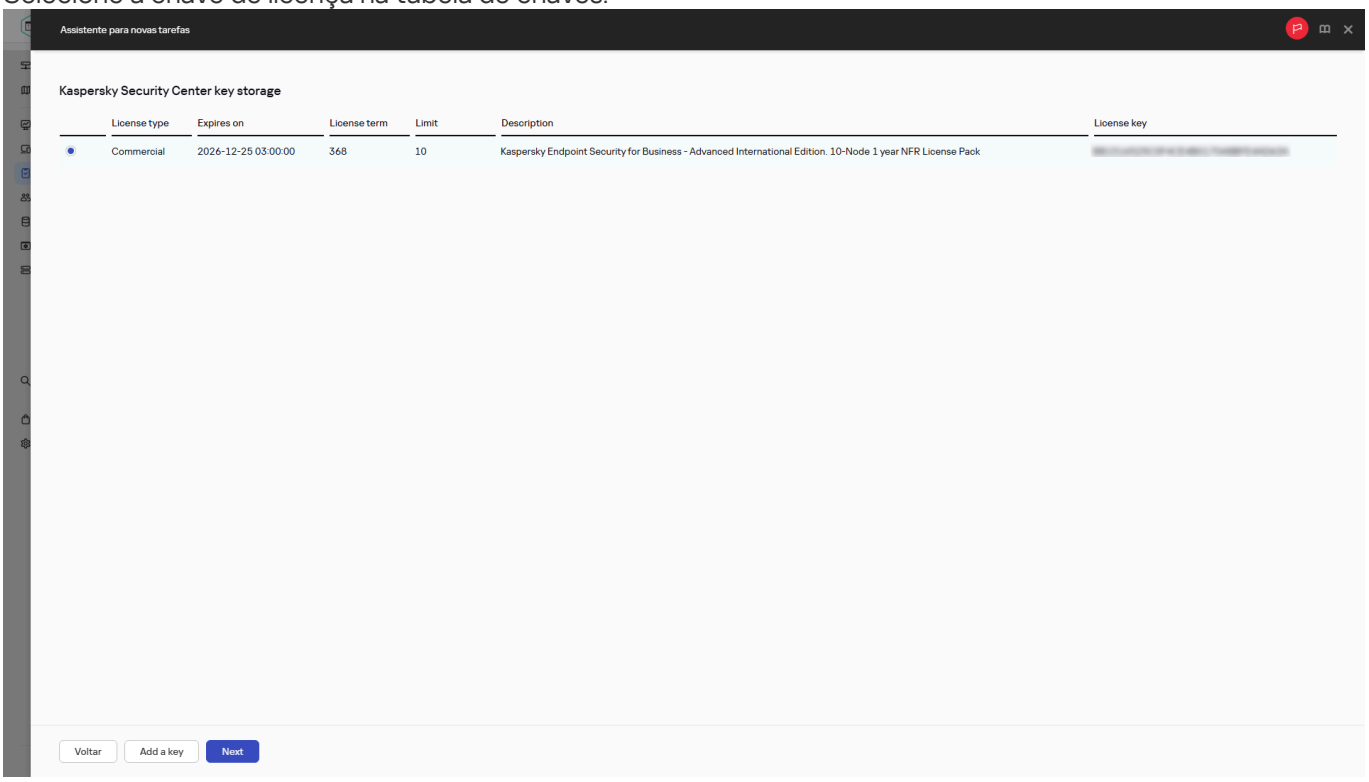
  As informações sobre a chave de licença são exibidas no painel de adição de chave de licença.

  c. Clique no botão **Salvar**.

Se você quiser distribuir automaticamente a chave de licença para dispositivos gerenciados, ative a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

O painel de adição de chave é fechado.

9. Selecione a chave de licença na tabela de chaves.

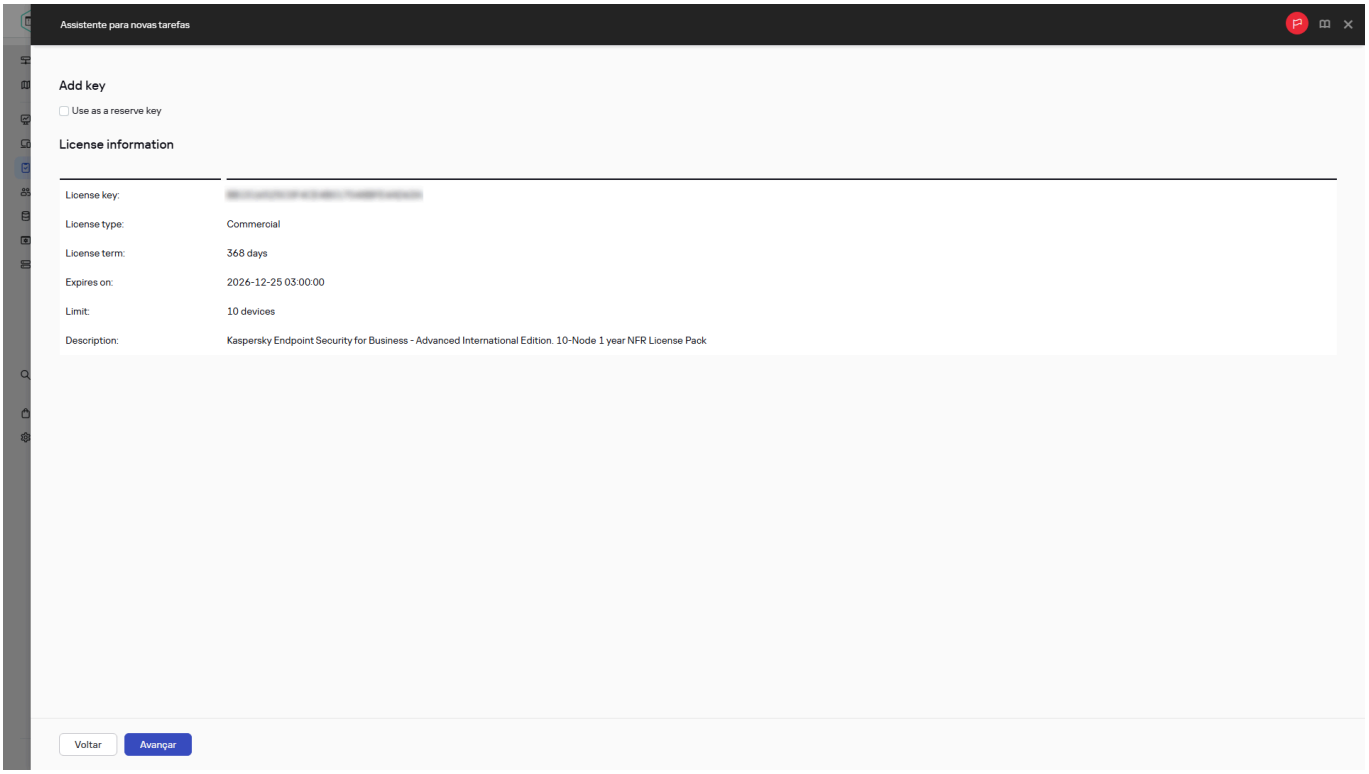


Seleção da chave de licença

10. Na etapa **Informações da licença** do assistente, desmarque a caixa de seleção padrão **Usar como chave reserva** caso queira substituir a chave de licença ativa.

    Por exemplo, isso é necessário quando a organização muda e a chave de outra organização é necessária no dispositivo; ou se a chave for emitida novamente e uma nova licença expirar antes da licença atual. Para evitar erros, é necessário desmarcar a caixa de seleção **Usar como chave reserva**.

Caso queira mais informações sobre os problemas que podem ocorrer ao adicionar uma chave de licença ao Kaspersky Security Center e como resolvê-los, consulte a base de conhecimento do Kaspersky Security Center.



Especificação da chave de licença reserva

11. Na etapa **Concluir a criação da tarefa** do assistente, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** para modificar as configurações padrão da tarefa.

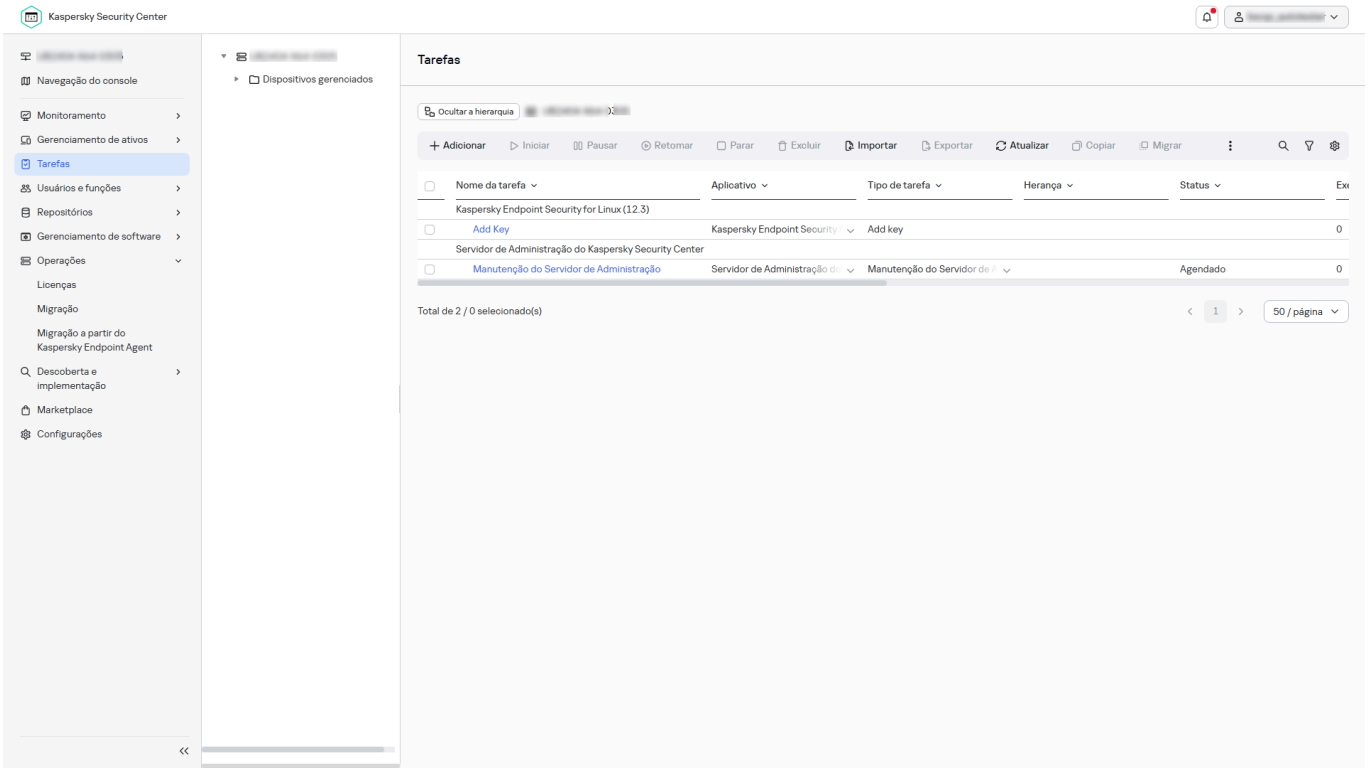
    Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois.

12. Clique no botão **Concluir**.

    O assistente cria a tarefa. Caso a opção **Abrir detalhes da tarefa quando a criação for concluída** tenha sido ativada, a janela de propriedades da tarefa abrirá automaticamente. Nesta janela, você pode especificar as configurações gerais da tarefa e, se necessário, alterar as configurações especificadas durante a criação da tarefa.

    Você também pode abrir a respectiva janela de propriedades clicando no nome da tarefa criada na lista de tarefas.

A tarefa é criada, configurada e exibida na lista de tarefas.



A lista de tarefas

13. Para executar a tarefa, selecione-a na lista de tarefas e, então, clique no botão **Iniciar**.

    Você também pode definir um agendamento de início de tarefa na guia **Agendamento** da janela de propriedades da tarefa.

    Para obter uma descrição detalhada das configurações de início agendado, consulte as configurações gerais da tarefa.

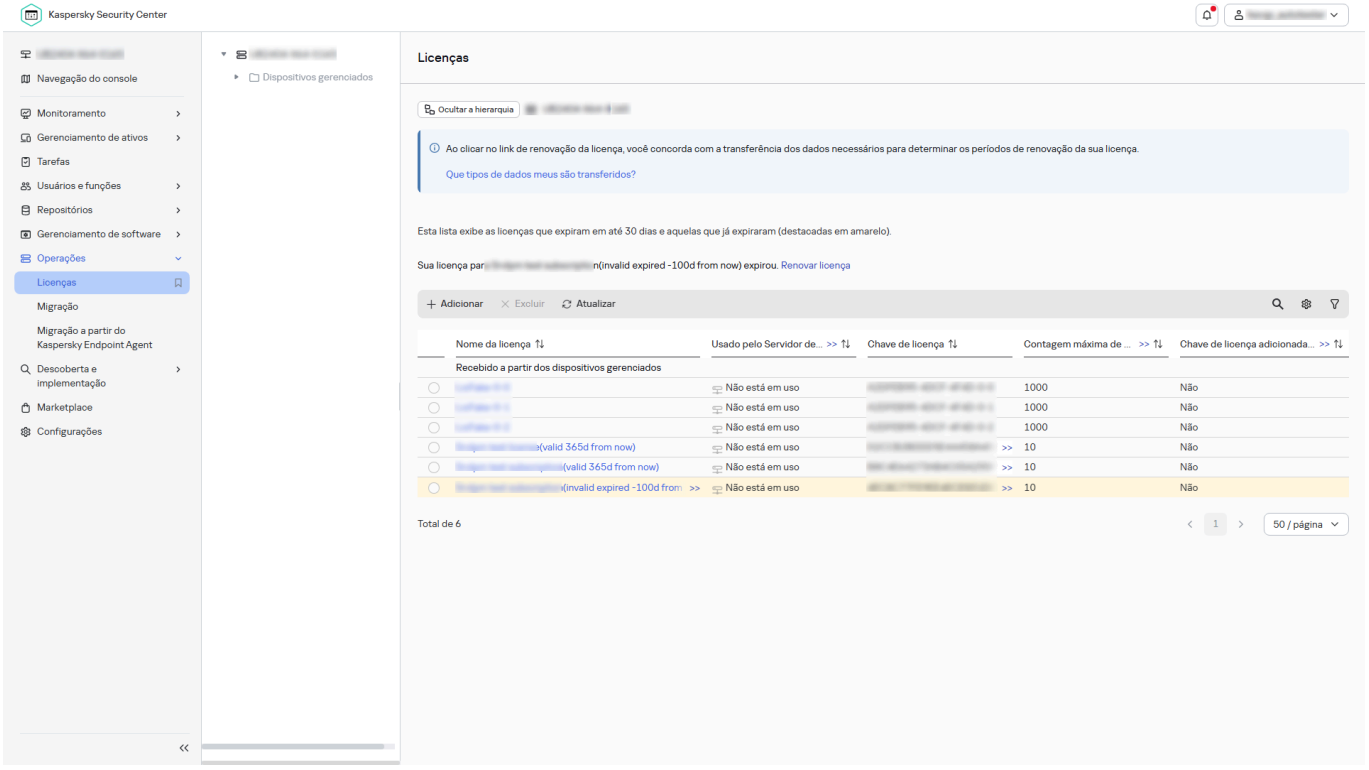
Depois que a tarefa for concluída, a chave de licença será implementada nos dispositivos selecionados.

Distribuição automática de uma chave de licença

O Kaspersky Security Center Linux permite a distribuição automática de chaves de licença para os dispositivos gerenciados, se elas estiverem localizadas no repositório de chaves de licença do Servidor de Administração.

Para distribuir automaticamente uma chave de licença para os dispositivos gerenciados:

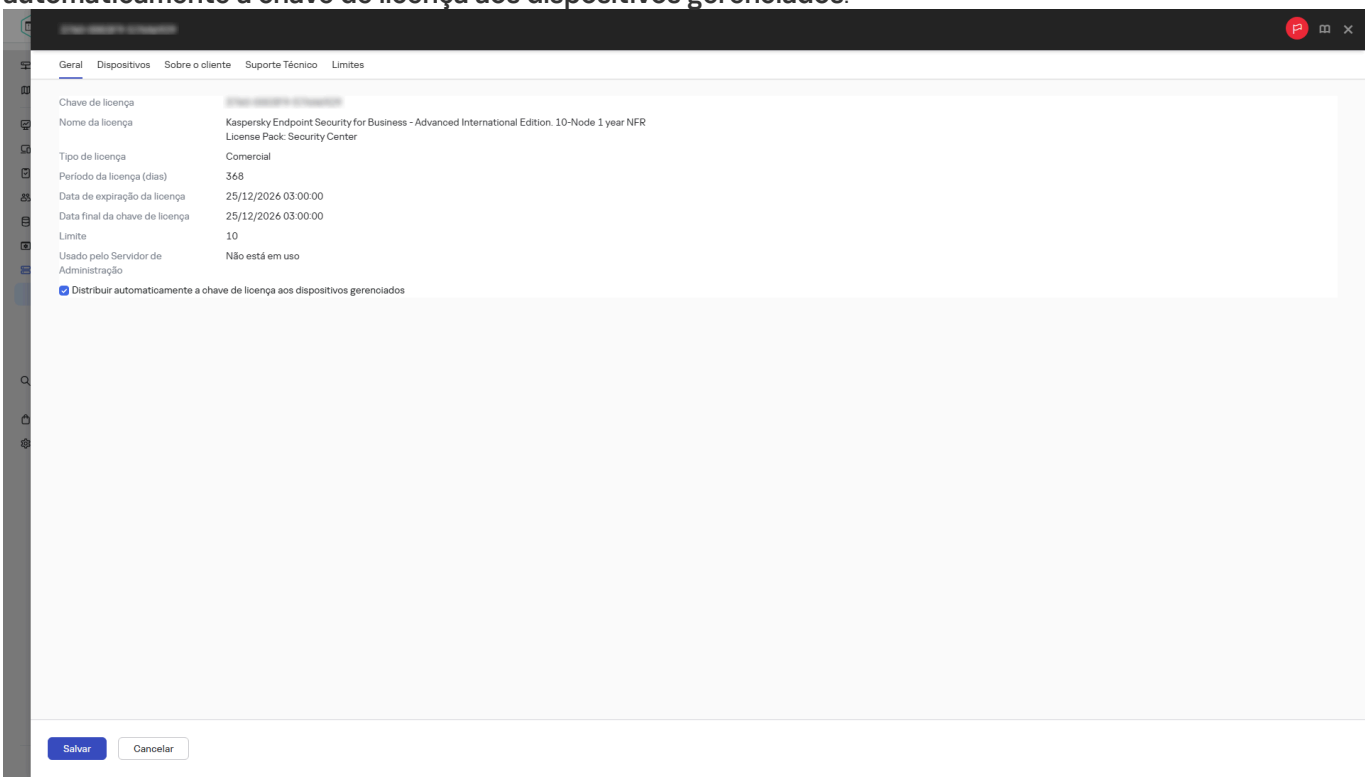
1. No menu principal, vá para **Operações → Licenciamento → Licenças**.



A lista de licenças

2. Clique em o nome da chave de licença que você pretende distribuir automaticamente para os dispositivos.

3. Na janela de propriedades da chave de licença que abrir, selecione a caixa de seleção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.



A janela de propriedades da chave de licença

4. Clique no botão **Salvar**.

A chave de licença será distribuída automaticamente para todos os dispositivos compatíveis.

A distribuição de chaves de licença é realizada através do Agente de Rede. Não é criada nenhuma tarefa de distribuição de chaves de licença para o aplicativo.

Durante a distribuição automática de uma chave de licença, o limite de licenciamento no número de dispositivos é levado em conta. O limite da licença é definido nas propriedades da chave de licença. Se o limite da licença for alcançado, a distribuição desta chave de licença nos dispositivos termina automaticamente.

Observe que uma chave de licença distribuída automaticamente pode não ser exibida no repositório do Servidor de Administração virtual nos seguintes casos:

- A chave de licença não é válida para o aplicativo.
- O Servidor de Administração virtual não tem dispositivos gerenciados.
- A chave de licença já foi usada para dispositivos gerenciados por outro Servidor de Administração virtual e o limite no número de dispositivos foi atingido.

O Servidor de Administração virtual distribui automaticamente chaves de licença de seu repositório e do repositório do Servidor de Administração. Recomendamos que você:

- Use a tarefa *Adicionar chave de licença* para selecionar a chave de licença que deve ser implementada nos dispositivos.
- Evite desativar a opção **Permitir a implementação automática das chaves de licença deste Servidor de Administração virtual em seus dispositivos** nas configurações do Servidor de Administração virtual. Caso contrário, o Servidor de Administração virtual não distribuirá chaves de licença aos dispositivos, incluindo as chaves de licença do repositório do Servidor de Administração.

Se a caixa de seleção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados** for marcada na janela de propriedades da chave de licença, uma chave de licença é distribuída em sua rede imediatamente. Caso essa opção não seja selecionada, será possível usar uma tarefa para distribuir uma chave de licença posteriormente.

A distribuição automática de chaves de licença configuradas no Servidor de Administração principal não se estende a dispositivos gerenciados por Servidores de Administração secundários não virtuais.

Visualizando de informações sobre chaves de licença em uso

Para exibir a lista das chaves de licença adicionadas ao repositório do Servidor de Administração:

No menu principal, vá para **Operações → Licenciamento → Licenças**.

A lista exibida contém os arquivo de chave e os códigos de ativação adicionados ao repositório do Servidor de Administração.

Para exibir as informações detalhadas sobre uma chave de licença:

1. No menu principal, vá para **Operações → Licenciamento → Licenças**.
2. Clique no nome da chave de licença necessária.

Na janela de propriedades da chave de licença que se abre, você pode visualizar:

- Na guia **Geral**: as informações principais sobre a chave de licença
- Na guia **Dispositivos**: a lista de dispositivos clientes em que a chave de licença foi usada para a ativação do aplicativo da Kaspersky instalado
- Na guia **Limites**: a lista de limites da licença

  Se você ativou o Servidor de Administração sob a licença do Kaspersky Next XDR Optimum, a guia **Limites** exibe o campo **XDR-O** com o valor **Ativado**.

Para exibir quais chaves de licença são implementadas em um dispositivo cliente específico:

1. No menu principal, vá para **Gerenciamento de ativos → Dispositivos gerenciados**.
2. Clique no nome do dispositivo necessário.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Aplicativos**.

4. Clique no nome do aplicativo do qual deseja exibir as informações sobre a chave de licença.

5. Na janela de propriedades do aplicativo que se abre, clique na guia **Geral** e abra a seção **Licença**.

   As informações principais sobre as chaves de licença adicional ativas são exibidas.

Para definir configurações atualizadas das chaves de licença do Servidor de Administração virtual, o Servidor de Administração envia uma solicitação para os servidores de ativação da Kaspersky ao menos uma vez por dia. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos.

Eventos do limite da licença excedidos

O Kaspersky Security Center Linux permite que você obtenha informações sobre eventos quando alguns limites da licença são excedidos pelos aplicativos da Kaspersky instalados nos dispositivos clientes.

O nível de importância desses eventos, quando excedido um limite da licença, é definido de acordo com as seguintes regras:

- Se o número de unidades atualmente usadas cobertas por uma única licença estiver entre 90% e 100% do número total de unidades cobertas pela licença, o evento é publicado com o nível de importância **Informação**.
- Se o número de unidades atualmente usadas cobertas por uma única licença estiver entre 100% e 110% do número total de unidades cobertas pela licença, o evento é publicado com o nível de importância **Advertência**.
- Se o número de unidades atualmente usadas cobertas por uma licença exceder 110% do número total de unidades cobertas pela mesma licença, o evento será publicado com o nível de importância de **Evento crítico**.

Excluindo uma chave de licença do repositório

Quando você excluir a chave de licença ativa implementada em um dispositivo gerenciado, o aplicativo continuará funcionando no dispositivo gerenciado.

Para excluir um arquivo de chave ou um código de ativação do repositório do Servidor de Administração:

1. Verifique se o Servidor de Administração não usa um arquivo de chave ou um código de ativação que se deseja excluir. Caso este seja o caso, não será possível removê-los. Para executar o teste:

   a. No menu principal, clique no nome do Servidor de Administração.

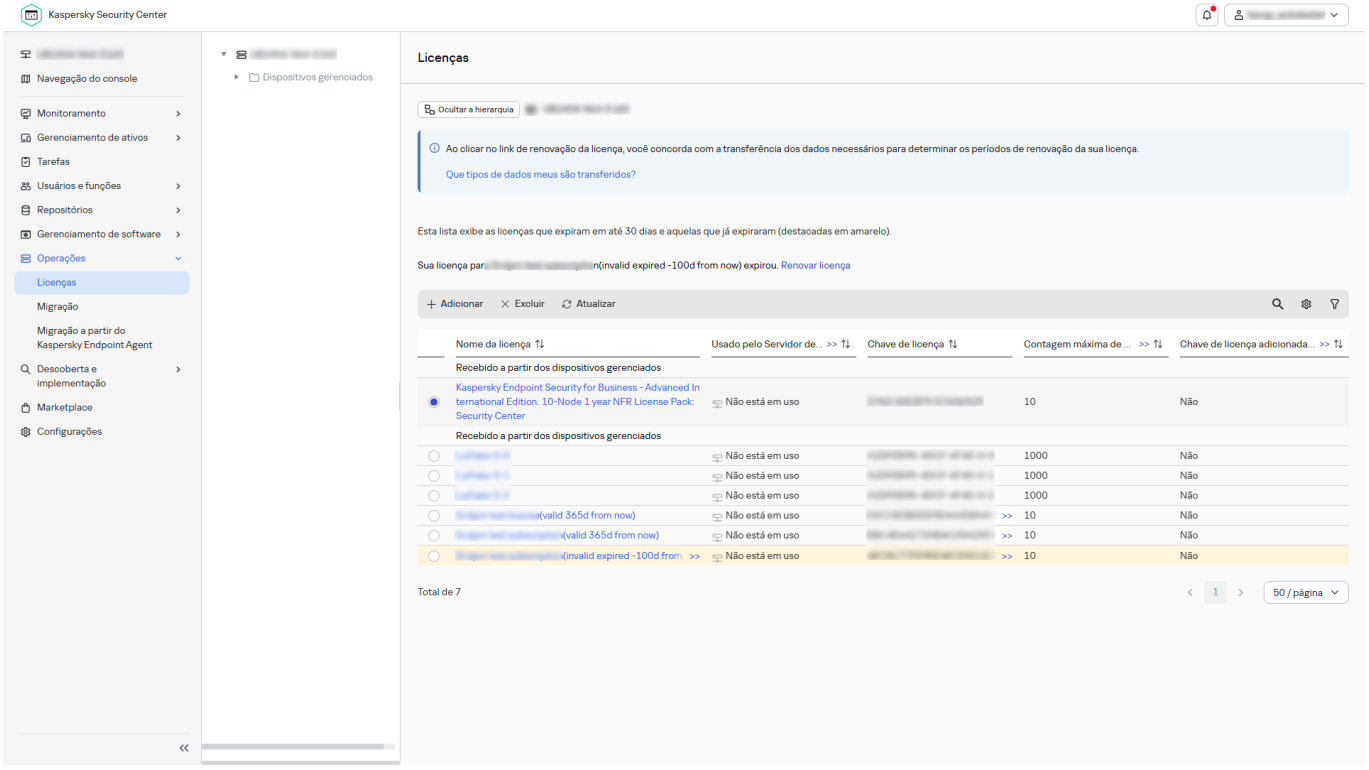
      A janela Propriedades do Servidor de Administração é aberta.

   b. Na guia **Geral**, selecione a seção **Chaves de licença**.

   c. Caso o arquivo de chave ou o código de ativação necessário seja exibido na seção aberta, clique no botão **Remover chave de licença ativa** e, em seguida, confirme a operação. Depois disso, o Servidor de Administração não usa a chave de licença removida, mas a chave permanece no repositório do Servidor de Administração. Caso o arquivo de chave ou o código de ativação necessário não seja exibido, o Servidor de Administração não o utilizará.

2. No menu principal, vá para **Operações** → **Licenciamento** → **Licenças**.

3. Selecione o arquivo de chave ou o código de ativação necessário e clique no botão **Excluir**.



A lista de licenças

O arquivo de chave ou o código de ativação selecionado são excluídos do repositório.

É possível adicionar novamente uma chave de licença removida ou adicionar uma nova chave de licença.

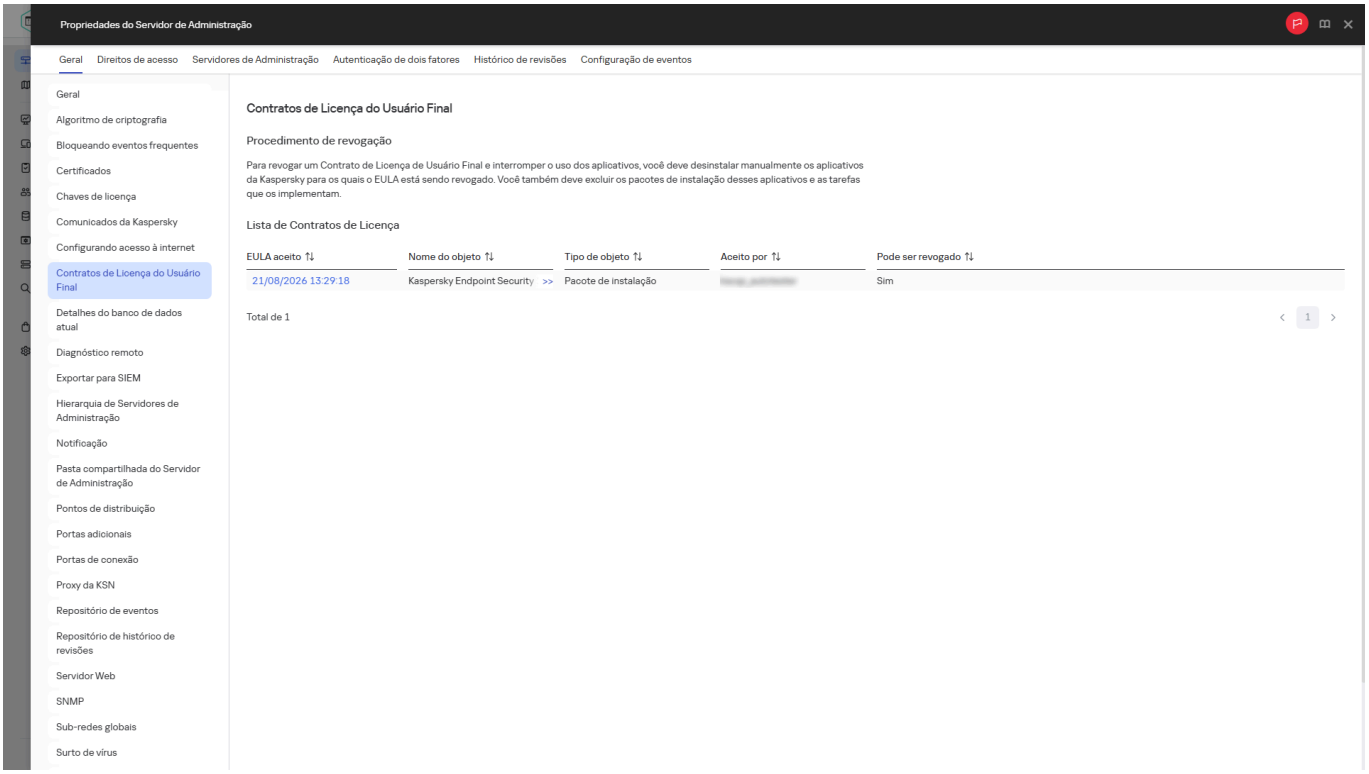
Revogando o consentimento com um Contrato de Licença do Usuário Final

Se você decidir parar de proteger alguns de seus dispositivos clientes, poderá revogar o Contrato de Licença do Usuário Final (EULA) para qualquer aplicativo da Kaspersky gerenciado. É necessário desinstalar o aplicativo selecionado antes de revogar seu EULA.

Para revogar o EULA dos aplicativos gerenciados da Kaspersky:

1. Abra a janela de propriedades do Servidor de Administração e, na guia **Geral**, selecione a seção **Contratos de Licença do Usuário Final**.

É exibida uma lista de EULAs, aceitos ao criar pacotes de instalação, durante a instalação contínua de atualizações ou mediante implementação do Kaspersky Security for Mobile.



A lista de EULAs

2. Na lista, selecione o EULA que deseja revogar.

   Você pode visualizar as seguintes propriedades da EULA:

   - Data em que o EULA foi aceito
   - Nome do usuário que aceitou o EULA

3. Clique na data de aceite de qualquer EULA para abrir sua janela de propriedades que exibe os seguintes dados:

   - Nome do usuário que aceitou o EULA
   - Data em que o EULA foi aceito
   - Identificador exclusivo (UID) do EULA
   - Texto completo do EULA
   - Lista de objetos (pacotes de instalação, atualizações contínuas, aplicativos móveis) vinculados ao EULA e seus respectivos nomes e tipos

4. Na parte inferior da janela de propriedades do EULA, clique no botão **Revogar Contrato de Licença**.

   Se existirem objetos (pacotes de instalação e suas respectivas tarefas) que impeçam a revogação do EULA, a notificação correspondente será exibida. Não é possível continuar com a revogação até que esses objetos sejam excluídos.

Na janela que se abre, você é informado que deve primeiro desinstalar o aplicativo da Kaspersky que corresponde ao EULA.

5. Clique no botão para confirmar a revogação.

A EULA foi revogada. Ele não é mais exibido na lista de Contratos de licença na seção **Contratos de Licença do Usuário Final**. A janela de propriedades do EULA se fecha; o aplicativo não estará mais instalado.

Renovando licenças para aplicativos da Kaspersky

Você pode renovar uma licença de um aplicativo da Kaspersky que expirou ou está prestes a expirar (em menos de 30 dias).

Para renovar uma licença expirada ou uma licença prestes a expirar:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Operações** → **Licenciamento** → **Licenças**.
   - No menu principal, vá para **Monitoramento** → **Painel**, e depois clique no link **Ver licenças expiradas** ao lado de uma notificação.

   A janela **Licenças** é aberta, permitindo visualiza e renovar licenças.

2. Clique no link **Renovar licença** ao lado da licença necessária.

   Ao clicar no link de renovação da licença, você concorda em transferir à Kaspersky as seguintes informações sobre o Kaspersky Security Center Linux: a versão, a localização de uso, o ID de licença do software (ou seja, o ID da licença sendo renovada), se a licença foi comprada via empresa parceira ou não.

3. Na janela aberta do serviço de renovação de licença, siga as instruções para renovar uma licença.

   A licença foi renovada.

No Kaspersky Security Center Web Console, são exibidas notificações quando uma licença está prestes a expirar, de acordo com a seguinte programação:

- 30 dias antes do vencimento
- 7 dias antes do vencimento
- 3 dias antes do vencimento
- 24 horas antes do vencimento
- Quando uma licença expirou

Usando o Kaspersky Marketplace para escolher as soluções comerciais Kaspersky de sua preferência

Marketplace é uma seção no menu principal que permite visualizar toda a gama de soluções comerciais Kaspersky. Selecione as que você precisa e prossiga com a compra no site da Kaspersky. Você pode usar filtros para visualizar apenas as soluções que se adaptam à sua organização e aos requisitos do seu sistema de segurança da informação. Ao selecionar uma solução, o Kaspersky Security Center Linux redireciona o acesso para a página da web relacionada ao site da Kaspersky para saber mais detalhes sobre essa solução. Cada página da web permite efetuar compra ou contém instruções sobre o processo de compra.

Na seção **Marketplace**, você pode filtrar as soluções Kaspersky usando os seguintes critérios:

- Número de dispositivos (endpoints, servidores e outros tipos de ativos) que você deseja proteger:
  - 50–250
  - 250–1000
  - Mais de 1000
- Nível de experiência da equipe de segurança da informação da sua organização:
  - **Foundations**

    Este nível é típico para empresas que possuem apenas uma equipe de TI. O número máximo possível de ameaças é bloqueado automaticamente.
  - **Optimum**

    Esse nível é típico para empresas que têm uma função de segurança de TI específica na equipe de TI. Nesse nível, as empresas precisam de soluções que lhes permitam enfrentar as ameaças genéricas e também as que desviam dos mecanismos preventivos existentes.
  - **Expert**

    Este nível é típico para empresas com ambientes de TI complexos e distribuídos. A equipe de segurança de TI é experiente ou a empresa possui uma equipe de SOC (Security Operations Center). As soluções necessárias permitem que as empresas enfrentem ameaças complexas e ataques direcionados.
- Tipos de ativos que você deseja proteger:
  - **Endpoints**: estações de trabalho de funcionários, máquinas físicas e virtuais, sistemas integrados
  - **Servidores**: servidores físicos e virtuais
  - **Nuvem**: ambientes de nuvem pública, privada ou híbrida; serviços na nuvem
  - **Rede**: rede local, infraestrutura de TI
  - **Serviço**: serviços relacionados à segurança fornecidos pela Kaspersky

Para encontrar e adquirir uma solução empresarial Kaspersky:

1. No menu principal, vá para **Marketplace**.

   Por padrão, a seção exibe todas as soluções comerciais Kaspersky disponíveis.

2. Para visualizar apenas as soluções adequadas à sua organização, selecione os valores necessários nos filtros.

3. Clique na solução que deseja adquirir ou sobre a qual deseja saber mais.

Você será redirecionado para a página da solução. Você pode seguir as instruções na tela para prosseguir com a compra.

Configuração de aplicativos da Kaspersky

Esta seção contém informações sobre a configuração manual de políticas e tarefas, funções de usuário, criação de uma estrutura de grupo de administração e hierarquia de tarefas.

Cenário: Configurar a proteção da rede

O Assistente de início rápido cria políticas e tarefas com as configurações padrão. Essas configurações podem ficar abaixo do ideal ou até mesmo não serem permitidas por uma organização. Portanto, recomendamos que você ajuste essas políticas e tarefas e, então, crie outras se forem necessárias para a sua rede.

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- Servidor de Administração do Kaspersky Security Center Linux instalado
- Kaspersky Security Center Web Console instalado
- Cenário principal de instalação do Kaspersky Security Center Linux concluído
- Concluiu o Assistente de início rápido ou criou manualmente as seguintes políticas e tarefas no grupo de administração **Dispositivos gerenciados**:
  - Política do Kaspersky Endpoint Security
  - Tarefa de grupo para atualizar o Kaspersky Endpoint Security
  - Política de Agente de Rede
  - Tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*

Fases

A configuração da proteção de rede continua em fases:

1. **Configuração e propagação de políticas e perfis da política de aplicativos Kaspersky**

   Para configurar e propagar as configurações dos aplicativos Kaspersky instalados nos dispositivos gerenciados, você pode usar duas abordagens de gerenciamento de segurança diferentes: centrado no dispositivo ou centrado no usuário. Essas duas abordagens também podem ser combinadas.

2. **Configuração de tarefas de gerenciamento remoto de aplicativos Kaspersky**

   Verifique as tarefas criadas com o Assistente de início rápido e faça o ajuste fino delas, se necessário.

Instruções de procedimento: Configurar a tarefa de grupo para atualizar o Kaspersky Endpoint Security, Criar a tarefa Encontrar as vulnerabilidades e as atualizações necessárias.

Se necessário, crie tarefas adicionais para gerenciar os aplicativos da Kaspersky instalados nos dispositivos clientes.

3. **Avaliação e limitação da carga de eventos no banco de dados**

   As informações sobre eventos que ocorrem durante a operação de aplicativos gerenciados são transferidas a partir de um dispositivo cliente e registradas no banco de dados do Servidor de Administração. Para reduzir a carga do Servidor de Administração, avalie e limite o número máximo de eventos que podem ser armazenados no banco de dados.

   Instruções: Configurando o número máximo de eventos.

Resultados

Quando você concluir esse cenário, sua rede estará protegida pela configuração de aplicativos, tarefas e eventos da Kaspersky recebidos pelo Servidor de Administração:

- Os aplicativos Kaspersky são configurados de acordo com as políticas e perfis de política.
- Os aplicativos são gerenciados através de um conjunto de tarefas.
- O número máximo de eventos que podem ser armazenados no banco de dados está definido.

Quando a configuração da proteção de rede for concluída, você poderá prosseguir para configurar atualizações regulares para bancos de dados e aplicativos Kaspersky.

Sobre as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário

Você pode gerenciar configurações de segurança do ponto de vista de recursos de dispositivo e do ponto de vista de funções de usuário. A primeira abordagem é chamada de *gerenciamento de segurança centrado no dispositivo*, e a segunda, *gerenciamento de segurança centrado no usuário*. Para aplicar configurações de aplicativos diferentes a dispositivos diferentes, é possível usar um dos tipos de gerenciamento ou ambos em conjunto.

O gerenciamento de segurança centralizado no dispositivo permite aplicar diferentes configurações de aplicativos de segurança aos dispositivos gerenciados, dependendo dos recursos específicos do dispositivo. Por exemplo, você pode aplicar configurações diferentes aos dispositivos alocados em diferentes grupos de administração.

O gerenciamento de segurança centralizado no usuário permite aplicar diferentes configurações do aplicativo de segurança à diferentes funções do usuário. Você pode criar várias funções de usuário, atribuir uma função de usuário apropriada á cada usuário e definir configurações de aplicativos diferentes para os dispositivos pertencentes a usuários com funções diferentes. Por exemplo, convém aplicar configurações do aplicativo diferentes nos dispositivos de contadores e especialistas em recursos humanos (RH). Como resultado, quando o gerenciamento de segurança centrado no usuário é implementado, cada departamento, o departamento de contas e o departamento de RH, têm a sua própria configuração para os aplicativos Kaspersky. Uma configuração define qual configuração do aplicativo pode ser modificada pelos usuários e que são impostas e bloqueadas pelo administrador.

Ao usar o gerenciamento de segurança centrado no usuário, você pode aplicar configurações de aplicativo específicas a usuários individuais. Isso pode ser necessário quando um funcionário tem uma função única na empresa ou quando o usuário quer monitorar os problemas de segurança relacionados aos dispositivos de uma pessoa específica. Dependendo da função desse funcionário na empresa, você pode expandir ou limitar os direitos dessa pessoa para alterar as configurações do aplicativo. Por exemplo, é possível expandir os direitos de um administrador do sistema que gerencia dispositivos clientes em um escritório local.

Você também pode combinar as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário. Por exemplo, você pode configurar uma política de aplicativo específica para cada grupo de administração e, adicionalmente, criar perfis de política para uma ou várias funções dos usuários da sua empresa. Nesse caso, as políticas e os perfis de política são aplicados na seguinte ordem:

1. As políticas criadas para o gerenciamento de segurança centrado no dispositivo são aplicadas.
2. Elas são modificadas pelos perfis de política segundo as prioridades de perfil de política.
3. As políticas são modificadas pelos perfis de política associados às funções de usuário.

Configuração e propagação de políticas: abordagem centrada no dispositivo

Quando você concluir este cenário, os aplicativos serão configurados em todos os dispositivos gerenciados em conformidade com as políticas de aplicativo e perfis da política definidos por você.

Pré-requisitos

Antes de iniciar, verifique e confirme se foi instalado o Servidor de Administração do Kaspersky Security Center Linux e o Kaspersky Security Center Web Console. Você pode também considerar o gerenciamento de segurança centrado no usuário como uma alternativa ou opção adicional à abordagem centrada no dispositivo. Saiba mais sobre duas abordagens de gerenciamento.

Fases

O cenário de gerenciamento centrado no dispositivo dos aplicativos Kaspersky consiste nas seguintes etapas:

1. **Configurar os políticas de aplicativo**

   Defina as configurações para aplicativos Kaspersky instalados nos dispositivos gerenciados por meio da criação de uma política para cada aplicativo. Esse conjunto de políticas será propagado para os dispositivos cliente.

   Quando a proteção da rede é configurada no assistente de início rápido, o Kaspersky Security Center Linux cria a política padrão para os seguintes aplicativos:

   - Kaspersky Endpoint Security for Linux – para dispositivos clientes baseados em Linux
   - Kaspersky Endpoint Security for Windows – para dispositivos clientes baseados em Windows

Se tiver concluído o processo de configuração usando este assistente, você não precisará criar uma nova política para este aplicativo.

Se você tiver uma estrutura hierárquica de vários Servidores de Administração e/ou grupos de administração, os Servidores de Administração secundários e os grupos de administração secundários herdarão as políticas do Servidor de Administração principal por padrão. Você pode forçar a herança pelos grupos secundários e Servidores de Administração secundários para proibir qualquer modificação das configurações definidas na política de fluxo acima. Se você quiser que somente uma parte das configurações seja herdada por imposição, poderá bloqueá-las na política de fluxo acima. O restante das configurações desbloqueadas ficarão disponíveis para modificação nas políticas de fluxo abaixo. A hierarquia de políticas criada permite que você gerencie dispositivos nos grupos de administração com mais eficiência.

Instruções: Criação de uma política

2. **Criar os perfis da política (opcional)**

   Se você quiser que os dispositivos em um único grupo de administração seja executado sob diferentes configurações de política, crie perfis de políticas para esses dispositivos. Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos de destino em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo gerenciado.

   Usando condições de ativação do perfil, você pode aplicar diferentes perfis de políticas, por exemplo, nos dispositivos, tendo a configuração de hardware específica ou marcada com tags específicas. Use tags para filtrar dispositivos que atendem a critérios específicos. Por exemplo, você pode criar uma tag denominada *CentOS*, marcar todos os dispositivos executando o sistema operacional CentOS com essa tag e especificar essa tag como uma condição de ativação para um perfil da política. Como resultado, os aplicativos Kaspersky instalados em todos os dispositivos executando o CentOS serão gerenciados por seu próprio perfil da política.

   Instruções:

   - Criar um perfil da política
   - Criar uma regra de ativação do perfil da política

3. **Propagar políticas e perfil da política para os dispositivos gerenciados**

   Por padrão, o Servidor de Administração sincroniza automaticamente com os dispositivos gerenciados a cada 15 minutos. Durante a sincronização, as políticas novas ou alteradas e os perfis da política são propagados para os dispositivos gerenciados. Você pode ignorar a sincronização automática e executar a sincronização manualmente usando o comando Forçar a sincronização. Quando a sincronização estiver concluída, as políticas e os perfis da política serão entregues e aplicados aos aplicativos Kaspersky instalados.

   Você pode verificar se as políticas e os perfis da política foram entregues a um dispositivo. O Kaspersky Security Center Linux especifica a data e hora de entrega nas propriedades do dispositivo.

   Instruções: Sincronização forçada

Resultados

Quando o cenário centrado no dispositivo for concluído, os aplicativos Kaspersky serão configurados segundo as configurações especificadas e propagadas por meio da hierarquia de políticas.

As políticas e perfis da política de aplicativo configuradas serão aplicadas automaticamente aos novos dispositivos adicionados aos grupos de administração.

Configuração e propagação de políticas: abordagem centrada no usuário

Esta seção descreve o cenário da abordagem centrada no usuário para configuração centralizada de aplicativos da Kaspersky instalados nos dispositivos gerenciados. Quando você concluir este cenário, os aplicativos serão configurados em todos os dispositivos gerenciados em conformidade com as políticas de aplicativo e perfis da política definidos por você.

Pré-requisitos

Antes de iniciar, verifique e confirme se foi instalado o Servidor de Administração do Kaspersky Security Center Linux e o Kaspersky Security Center Web Console, e concluído o cenário de implementação principal. Você pode também considerar o gerenciamento de segurança centrado no dispositivo como uma alternativa ou opção adicional à abordagem centrada no usuário. Saiba mais sobre duas abordagens de gerenciamento.

Processar

O cenário de gerenciamento centrado no usuário dos aplicativos da Kaspersky consiste nas seguintes etapas:

1. **Configurar os políticas de aplicativo**

   Defina as configurações para aplicativos Kaspersky instalados nos dispositivos gerenciados por meio da criação de uma política para cada aplicativo. Esse conjunto de políticas será propagado para os dispositivos cliente.

   Quando a proteção da sua rede é configurada no assistente de início rápido, o Kaspersky Security Center Linux cria a política padrão do Kaspersky Endpoint Security. Se tiver concluído o processo de configuração usando este assistente, você não precisará criar uma nova política para este aplicativo.

   Se você tiver uma estrutura hierárquica de vários Servidores de Administração e/ou grupos de administração, os Servidores de Administração secundários e os grupos de administração secundários herdarão as políticas do Servidor de Administração principal por padrão. Você pode forçar a herança pelos grupos secundários e Servidores de Administração secundários para proibir qualquer modificação das configurações definidas na política de fluxo acima. Se você quiser que somente uma parte das configurações seja herdada por imposição, poderá bloqueá-las na política de fluxo acima. O restante das configurações desbloqueadas ficarão disponíveis para modificação nas políticas de fluxo abaixo. A hierarquia de políticas criada permite que você gerencie dispositivos nos grupos de administração com mais eficiência.

   Instruções: Criação de uma política

2. **Especificar proprietários dos dispositivos**

   Atribua os dispositivos gerenciados aos usuários correspondentes.

   Instruções: Atribuição de um usuário como proprietário do dispositivo

3. **Definir funções do usuário típicas para a sua empresa**

   Pense sobre diferentes tipos de trabalhos que os funcionários da sua empresa normalmente executam. Você deve dividir todos de acordo com as funções. Por exemplo, você pode dividi-los por departamentos, profissões ou cargos. Depois disso, você precisará criar uma função do usuário para cada grupo. Tenha em mente que cada função do usuário terá seu próprio perfil da política contendo configurações do aplicativo específicas para essa função.

4. **Criar funções de usuário**

   Crie e configure uma função do usuário para cada grupo de funcionários que você definiu na etapa anterior ou use as funções do usuário predefinidas. As funções do usuário conterão o conjunto de direitos de acesso aos recursos do aplicativo.

   Instruções: Criação de uma função de usuário

5. **Especificar o escopo de cada função de usuário**

   Para cada uma das funções de usuário criadas, defina usuários e/ou grupos de segurança e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

   Instruções: Edição do escopo de uma função de usuário

6. **Criar os perfis da política**

   Crie um perfil da política para cada função de usuário em sua empresa. Os perfis da política definem quais configurações serão aplicadas aos aplicativos instalados em dispositivos de usuários dependendo da função de cada usuário.

   Instruções: Criação de um perfil da política

7. **Associar perfis da política com as funções do usuário**

   Associe os perfis de política criados com as funções do usuário. Depois disso: o perfil da política fica ativo para um usuário com a função especificada. As configurações definidas no perfil da política serão aplicadas aos aplicativos da Kaspersky instalados nos dispositivos do usuário.

   Instruções: Associar perfis da política a funções

8. **Propagar políticas e perfil da política para os dispositivos gerenciados**

   Por padrão, o Kaspersky Security Center Linux sincroniza automaticamente o Servidor de Administração com os dispositivos gerenciados a cada 15 minutos. Durante a sincronização, as políticas novas ou alteradas e os perfis da política são propagados para os dispositivos gerenciados. Você pode ignorar a auto sincronização e executar a sincronização manualmente usando o comando Forçar a sincronização. Quando a sincronização estiver concluída, as políticas e os perfis da política serão entregues e aplicados aos aplicativos Kaspersky instalados.

   Você pode verificar se as políticas e os perfis da política foram entregues a um dispositivo. O Kaspersky Security Center Linux especifica a data e hora de entrega nas propriedades do dispositivo.

   Instruções: Sincronização forçada

Resultados

Quando o cenário centrado no usuário for concluído, os aplicativos da Kaspersky serão configurados segundo as configurações especificadas e propagadas por meio da hierarquia de políticas e perfis de política.

Para um novo usuário, você terá de criar uma nova conta, atribuir o usuário com uma das funções de usuário criadas e atribuir os dispositivos ao usuário. As políticas e perfis da política de aplicativo configuradas serão automaticamente aplicadas aos novos dispositivos adicionados aos dispositivos de esse usuário.

Políticas e perfis da política

No Kaspersky Security Center Web Console, é possível criar políticas para aplicativos da Kaspersky. Esta seção descreve políticas e perfis da política e fornece instruções para criá-las e modificá-las.

Sobre as políticas e perfis de política

Uma *política* é um conjunto de configurações do aplicativo Kaspersky, aplicadas a um grupo de administração e seus subgrupos. Você pode instalar vários aplicativos Kaspersky nos dispositivos de um grupo de administração. O Kaspersky Security Center fornece uma única política para cada aplicativo Kaspersky em um grupo de administração. Uma política possui um dos seguintes status:

O status da política

Estado	Descrição
Ativo	A política atual aplicada ao dispositivo. Apenas uma política pode estar ativa por aplicativo Kaspersky em cada grupo de administração. Os dispositivos aplicam os valores de configuração de uma política ativa para um aplicativo Kaspersky.
Inativo	Uma política que não é aplicada atualmente a um dispositivo.
Ausência	Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

As políticas funcionam de acordo com as seguintes regras:

- Várias políticas com valores diferentes podem ser configuradas para um único aplicativo.
- Apenas uma política pode estar ativa para o aplicativo atual.
- Uma política pode ter políticas secundárias.

Geralmente, você pode usar políticas como preparação para situações de emergência, como um ataque de vírus. Se houver um ataque por meio de unidades flash, você pode ativar uma política que bloqueie o acesso a unidades flash. Nesse caso, a política ativa atual torna-se automaticamente inativa.

Para evitar ter que efetuar manutenção de várias políticas, por exemplo, quando ocasiões diferentes pressupõem a alteração de várias configurações apenas, você pode usar perfis de política.

Um *perfil* de *política* é um subconjunto nomeado de valores de configuração que substitui os valores de configuração de uma política. Um perfil de política afeta a formação de configurações efetivas em um dispositivo gerenciado. *Configurações em vigor* são um conjunto de configurações de política, configurações de perfil de política e configurações de aplicativo locais aplicadas atualmente ao dispositivo.

Os perfis de política funcionam de acordo com as seguintes regras:

- Um perfil de política entra em vigor quando ocorre uma condição de ativação específica.
- Os perfis contêm valores de configurações que diferem das configurações de política.

- A ativação de um perfil de política altera as configurações em vigor do dispositivo gerenciado.
- Uma política pode incluir no máximo 100 perfis de política.

Sobre as configurações de bloqueio e bloqueadas

Cada configuração de política tem um ícone de botão de bloqueio (). A tabela abaixo mostra os status do botão de bloqueio:

Status do botão de bloqueio

Estado	Descrição
Undefined	Se um cadeado aberto for exibido ao lado de uma configuração e o botão de alternância estiver desativado, a configuração não será especificada na política. Um usuário pode alterar essas configurações na interface gerenciada do aplicativo. Esse tipo de configuração é chamado de *desbloqueado*.
Enforce	Se um cadeado fechado for exibido ao lado de uma configuração e o botão de alternância estiver ativado, a configuração será aplicada aos dispositivos nos quais essa política é aplicada. O usuário não pode modificar os valores dessas configurações na interface gerenciada do aplicativo. Esse tipo de configuração é chamado de *bloqueado*.

É altamente recomendável que você bloqueie as configurações da política que deseja aplicar nos dispositivos gerenciados. As configurações da política desbloqueadas podem ser reatribuídas pelas configurações do aplicativo da Kaspersky em um dispositivo gerenciado.

Você pode usar um botão de bloqueio para realizar as seguintes ações:

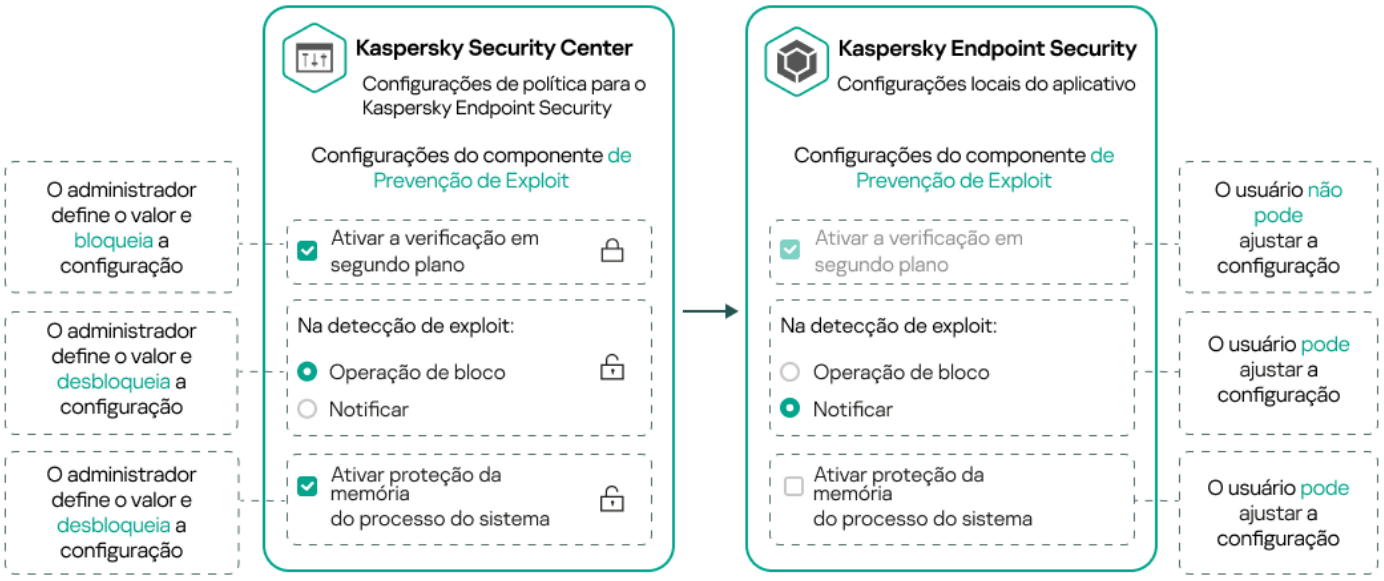
- Configurações de bloqueio para uma política de subgrupo de administração
- Bloqueando as configurações de um aplicativo da Kaspersky em um dispositivo gerenciado

Assim, uma configuração bloqueada é usada para implementar configurações efetivas em um dispositivo gerenciado.

Um processo de implementação de configurações eficazes inclui as seguintes ações:

- O dispositivo gerenciado aplica os valores de configuração do aplicativo da Kaspersky.
- O dispositivo gerenciado aplica valores de configurações bloqueados de uma política.

Uma política e um aplicativo da Kaspersky gerenciado contêm o mesmo conjunto de configurações. Ao definir as configurações de política, as configurações do aplicativo da Kaspersky mudam de valores em um dispositivo gerenciado. Não é possível ajustar as configurações bloqueadas em um dispositivo gerenciado (ver figura abaixo):



Configurações de bloqueio e de aplicativos da Kaspersky

Herança de políticas e perfis de política

Esta seção fornece informações sobre a hierarquia e herança de políticas e perfis de política.

Hierarquia de políticas

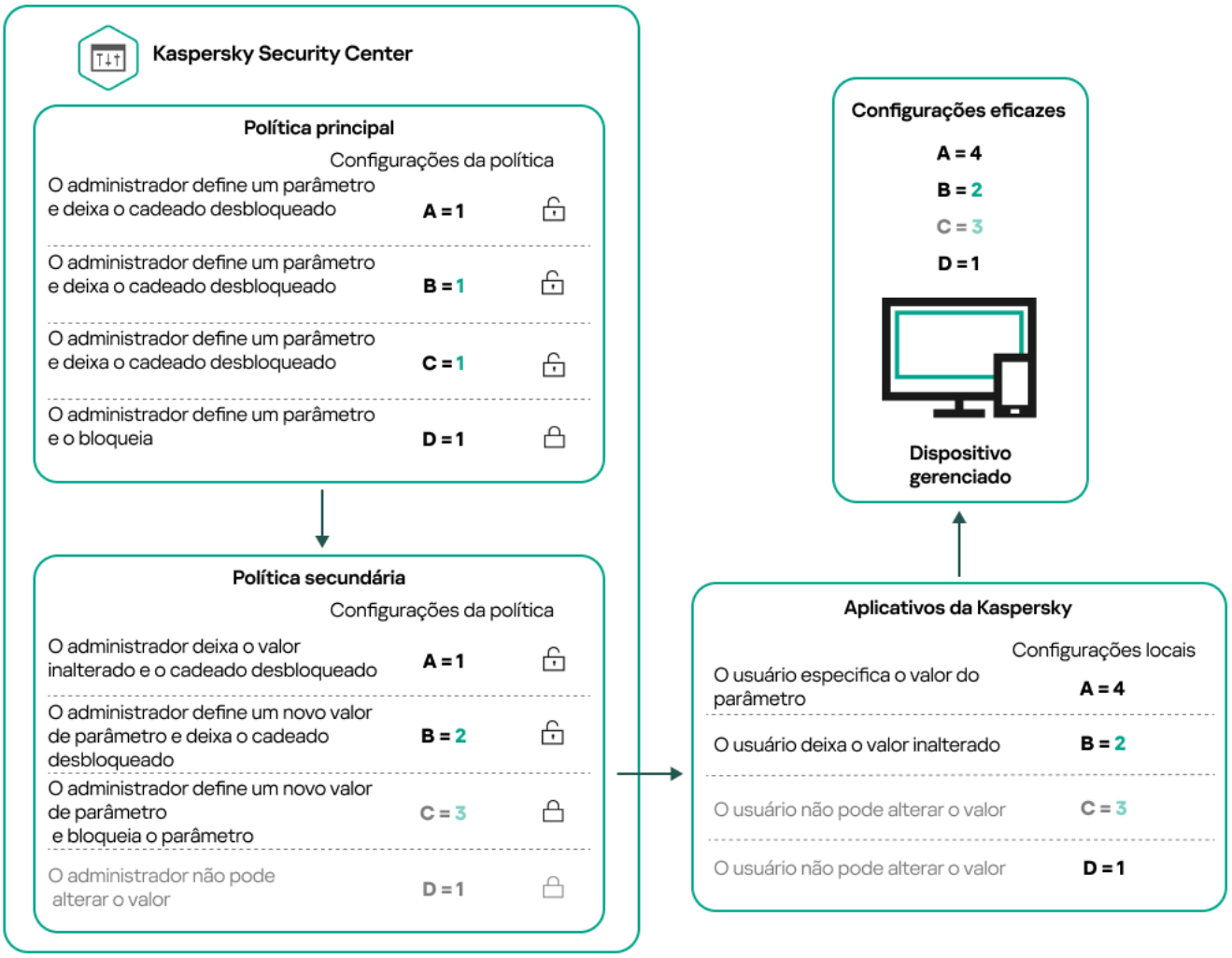
Se dispositivos diferentes precisarem de configurações diferentes, você pode organizar os dispositivos em grupos de administração.

Você pode especificar uma política para um único grupo de administração. As configurações de política podem ser *herdadas*. Herança significa receber valores de configurações de política em subgrupos (grupos secundários) de uma política de um grupo de administração de nível superior (principal).

Depois disso, a política de um grupo principal é também referida como uma *política principal*. Uma política para um subgrupo (grupo secundário) também é chamada de *política secundária*.

Por padrão, pelo menos um grupo de dispositivos gerenciados existe no Servidor de Administração. Se você deseja criar grupos personalizados, esses são criados como subgrupos (grupos secundários) dentro do grupo de dispositivos gerenciados.

Políticas de um mesmo aplicativo atuam entre si, de acordo com uma hierarquia de grupos de administração. As configurações bloqueadas de uma política de um grupo de administração de nível superior (principal) reatribuirão os valores das configurações de política de um subgrupo (ver figura abaixo).



Hierarquia de políticas

Perfis de política em uma hierarquia de políticas

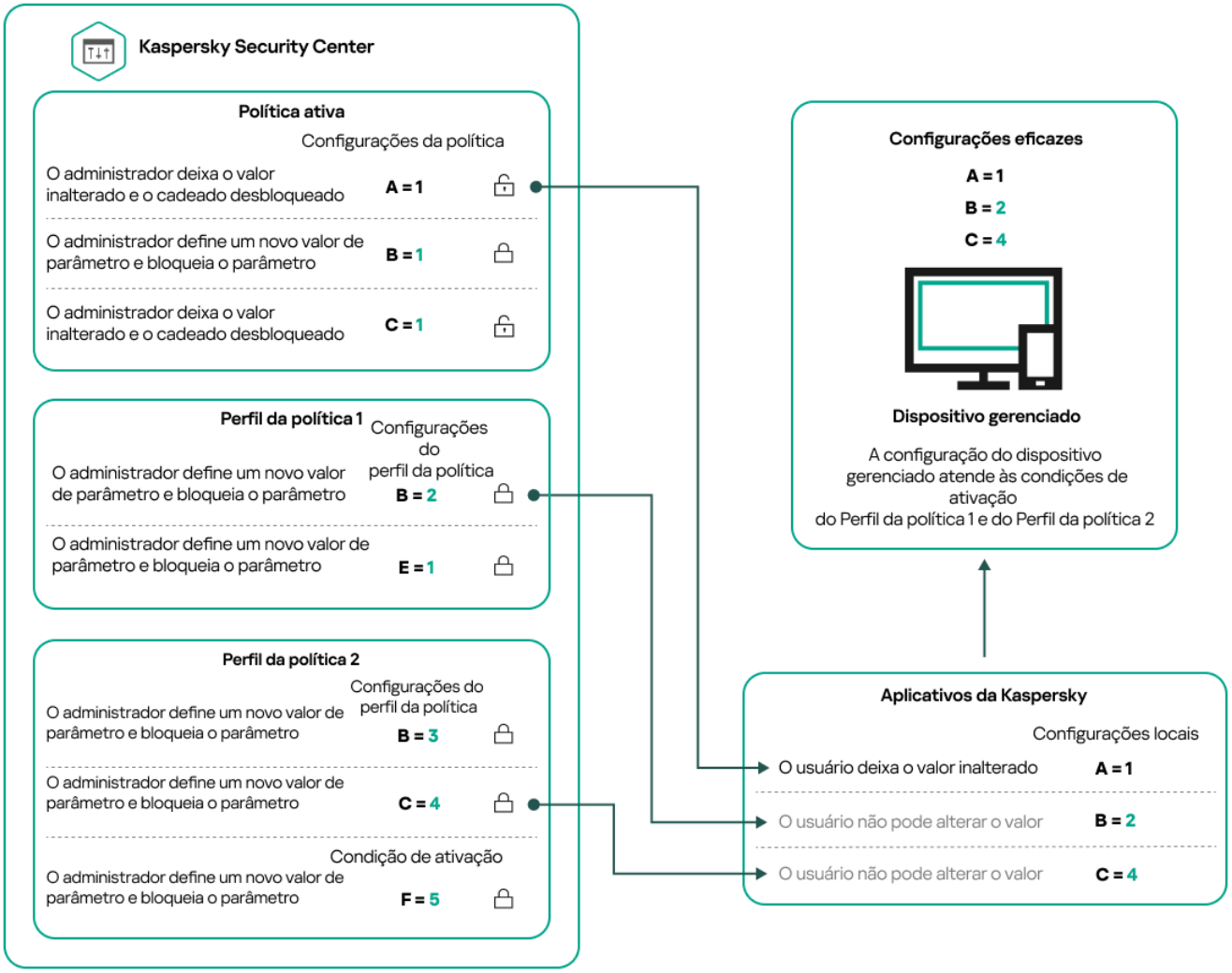
Os perfis de política têm as seguintes condições de atribuição de prioridade:

- A posição de um perfil em uma lista de perfis de política indica sua prioridade. Você pode alterar uma prioridade de perfil da política. A posição mais alta em uma lista indica a prioridade mais alta (veja a figura abaixo).



Definição de prioridade de um perfil de política

- As condições de ativação dos perfis de política não dependem umas das outras. Vários perfis de política podem ser ativados simultaneamente. Se vários perfis de política afetam a mesma configuração, o dispositivo obtém o valor de configuração do perfil de política com a prioridade mais alta (veja a figura abaixo).

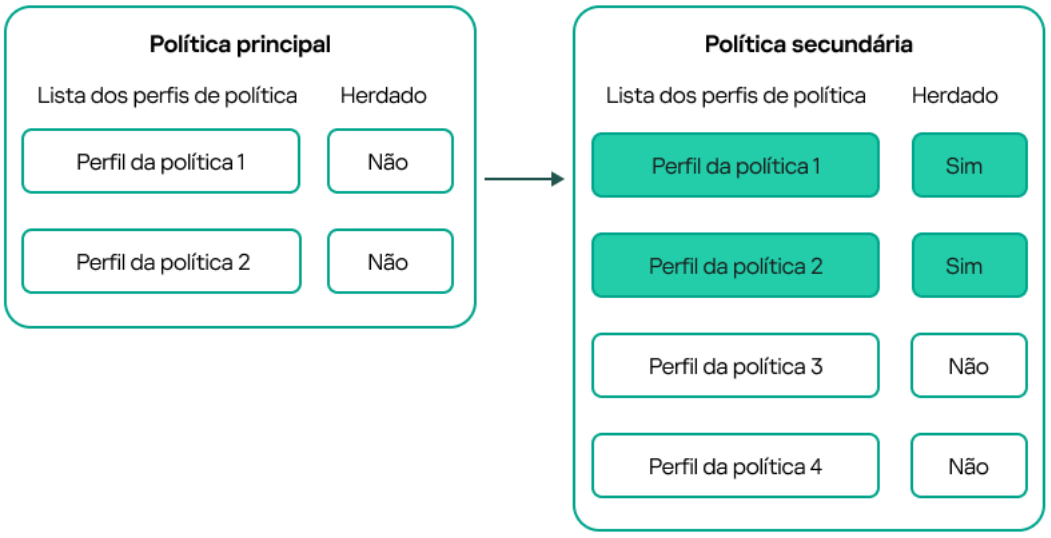


A configuração do dispositivo gerenciado atende às condições de ativação de vários perfis de política

Perfis de política em uma hierarquia de herança

Os perfis de política de diferentes políticas de nível de hierarquia estão em conformidade com as seguintes condições:

- Uma política de nível inferior herda perfis de política de uma política de nível superior. Um perfil de política herdado de uma política de nível superior obtém prioridade mais alta do que o nível do perfil de política original.
- Você não pode alterar a prioridade de um perfil de política herdado (veja a figura abaixo).

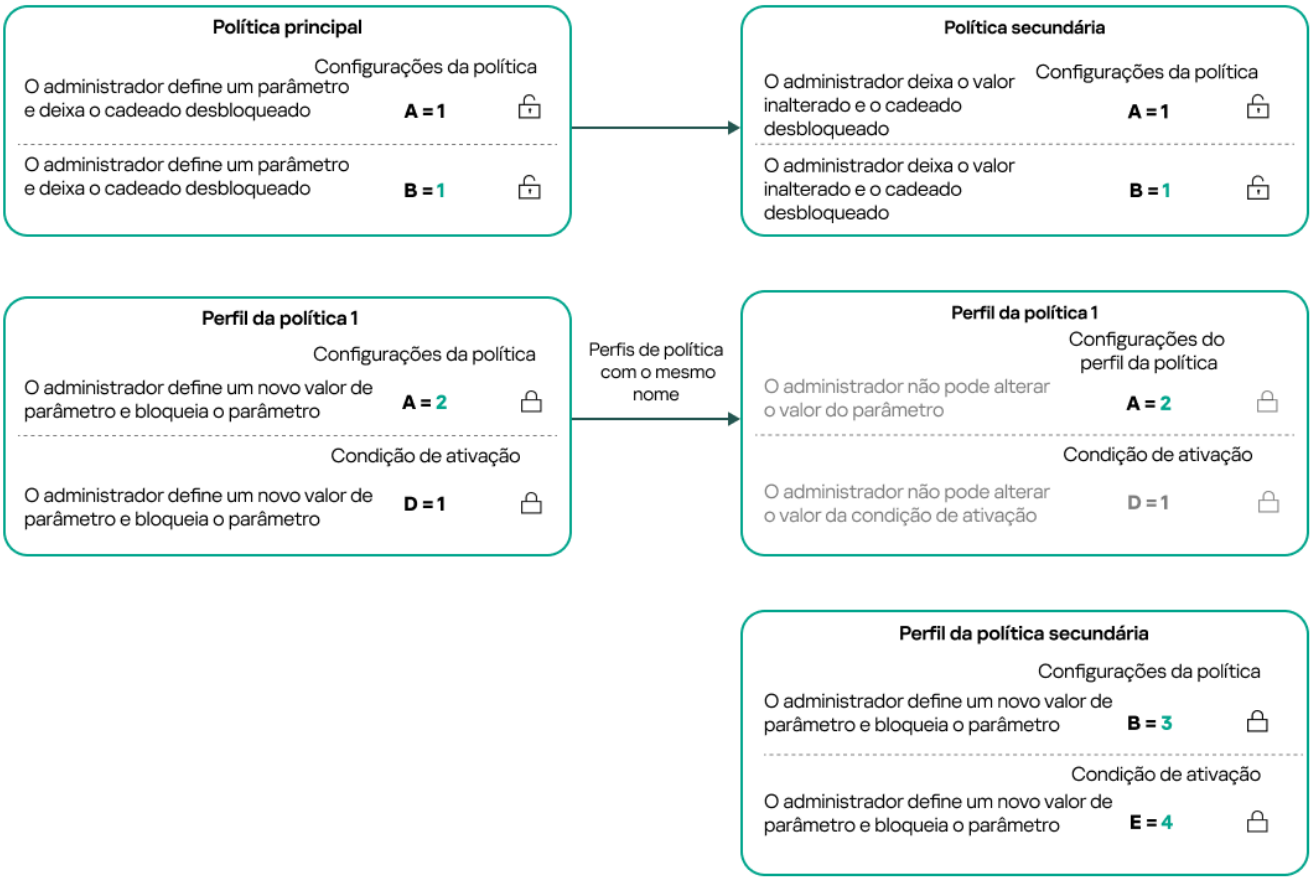


Herança de perfis de política

Perfis de política com o mesmo nome

Se houver duas políticas com o mesmo nome em diferentes níveis de hierarquia, essas funcionarão de acordo com as seguintes regras:

- As configurações bloqueadas e a condição de ativação de perfil de um perfil de política de nível superior alteram as configurações e a condição de ativação de perfil de um perfil de política de nível inferior (ver figura abaixo).



O perfil secundário herda os valores de configuração de um perfil de política principal

- As configurações desbloqueadas e a condição de ativação de perfil de um perfil de política de nível superior não alteram as configurações e a condição de ativação de perfil de um perfil de política de nível inferior.

Como as configurações são implementadas em um dispositivo gerenciado

A implementação eficaz de configurações em um dispositivo gerenciado pode ser descrita da seguinte forma:

- Os valores de todas as configurações não bloqueadas são obtidos a partir da política.
- Em seguida, são substituídos pelos valores das configurações do aplicativo gerenciado.
- Em seguida, os valores das configurações bloqueadas da política em vigor são aplicados. Os valores das configurações bloqueadas alteram os valores das configurações em vigor desbloqueadas.

Gerenciamento de políticas

Esta seção descreve o gerenciamento de políticas e fornece informações sobre como visualizar a lista de políticas, criar, modificar, copiar, mover políticas, sincronização forçada, visualizar o gráfico de status de distribuição de política e excluir uma política.

Visualização da lista de políticas

Você pode visualizar listas de políticas criadas para o Servidor de Administração ou para qualquer grupo de administração.

Para visualizar uma lista de políticas:

1. No menu principal, vá para **Gerenciamento de ativos** → **Hierarquia de grupos**.
2. Na estrutura de grupos de administração, selecione o grupo de administração para o qual você deseja exibir a lista de políticas.

A lista de políticas aparece em formato tabular. Se não houver políticas, a tabela ficará vazia. Você pode mostrar ou ocultar as colunas da tabela, modificar a sua ordem, exibir apenas linhas que contenham um valor especificado ou usar a pesquisa.

Criação de uma nova política

Você pode criar políticas; pode também modificar e excluir as políticas existentes.

Para criar uma política:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.
2. Selecione o grupo de administração para o qual a política deve ser criada:
   - Para o grupo raiz.

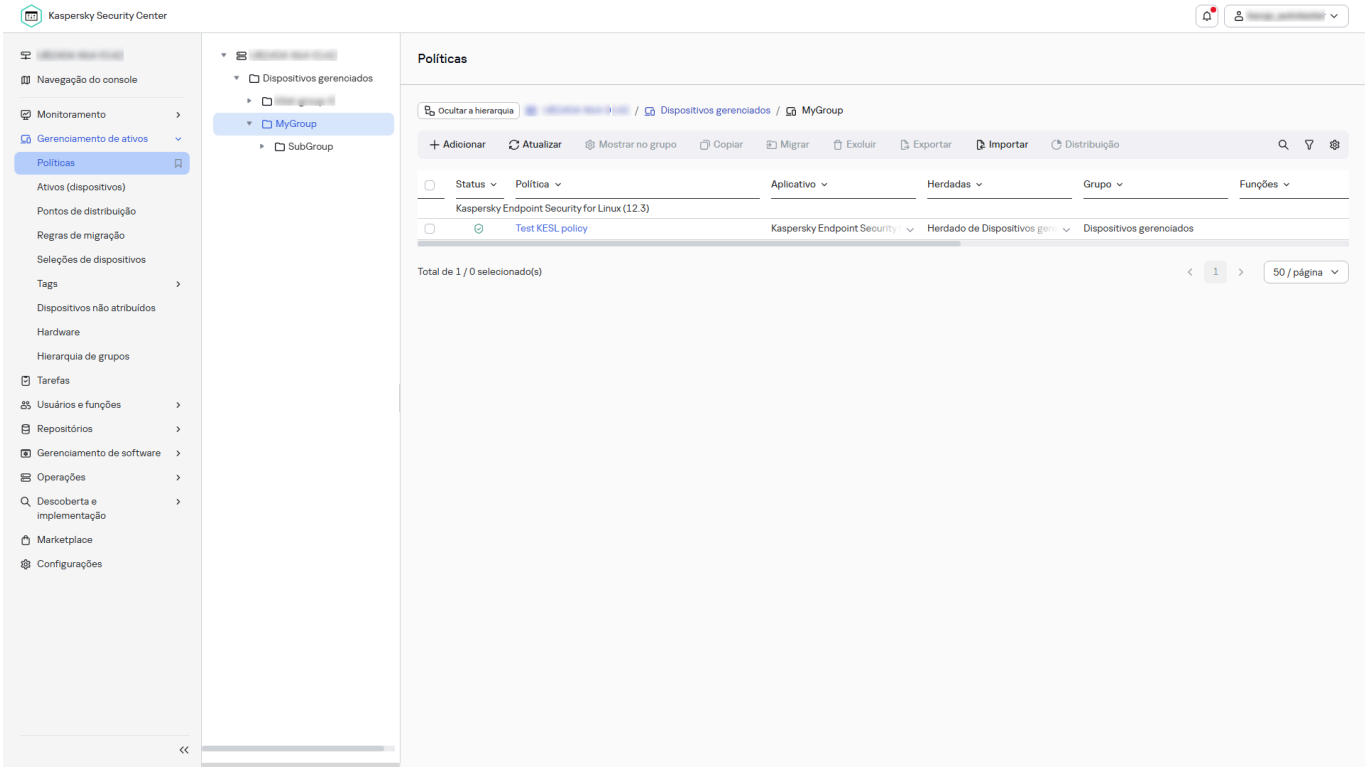
     Neste caso, é necessário prosseguir para a próxima etapa.
   - Para um subgrupo:

     a. Clique no botão **Mostrar a hierarquia** na parte superior da página.

     O nome do botão mudará para **Ocultar a hierarquia**.

     b. Na janela aberta, clicar no nome do subgrupo necessário.

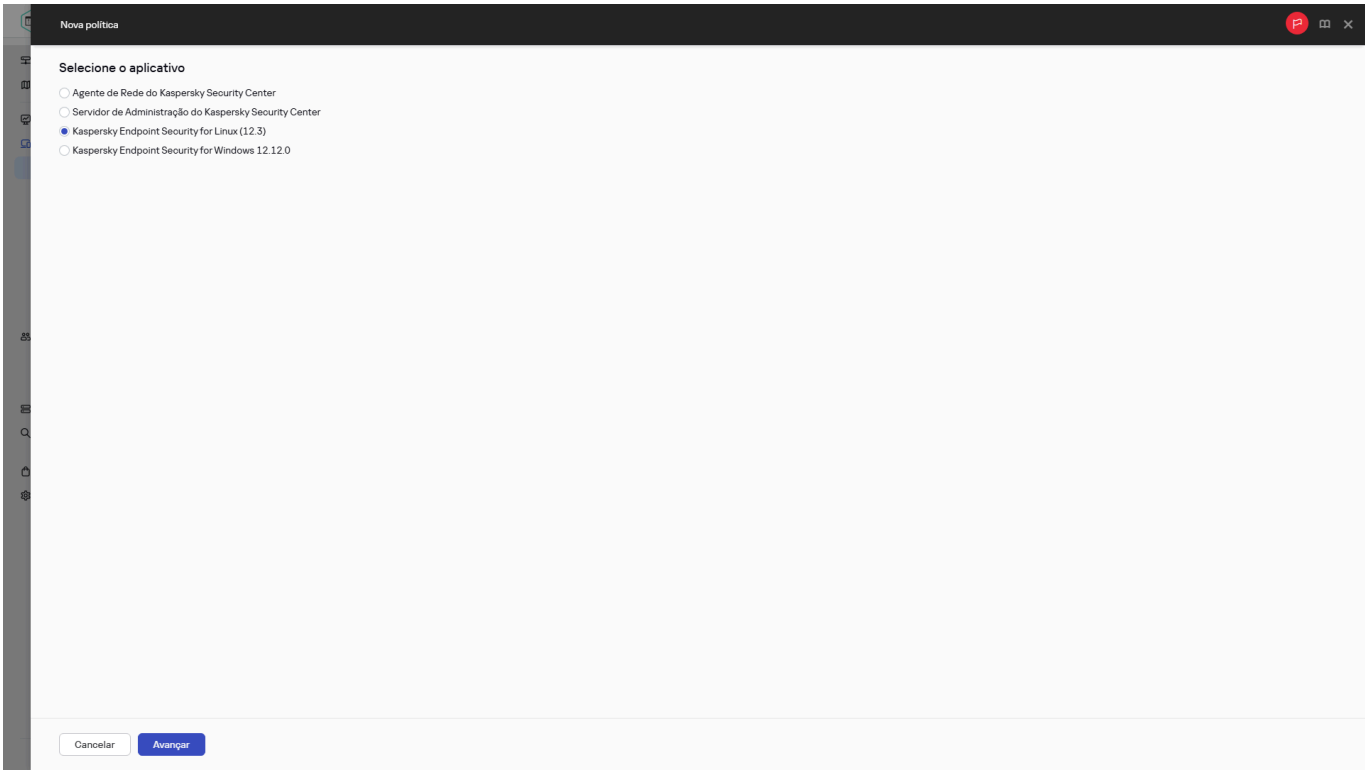
O caminho para o grupo selecionado é exibido na parte superior da página. Caso necessário, é possível clicar em um link com o nome do grupo de administração para ir até o grupo. Por padrão, o último link no caminho fica inativo. Além disso, é possível fechar a janela de hierarquia clicando no botão **Ocultar a hierarquia**.



A lista de políticas

3. Clique em **Adicionar**.

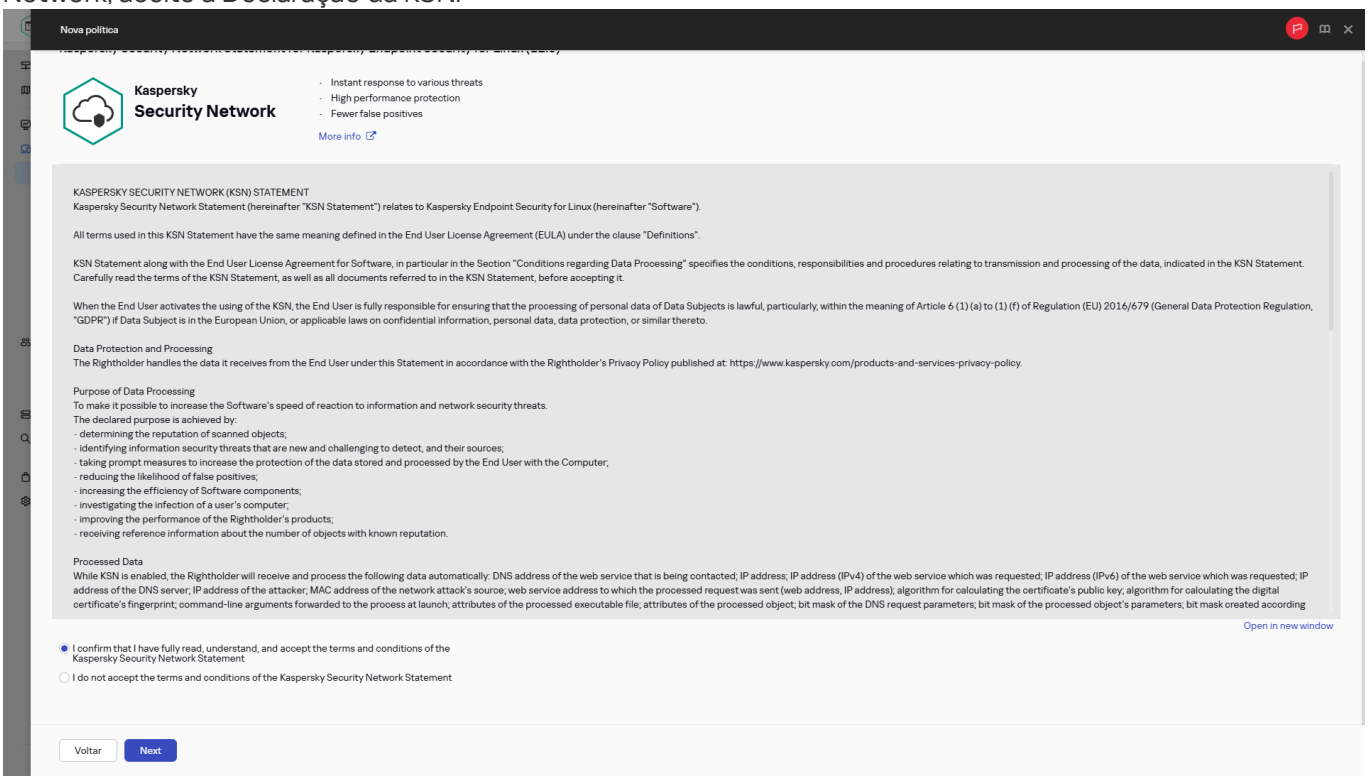
   A janela **Selecione o aplicativo** se abre.



Criação de uma nova política

4. Selecione o aplicativo para o qual você deseja criar uma política.

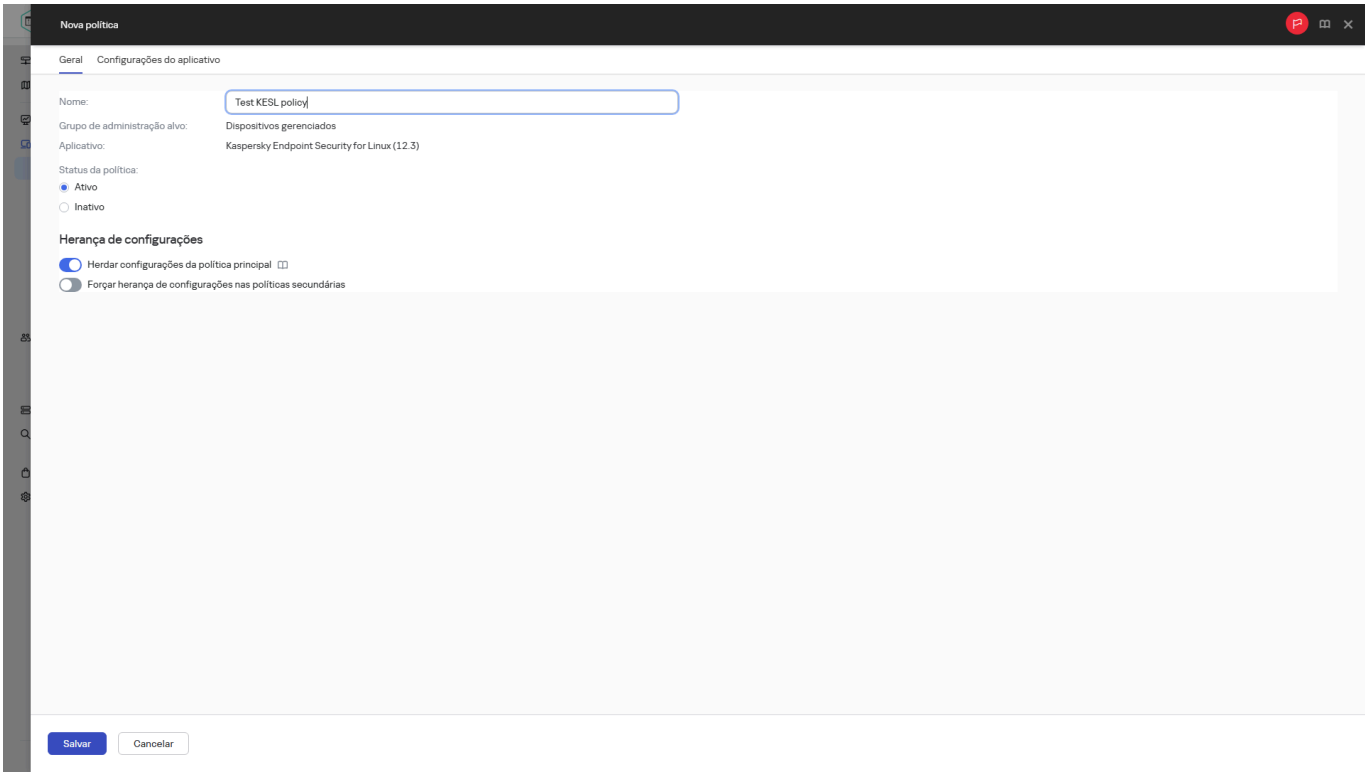
5. Se a Kaspersky Security Network for compatível com o aplicativo da Kaspersky para o qual você está criando uma política, você será solicitado a aceitar a Declaração da KSN. Se você quiser usar a Kaspersky Security Network, aceite a Declaração da KSN.



Aceitação da Declaração da KSN

6. Clique em **Avançar**.

   A nova janela de configurações de política é exibida com a guia **Geral** selecionada. Se quiser, altere o nome padrão, o status padrão e as configurações de herança padrão da política.



A janela de configurações da nova política

7. Selecione a guia **Configurações do aplicativo**.

Ou você pode clicar em **Salvar** e sair. A política aparecerá na lista de políticas, e você poderá editar as suas configurações depois.

8. Na guia **Configurações do aplicativo**, no painel esquerdo, selecione a categoria desejada e, no painel de resultados à direita, edite as configurações da política. Você pode editar as configurações da política em cada categoria (seção).

   O conjunto de configurações depende do aplicativo para o qual você cria uma política. Para mais detalhes, consulte:

   - Configurando o Servidor de Administração
   - Configurações de política do Agente de Rede
   - Ajuda do Kaspersky Endpoint Security for Linux
   - Ajuda do Kaspersky Endpoint Security for Windows

   Para detalhes sobre as configurações de outros aplicativos de segurança, consulte a documentação do aplicativo correspondente.

   Ao editar as configurações, você pode clicar em **Cancelar** para cancelar a última operação.

9. Clique em **Salvar** para salvar a política.

   Uma notificação é exibida com a seguinte mensagem: **A política está sendo salva e distribuída pela hierarquia de Servidores de Administração**.

   Se a política for validada, a seguinte notificação aparecerá: **A política foi salva**.

   Se a validação da política falhar, a seguinte notificação será exibida: **Falha ao salvar e distribuir a política pela hierarquia de Servidores de Administração. Entre em contato com o Suporte Técnico**. Revise as configurações da política e tente novamente. Se o problema persistir, entre em contato com o Suporte Técnico.

A política será exibida na lista de políticas. Depois que a política for criada, os eventos de alteração de política serão exportados para o sistema SIEM se essa opção estiver ativada.

Configurações da política gerais

Geral

Na guia **Geral**, você pode modificar o status da política e especificar a herança das configurações da política:

- No bloco **Status da política**, você poderá selecionar um dos modos de política:

  Ativo

  Se esta opção estiver selecionada, a política é habilitada.

  Por padrão, esta opção está selecionada.

  Fora do escritório

  Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

  Inativo

Se esta opção estiver selecionada, a política é habilitada, mas continua armazenada na pasta **Políticas**. Se necessário, a política pode ser habilitada.

- No grupo de configurações **Herança de configurações**, você pode configurar a herança de política:

  Herdar configurações da política principal

  Se esta opção estiver ativada, os valores das configurações de política são herdados da política de grupo de nível superior e, portanto são bloqueados.

  Por padrão, esta opção está ativada.

  Forçar herança de configurações nas políticas secundárias

  Se esta opção estiver ativada, após a aplicação das alterações da política, as seguintes ações serão realizadas:

  - Os valores das configurações da política serão propagados às políticas de subgrupos de administração, ou seja, às políticas secundárias.
  - No bloco **Herança de configurações** da seção **Geral** na janela Propriedades de cada política secundária, a opção **Herdar configurações da política principal** será automaticamente ativada.

  Se a opção estiver ativada, as configurações das políticas secundárias são bloqueadas.

  Por padrão, esta opção está desativada.

Configuração de eventos

Na guia **Configuração de eventos**, configure o registro e a notificação de eventos. Os eventos são distribuídos por nível de importância nas seguintes guias:

- **Crítico**

  A seção **Crítico** não é exibida nas propriedades de política do Agente de Rede.

- **Falha funcional**
- **Advertência**
- **Informações**

Em cada seção, a lista exibe os tipos de eventos e o prazo de armazenamento de eventos padrão no Servidor de Administração (em dias). Clicar em um tipo de evento permite especificar as seguintes configurações:

- **Registro de eventos**

  Você pode especificar por quantos dias armazenar o evento e selecionar onde armazená-lo:

  - **Exportar para o sistema SIEM usando o Syslog**
  - **Armazenar no log de eventos do SO no dispositivo**
  - **Armazenar no log de eventos do SO no Servidor de Administração**

- **Notificações de eventos**

Você pode selecionar se deseja ser notificado sobre o evento de uma das seguintes formas:

- **Notificar por e-mail**
- **Notificar por SMS**
- **Notificar ao executar o arquivo executável ou o script**
- **Notificar via SNMP**

Por padrão, as configurações de notificação especificadas na guia Propriedades do Servidor de Administração (como endereço do destinatário) são usadas. Se desejar, você pode alterar as configurações na guia **E-mail**, **SMS** e **Arquivo executável a ser executado**.

Além disso, a guia **Configuração de eventos** exibe uma notificação quando um novo tipo de evento é adicionado (por exemplo, em uma nova versão do aplicativo) e possibilita a aplicação de novas configurações clicando-se no botão **Salvar** ou **Salvar e fechar**.

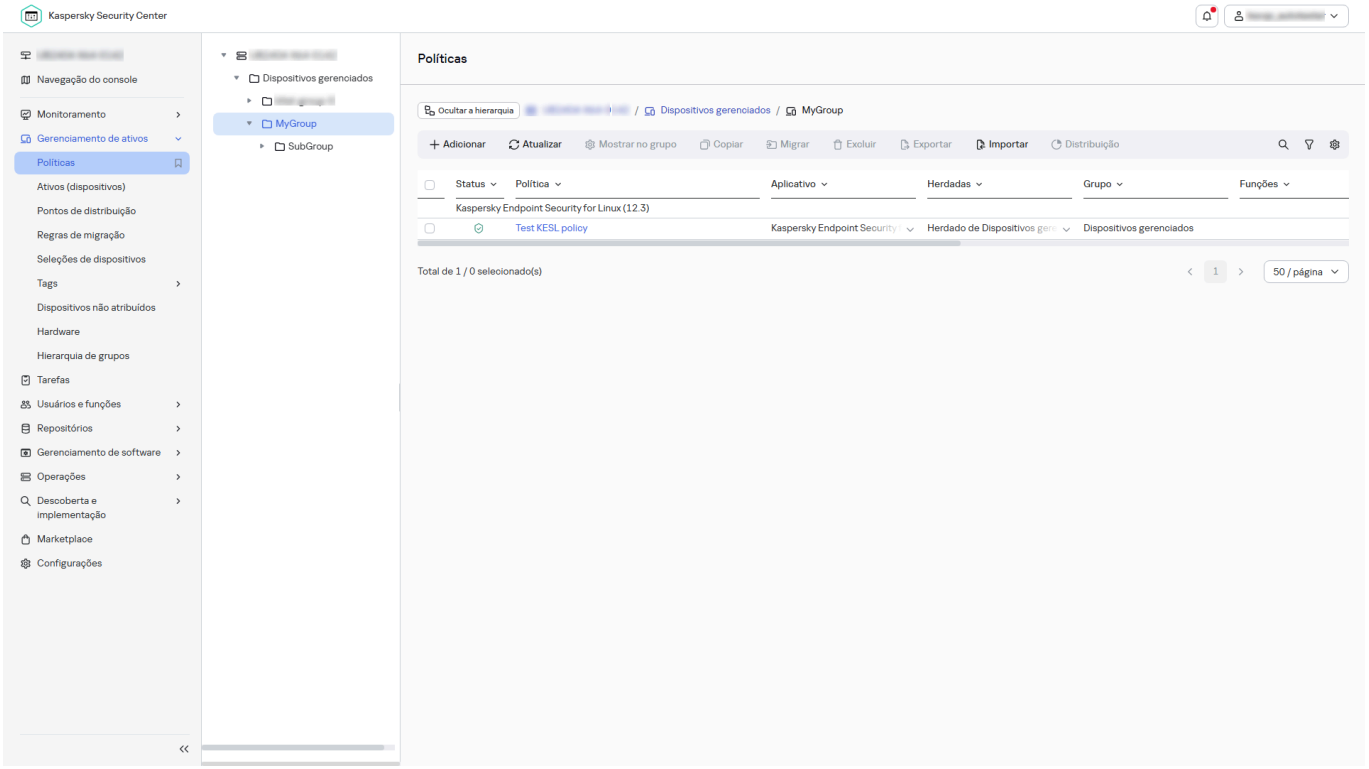
Histórico de revisões

A guia **Histórico de revisões** permite visualizar a lista das revisões da política, comparar as revisões da política e reverter as alterações feitas na política, se necessário.

Modificar uma política

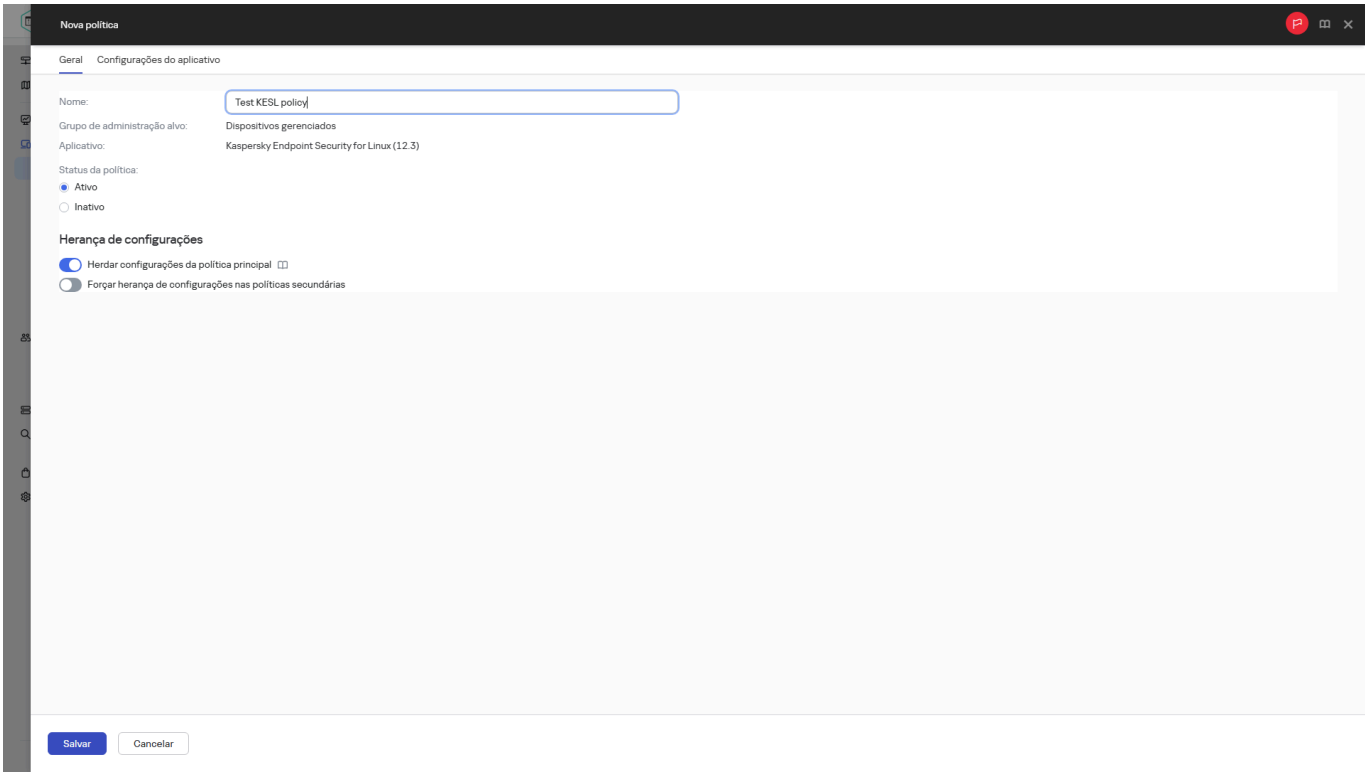
Para modificar uma política:

1. No menu principal, vá para **Gerenciamento de ativos → Políticas**.



2. Clique na política que deseja modificar.

A janela Propriedades da política será aberta.



3. Especifique as configurações gerais e as configurações do aplicativo para o qual a política está sendo criada. Para mais detalhes, consulte:

   - Configurando o Servidor de Administração
   - Configurações de política do Agente de Rede
   - Ajuda do Kaspersky Endpoint Security for Linux
   - Ajuda do Kaspersky Endpoint Security for Windows

   Para detalhes sobre as configurações de outros aplicativos de segurança, consulte a documentação desse aplicativo.

4. Clique no botão **Salvar**.

   Uma notificação é exibida com a seguinte mensagem: **A política está sendo salva e distribuída pela hierarquia de Servidores de Administração**.

   Se a política for validada, a seguinte notificação aparecerá: **A política foi salva**.

   Se a validação da política falhar, a seguinte notificação será exibida: **Falha ao salvar e distribuir a política pela hierarquia de Servidores de Administração. Entre em contato com o Suporte Técnico**. Revise as configurações da política e tente novamente. Se o problema persistir, entre em contato com o Suporte Técnico.

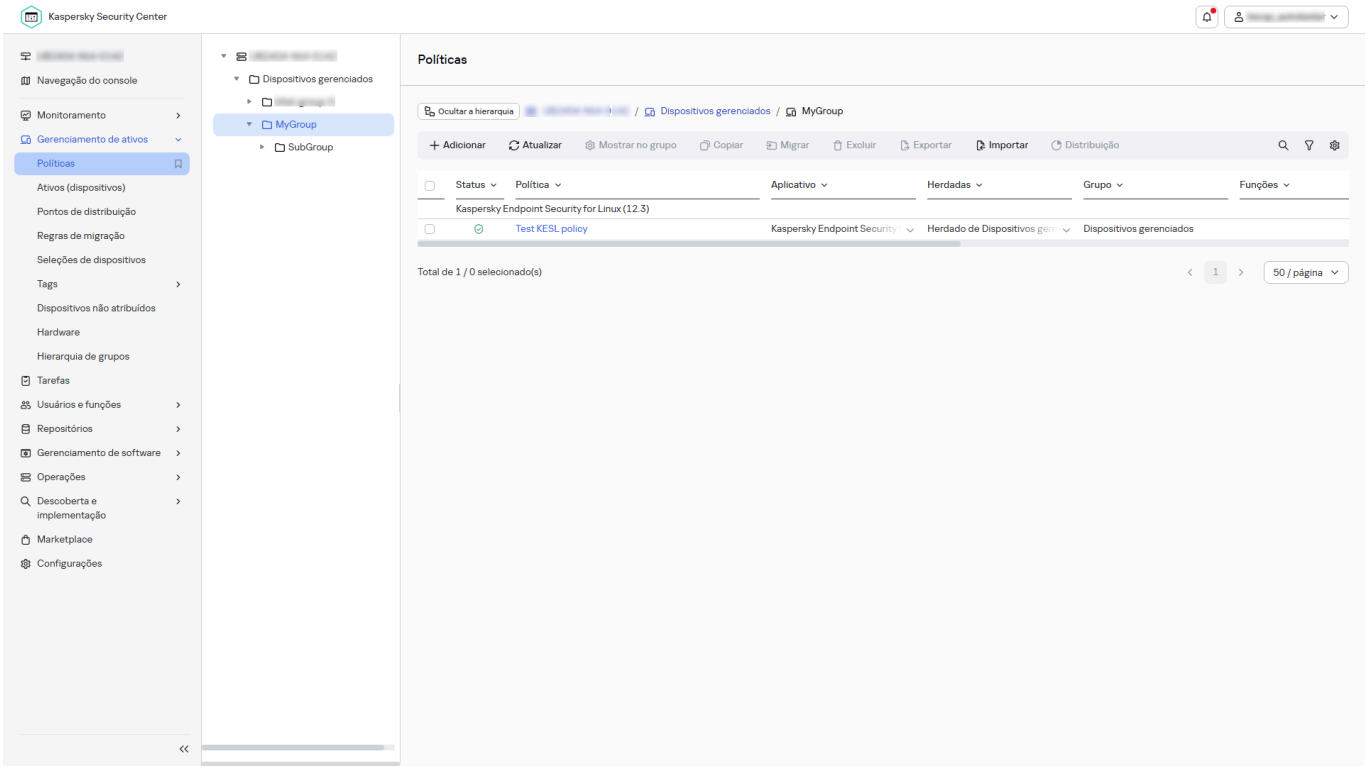
As alterações feitas à política serão salvas nas propriedades da política e aparecerão na seção **Histórico de revisões**. Depois que a política for modificada, os eventos de alteração de política serão exportados para o sistema SIEM se essa opção estiver ativada.

Se necessário, você pode comparar as revisões da política. A opção está disponível para as políticas do Servidor de Administração, Agente de Rede, Kaspersky Endpoint Security for Windows (a partir da versão 14.0 do plug-in da web) e Kaspersky Endpoint Security for Mac (a partir da versão 12.2.1 Patch A do plug-in da web).

Ativando o desativando uma opção de herança de política

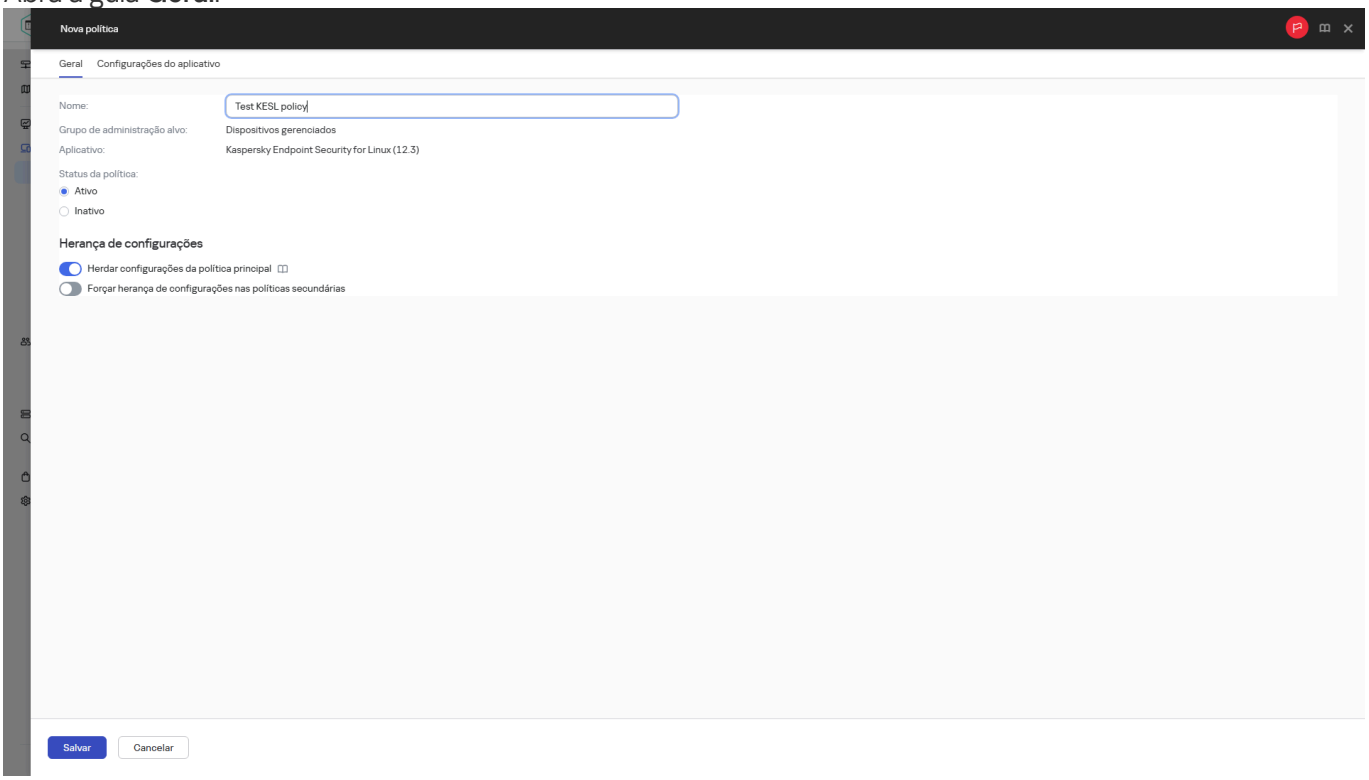
Para ativar ou desativar a opção de herança em uma política:

1. Abra a política necessária.



A lista de políticas

2. Abra a guia **Geral**.



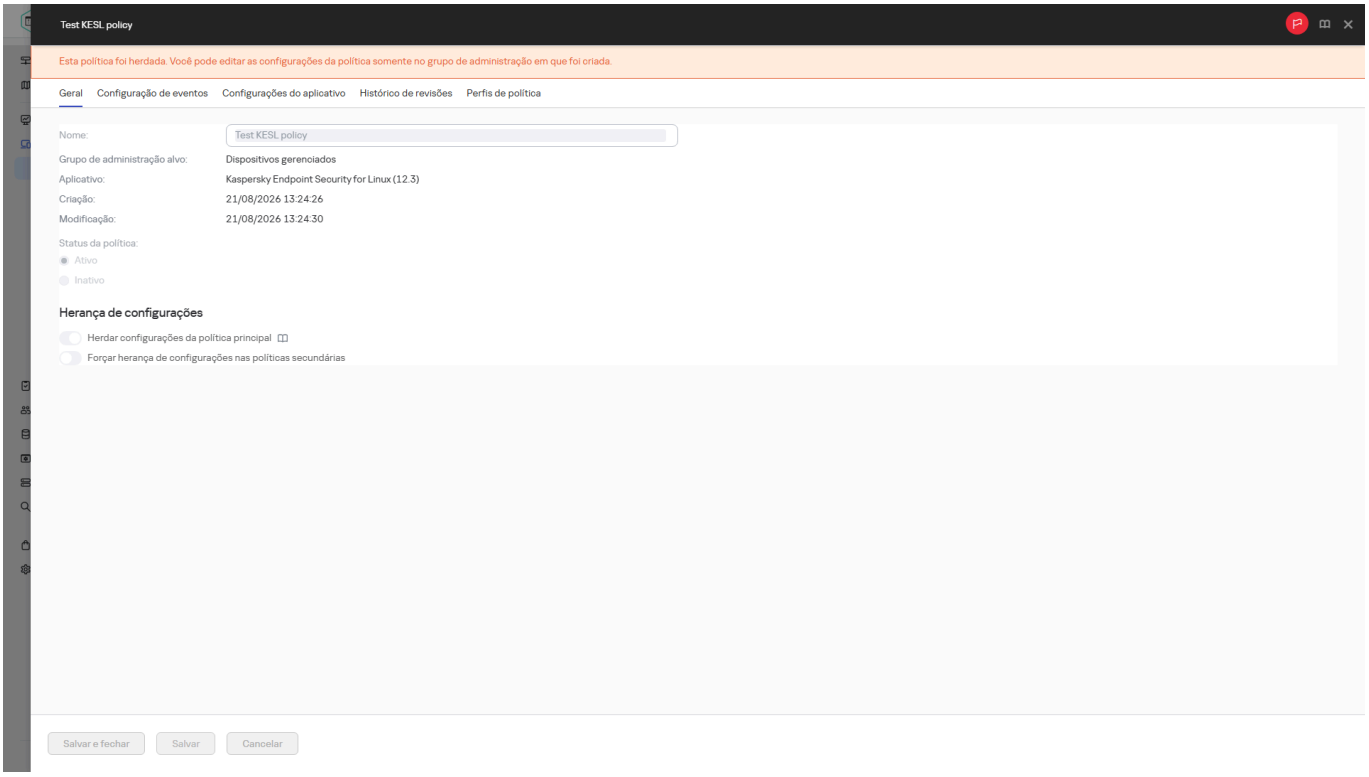
Criação de uma nova política

3. Ative ou desative a herança de política:

- Se você ativar **Herdar configurações da política principal** em uma política secundária e um administrador bloquear algumas configurações na política principal, então você não poderá alterar essas configurações na política do grupo secundário.

- Se você desativar **Herdar configurações da política principal** em uma política secundária, então você poderá alterar todas as configurações na política secundária, mesmo se algumas configurações estiverem bloqueadas na política principal.

- Se você ativar **Forçar herança de configurações nas políticas secundárias** no grupo principal, isso ativará a opção **Herdar configurações da política principal** para cada política secundária. Nesse caso, você não pode desativar esta opção para nenhuma política secundária. Todas as configurações bloqueadas na política principal são herdadas por imposição nos grupos secundários, e você não pode alterar essas configurações nos grupos secundários.



Configurações bloqueadas da política

4. Clique no botão **Salvar** para salvar as alterações ou clique no botão **Cancelar** para rejeitar as alterações.

Por padrão, a opção **Herdar configurações da política principal** está ativada para uma nova política.

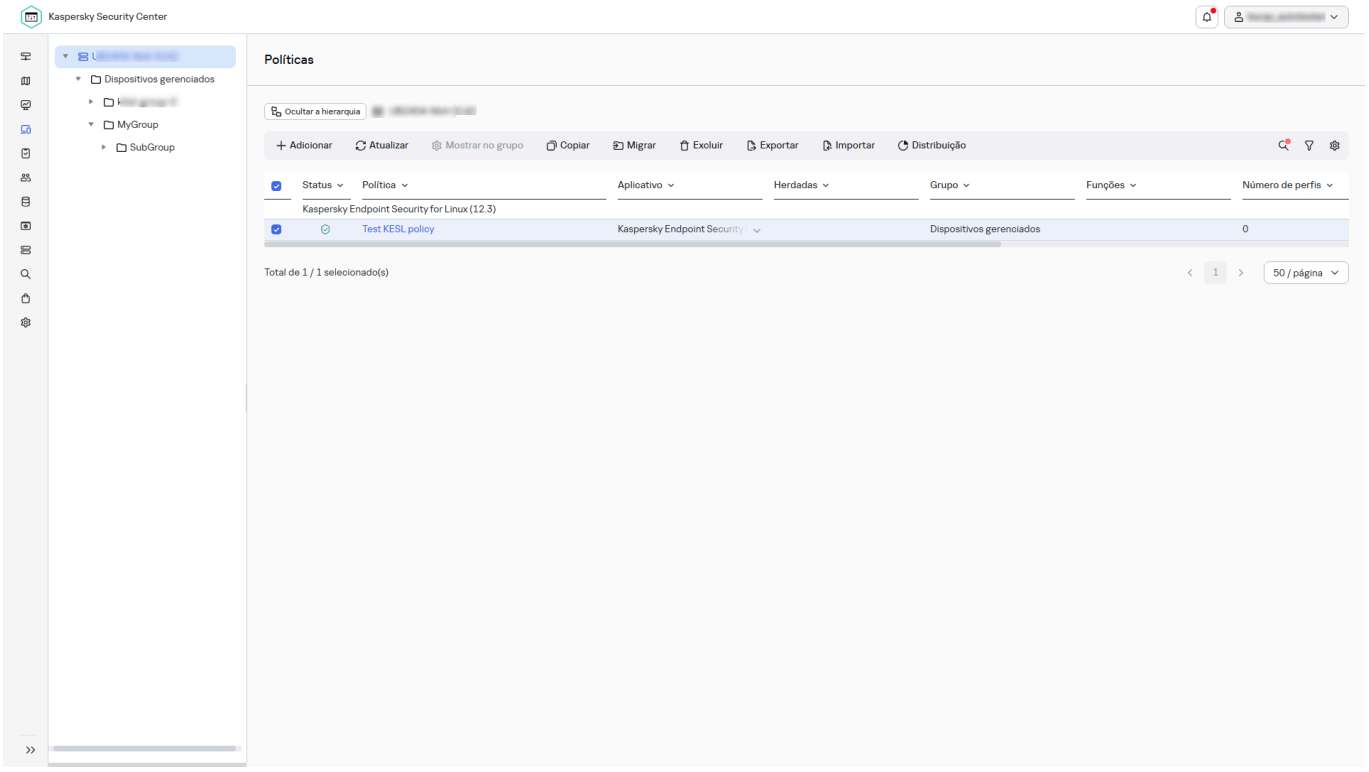
Se uma política tiver perfis, todas as políticas secundárias herdarão esses perfis.

Cópia de uma política

Você pode copiar políticas de um grupo de administração para outro.

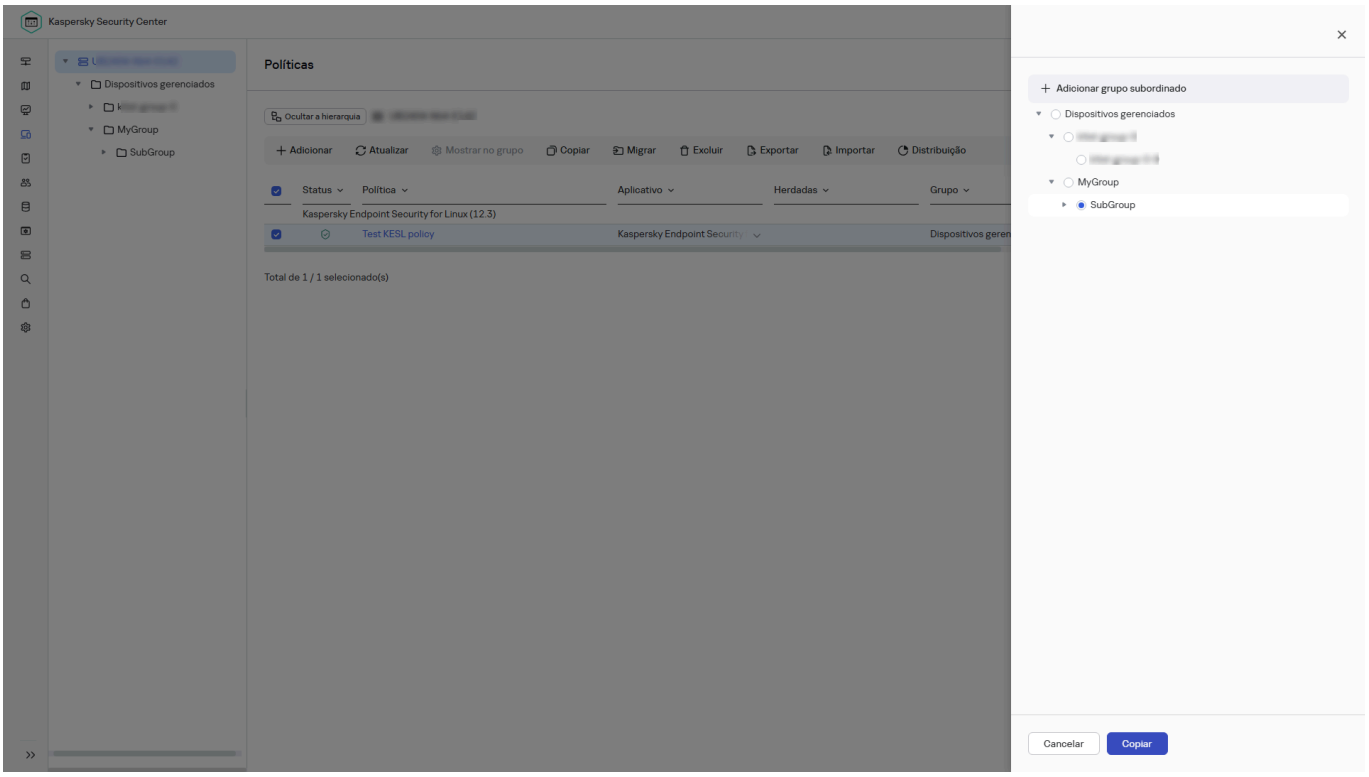
Para copiar uma política para outro grupo de administração:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.
2. Marque a caixa de seleção ao lado da política (ou políticas) que deseja copiar.



3. Clique em **Copiar**.

   No lado direito da tela, a árvore dos grupos de administração aparece.



4. Na árvore, selecione o grupo de destino, isto é, o grupo para o qual deseja copiar a política (ou políticas).

5. Clique no botão **Copiar** na parte inferior da tela.

6. Clique em **OK** para confirmar a operação.

A política (políticas) será copiada para o grupo de destino com todos os seus perfis. O status de cada política copiada no grupo de destino será **Inativo**. Você pode alterar o status para **Ativo** a qualquer momento.

Se uma política com um nome idêntico ao da política recém-movida já existir no grupo de destino, o nome da política recém-movida será expandido com o índice (<próximo número da sequência>), por exemplo: (1).

Mover uma política

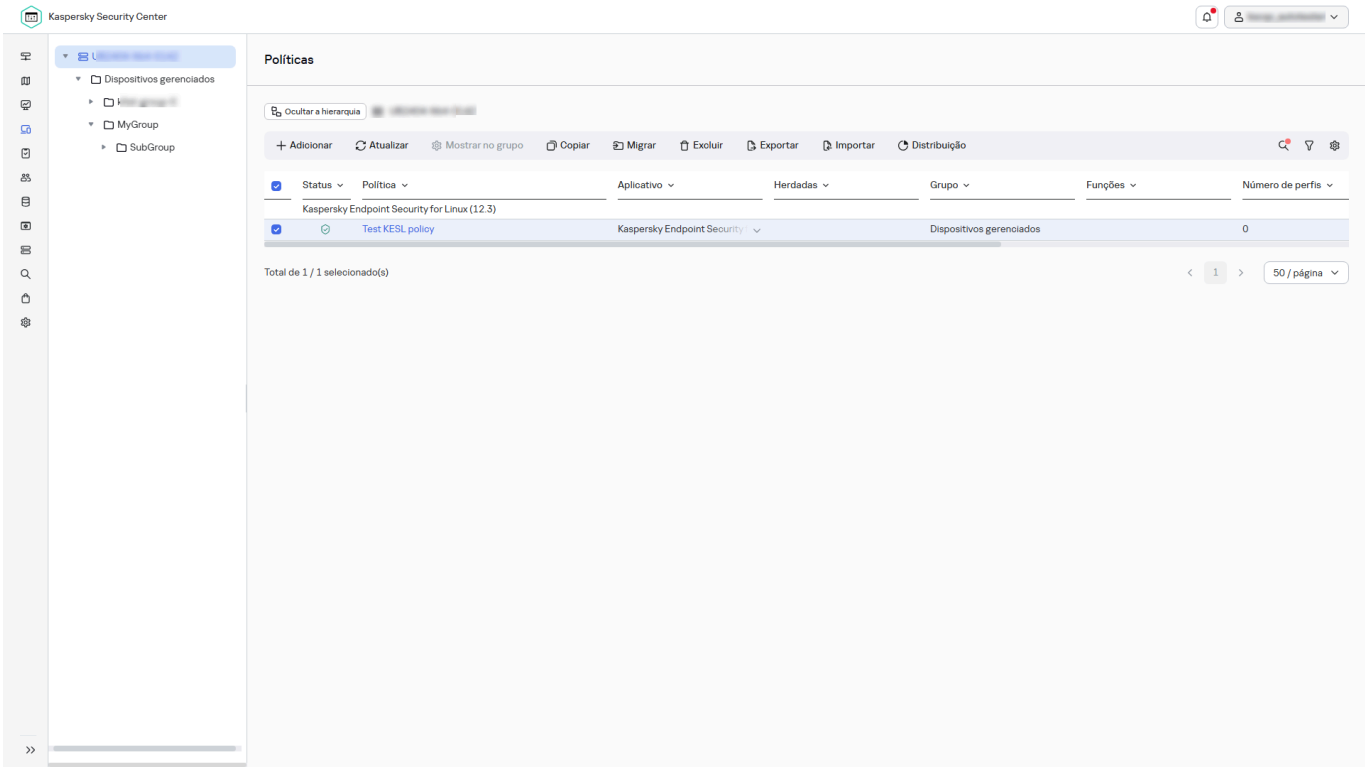
Você pode mover políticas de um grupo de administração para outro. Por exemplo, você quer excluir um grupo, mas deseja usar as políticas dele para outro grupo. Nesse caso, você move a política do grupo antigo para o novo antes de excluir o antigo.

> Ao mover uma política para outro grupo de administração, o histórico de revisões é apagado. A guia **Histórico de revisões** exibe informações somente sobre a alteração mais recente.

Para mover uma política para outro grupo de administração:

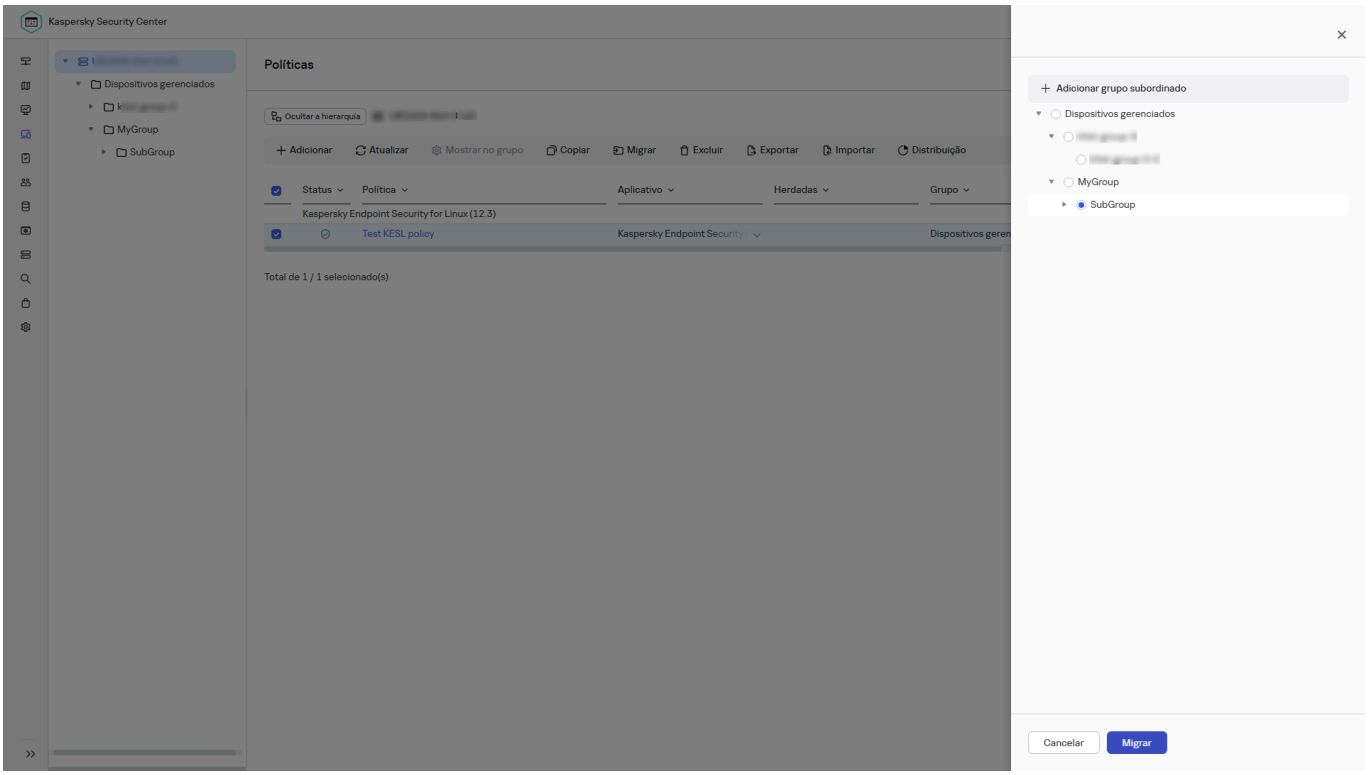
1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.

2. Marque a caixa de seleção ao lado da política (ou políticas) que deseja mover.



3. Clique no botão **Migrar**.

   No lado direito da tela, a árvore dos grupos de administração aparece.



4. Na árvore, selecione o grupo de destino, isto é, o grupo para o qual deseja mover a política (ou políticas).

5. Clique no botão **Migrar** na parte inferior da tela.

6. Clique em **OK** para confirmar a operação.

   Caso uma política não seja herdada do grupo de origem, ela será movida para o grupo de destino com todos os seus perfis. O status da política no grupo de destino é **Inativo**. Você pode alterar o status para **Ativo** a qualquer momento.

   Caso uma política seja herdada do grupo de origem, ela permanecerá no grupo de origem. Ela é copiada para o grupo de destino com todos os seus perfis. O status da política no grupo de destino é **Inativo**. Você pode alterar o status para **Ativo** a qualquer momento.

Se uma política com um nome idêntico ao da política recém-movida já existir no grupo de destino, o nome da política recém-movida será expandido com o índice (<próximo número da sequência>), por exemplo: (1).

Exportação de uma política

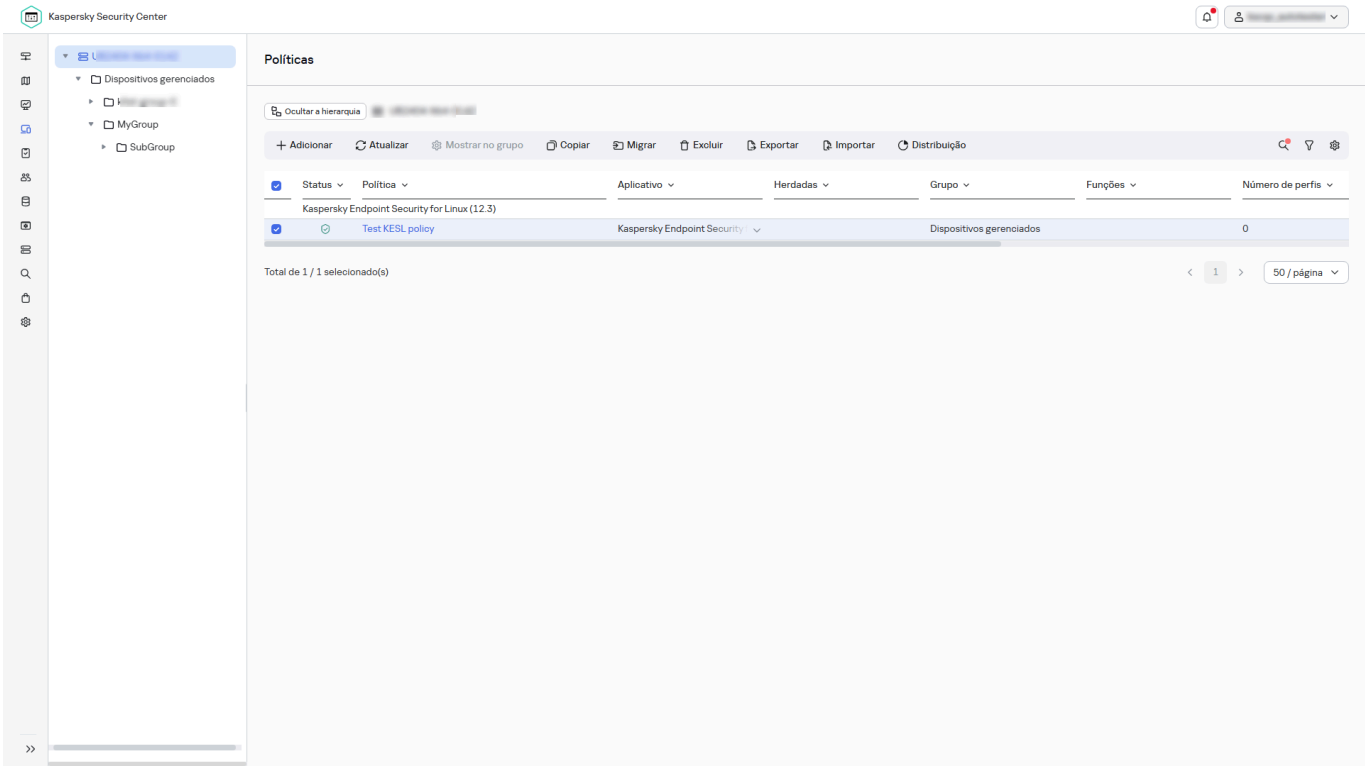
O Kaspersky Security Center Linux permite salvar uma política, suas configurações e os perfis da política em um arquivo KLP. Você pode usar este arquivo KLP para importar a política salva tanto para o Kaspersky Security Center Windows quanto para o Kaspersky Security Center Linux.

Para exportar uma política:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.

2. Marque a caixa de seleção ao lado da política que deseja exportar.

Você não pode exportar várias políticas ao mesmo tempo. Se selecionar mais de uma política, o botão **Exportar** será desabilitado.



Selecione uma política para exportação

3. Clique no botão **Exportar**.
4. Na janela **Salvar como** que abrir, especifique o nome e o caminho do arquivo de política. Clique no botão **Salvar**.

   A janela **Salvar como** é exibida apenas se você usar Google Chrome, Microsoft Edge ou Opera. Caso outro navegador seja usado, o arquivo da política será salvo automaticamente na pasta **Downloads**.

Importação de uma política

O Kaspersky Security Center Linux permite importar uma política de um arquivo KLP. O arquivo KLP contém a política exportada, suas configurações e os perfis da política.

Para importar uma política:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.
2. Clique no botão **Importar**.
3. Clique no botão **Procurar** para escolher um arquivo de política que você deseja importar.
4. Na janela aberta, especifique o caminho para o arquivo de política KLP e clique no botão **Abrir**. Observe que você pode selecionar apenas um arquivo de política.

   O processamento da política é iniciado.
5. Após o processamento com êxito da política, selecione o grupo de administração ao qual deseja aplicar a política.
6. Clique no botão **Concluir** para encerrar a importação da política.

A notificação com os resultados da importação é exibida. Se a política for importada com êxito, você poderá clicar no link **Detalhes** para visualizar as propriedades da política.

Após a importação com êxito, a política será exibida na lista de políticas. As configurações e os perfis da política também são importados. Independentemente do status da política selecionada durante a exportação, a política importada está inativa. Você pode alterar o status da política nas propriedades da política.

Se a política recém-importada tiver um nome idêntico ao de uma política existente, o nome da política importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Sincronização forçada

Embora o Kaspersky Security Center Linux automaticamente sincronize o status, configurações, tarefas e políticas para dispositivos gerenciados, em alguns casos, o administrador precisa saber exatamente, em um dado momento, se a sincronização já foi executada para um dispositivo especificado.

Sincronizar um único dispositivo

Para forçar a sincronização entre o Servidor de Administração e um dispositivo gerenciado:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo que deseja sincronizar com o Servidor de Administração.
   Uma janela de propriedades é exibida com a seção **Geral** selecionada.
3. Clique no botão **Forçar a sincronização**.

O aplicativo sincroniza o dispositivo selecionado com o Servidor de Administração.

Sincronizar vários dispositivos

Para forçar a sincronização entre o Servidor de Administração e vários dispositivos gerenciados:

1. Abra a lista de dispositivos de um grupo de administração ou uma seleção de dispositivos:
   - Execute uma seleção de dispositivos para visualizar a lista de dispositivos.
   - No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados** e selecione o grupo de administração que contém os dispositivos a serem sincronizados:
     - Para o grupo raiz, é possível prosseguir para a próxima etapa.
     - Para um subgrupo, clique no botão **Mostrar a hierarquia** na parte superior da página e, na janela que abrir, clique no nome do subgrupo.

       O caminho para o grupo selecionado é exibido na parte superior da página. Caso necessário, é possível clicar em um link com o nome do grupo de administração para ir até o grupo. Por padrão, o último link no caminho fica inativo. Além disso, é possível fechar a janela de hierarquia clicando no botão **Ocultar a hierarquia**.
2. Marque as caixas de seleção ao lado dos dispositivos que deseja sincronizar com o Servidor de Administração.
3. Acima da lista de dispositivos gerenciados, clique no botão de reticências (...) e, a seguir, clique no botão **Forçar a sincronização**.

   O aplicativo sincroniza os dispositivos selecionados com o Servidor de Administração.
4. Na lista de dispositivos, verifique se a hora da última conexão com o Servidor de Administração foi alterada para os dispositivos selecionados para a hora atual. Se a hora não tiver sido alterada, atualize o conteúdo da página clicando no botão **Atualizar**.

Os dispositivos selecionados são sincronizados com o Servidor de Administração.

Visualização da hora da entrega de uma política

Após alterar uma política de um aplicativo da Kaspersky no Servidor de Administração, o administrador pode verificar se a política alterada foi entregue a um dispositivo gerenciado específico. Uma política pode ser entregue durante uma sincronização normal ou uma sincronização forçada.

Para visualizar a data e a hora que uma política de aplicativo foi fornecida a um dispositivo gerenciado:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo que deseja sincronizar com o Servidor de Administração.

   Uma janela de propriedades é exibida com a seção **Geral** selecionada.
3. Clique na guia **Aplicativos**.
4. Selecione o aplicativo do qual do qual deseja visualizar a data de sincronização da política.

   A janela de política do aplicativo é exibida com a seção **Geral** selecionada e a data e a hora de entrega da política exibidas.

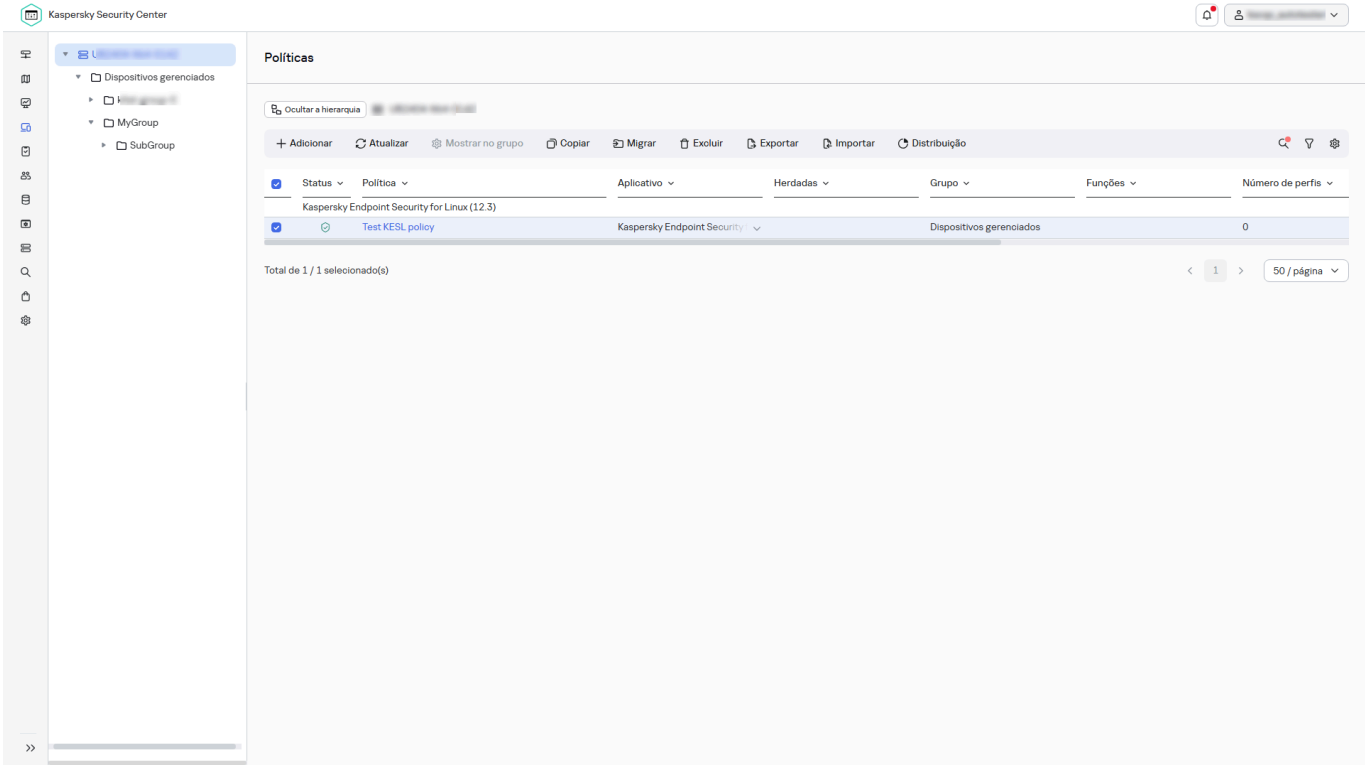
Visualizar o gráfico de status de distribuição da política

No Kaspersky Security Center Linux, é possível visualizar o status de aplicação da política em cada dispositivo por meio de um gráfico de status de distribuição de política.

Para analisar o status de distribuição da política em cada dispositivo:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.

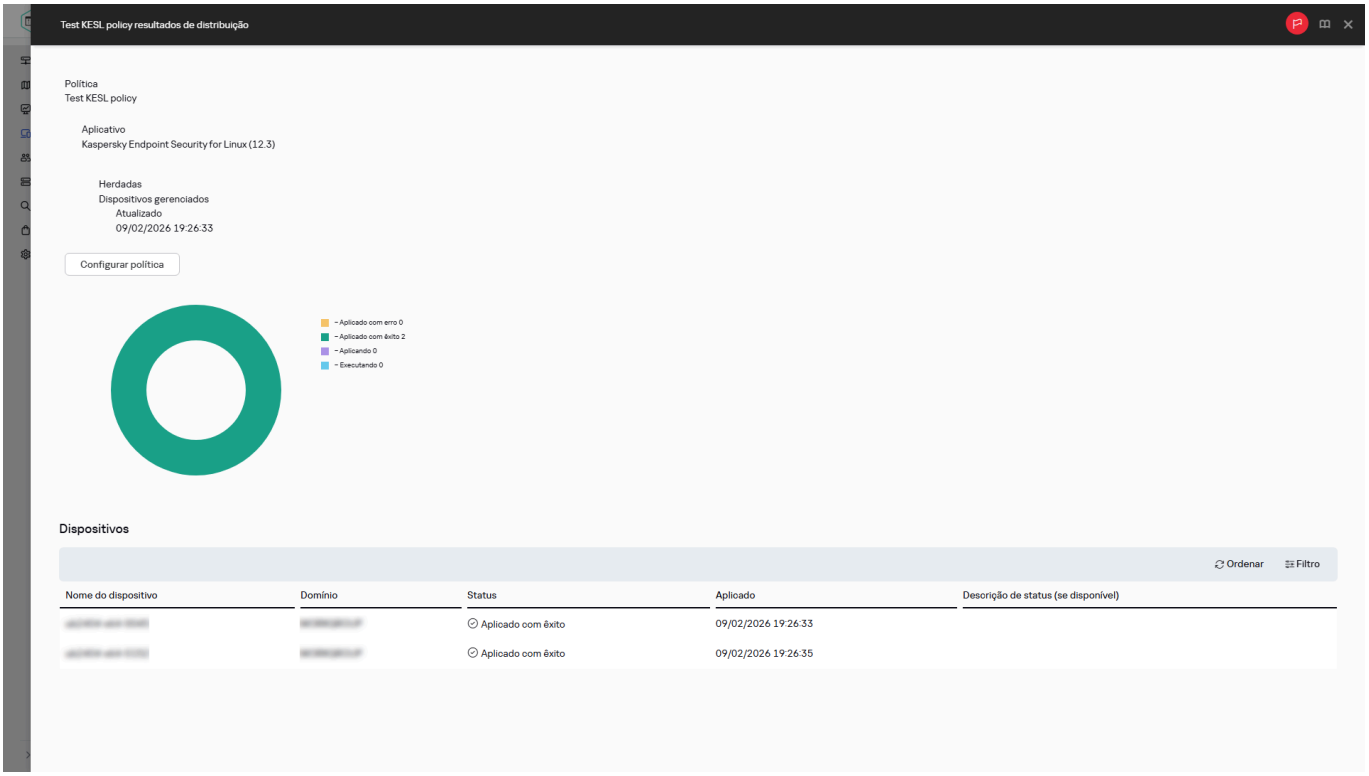
2. Marque a caixa de seleção ao lado da política para a qual deseja visualizar o status de distribuição nos dispositivos.



A lista de políticas

3. No menu exibido, selecione o link **Distribuição**.

A janela **Resultados de distribuição <Nome da política>** é aberta.



Os resultados da distribuição da política

4. Na janela aberta **Distribuição de resultados <Nome da política>** a **descrição do status** da política é exibida.

É possível alterar o número de resultados exibidos na lista com a distribuição da política. O número máximo de dispositivos é 100.000.

Para alterar o número de dispositivos exibidos na lista com os resultados de distribuição da política:

1. No menu principal, vá para **Configurações → Opções da interface**.
2. Em **Limite de dispositivos exibidos nos resultados da distribuição de políticas**, insira o número de dispositivos (até 100 mil).

   Por padrão, o número é 5.000.
3. Clique no botão **Salvar**.

   As configurações são salvas e aplicadas.

Ativação automática de uma política no evento Ataque de vírus

Para fazer com que uma política execute a ativação automática no evento de um ataque de vírus:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.
2. Selecione a seção **Surto de vírus**.
3. No painel direito, clique no link **Configurar as políticas para ativar em caso de um evento de surto de vírus**.

   A janela **Ativação da política** se abre.

4. Na seção relacionada ao componente que detecta um surto de vírus, Antivírus para estações de trabalho e servidores de arquivos, Antivírus para servidores de e-mail ou Antivírus para defesa de perímetro, selecione o botão de opção ao lado da entrada desejada e clique em **Adicionar**.

   Uma janela é aberta com o grupo de administração de **Dispositivos gerenciados**.

5. Clique no ícone do separador (>) ao lado de **Dispositivos gerenciados**.

   Uma hierarquia de grupos de administração e suas políticas é exibida.

6. Na hierarquia de grupos de administração e suas políticas, clique no nome de uma política ou políticas que são ativadas quando um surto de vírus é detectado.

   Para selecionar todas as políticas na lista ou em um grupo, marque a caixa de seleção ao lado do nome desejado.

7. Clique no botão **Salvar**.

   A janela com a hierarquia dos grupos de administração e suas políticas é fechada.

As políticas selecionadas são adicionadas à lista de políticas que são ativadas quando um surto de vírus é detectado. As políticas selecionadas são ativadas no surto de vírus, independentemente de estarem ativas ou inativas.

Se uma política tiver sido ativada no evento Ataque de vírus, você somente pode voltar à política anterior usando o modo manual.

Exclusão de uma política

Você pode excluir uma política se não precisar mais dela. Você pode excluir apenas uma política que não é herdada no grupo de administração especificado. Se uma política for herdada, você só poderá exclui-la no grupo de nível superior para o qual ela foi criada.

Para excluir uma política:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.

2. Marque a caixa de seleção ao lado da política que deseja excluir e clique em **Excluir**.

   O botão **Excluir** ficará indisponível (esmaecido) se você selecionar uma política herdada.

3. Clique em **OK** para confirmar a operação.

A política é excluída em conjunto com todos os seus perfis. Depois que a política for excluída, os eventos de alteração de política serão exportados para o sistema SIEM se essa opção estiver ativada.

Gerenciando perfis de política

Esta seção descreve o gerenciamento de perfis de política e fornece informações sobre como visualizar, alterar a prioridade, criar, copiar, criar uma regra de ativação, excluir, exportar e importar perfis de política.

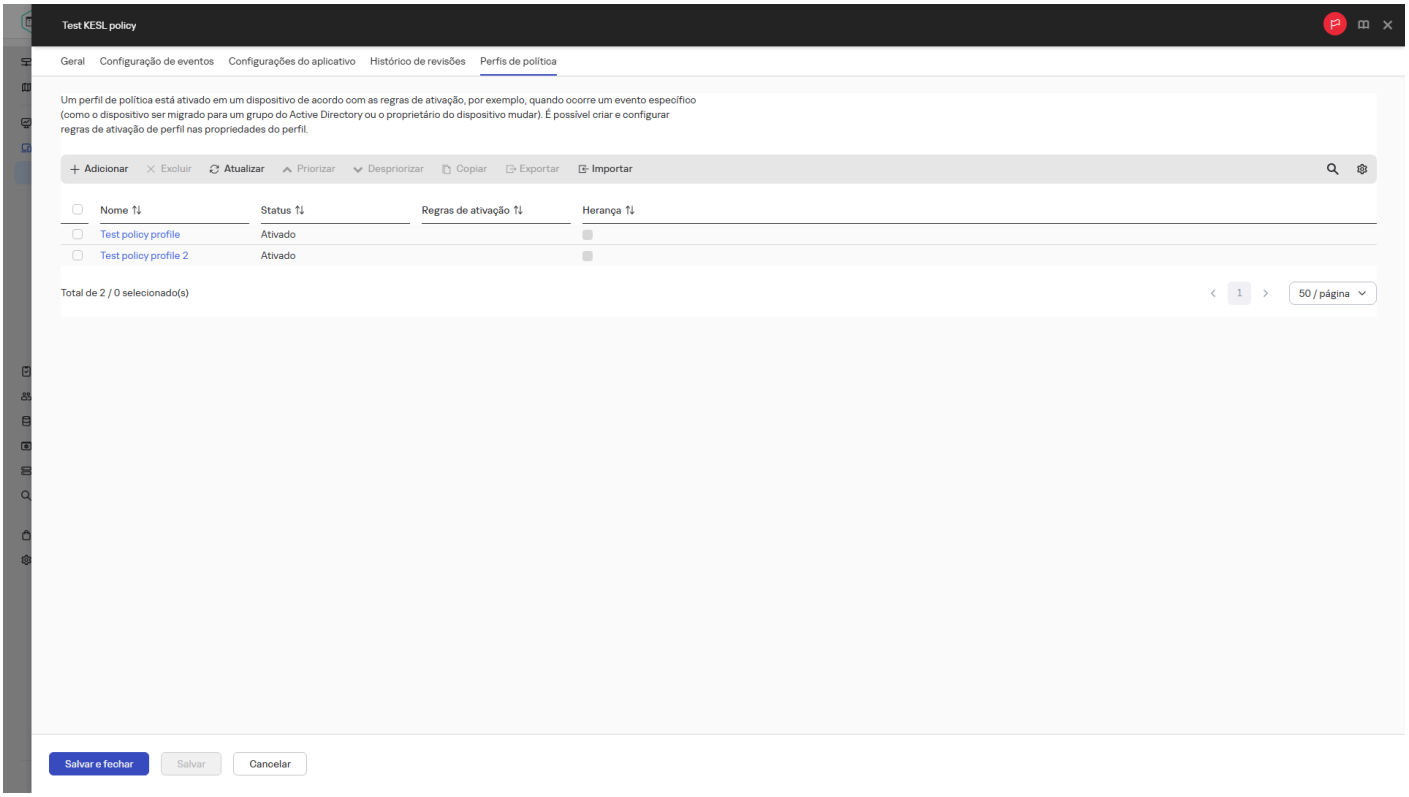
Visualização dos perfis de uma política

Para visualizar os perfis de uma política:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política cujos perfis deseja exibir.

   A janela de propriedades da política é exibida com a guia **Geral** selecionada.
3. Abra a guia **Perfis de política**.

A lista de perfis da política é exibida em formato tabular. Se a política não tiver perfis, uma tabela vazia será exibida.



A lista de perfis de política

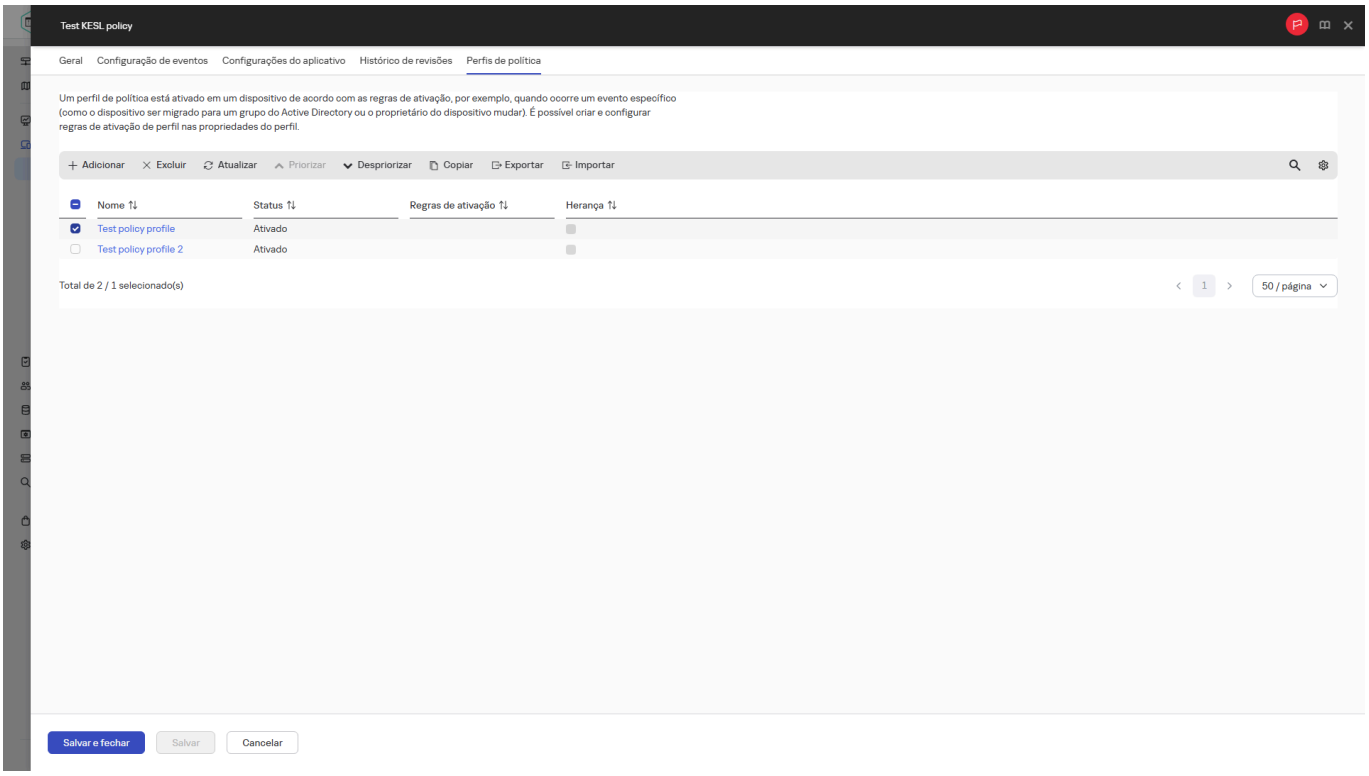
Alteração de uma prioridade de perfil da política

Para alterar uma prioridade de perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.
2. Na guia **Perfis de política**, marque a caixa de seleção ao lado do perfil da política para o qual deseja alterar a prioridade.
3. Defina uma nova posição do perfil da política na lista clicando em **Priorizar** ou **Despriorizar**.

   Quanto mais alto um perfil da política estiver localizado na lista, mais alta será sua prioridade.



4. Clique no botão **Salvar**.

   A prioridade do perfil da política selecionado é alterada e aplicada.

Criar um perfil da política

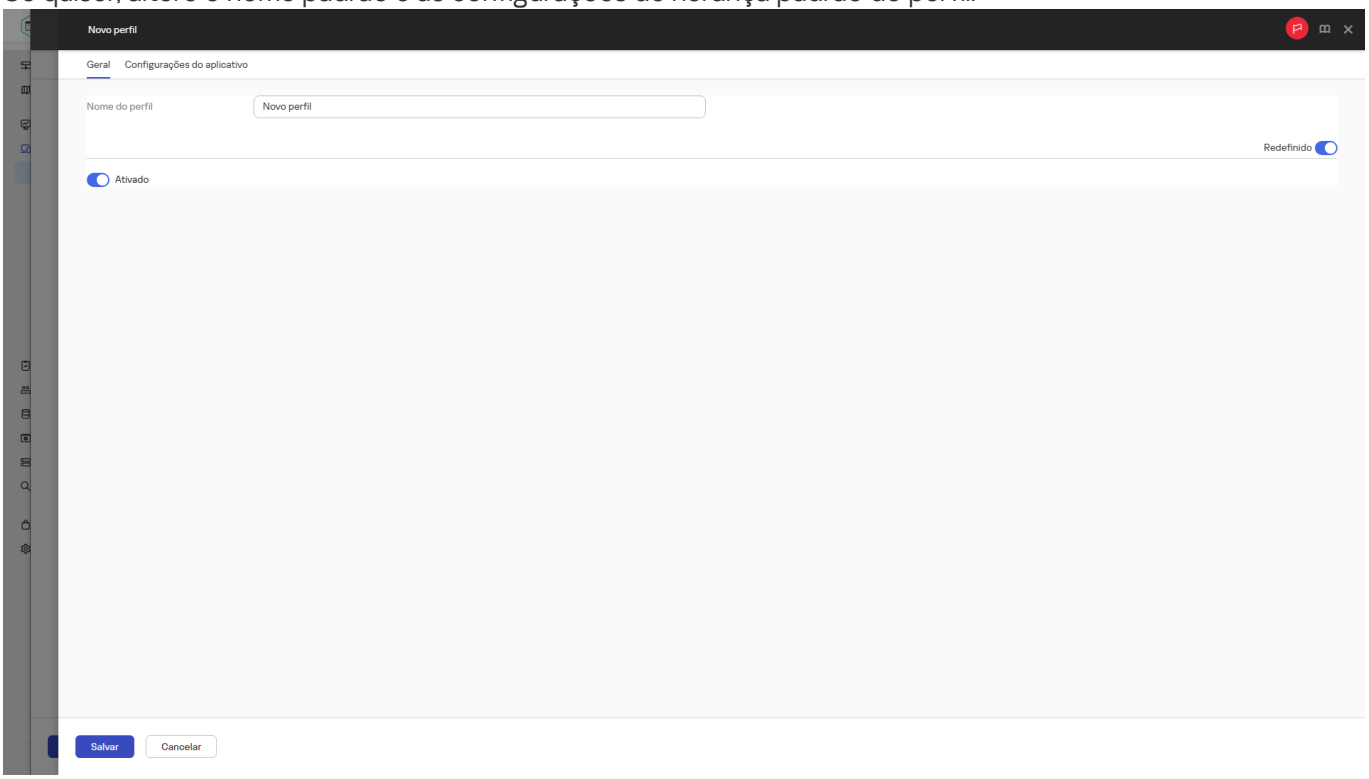
Para criar um perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida. Se a política não tiver perfis, uma tabela vazia será exibida.

2. Clique em **Adicionar**.

3. Se quiser, altere o nome padrão e as configurações de herança padrão do perfil.



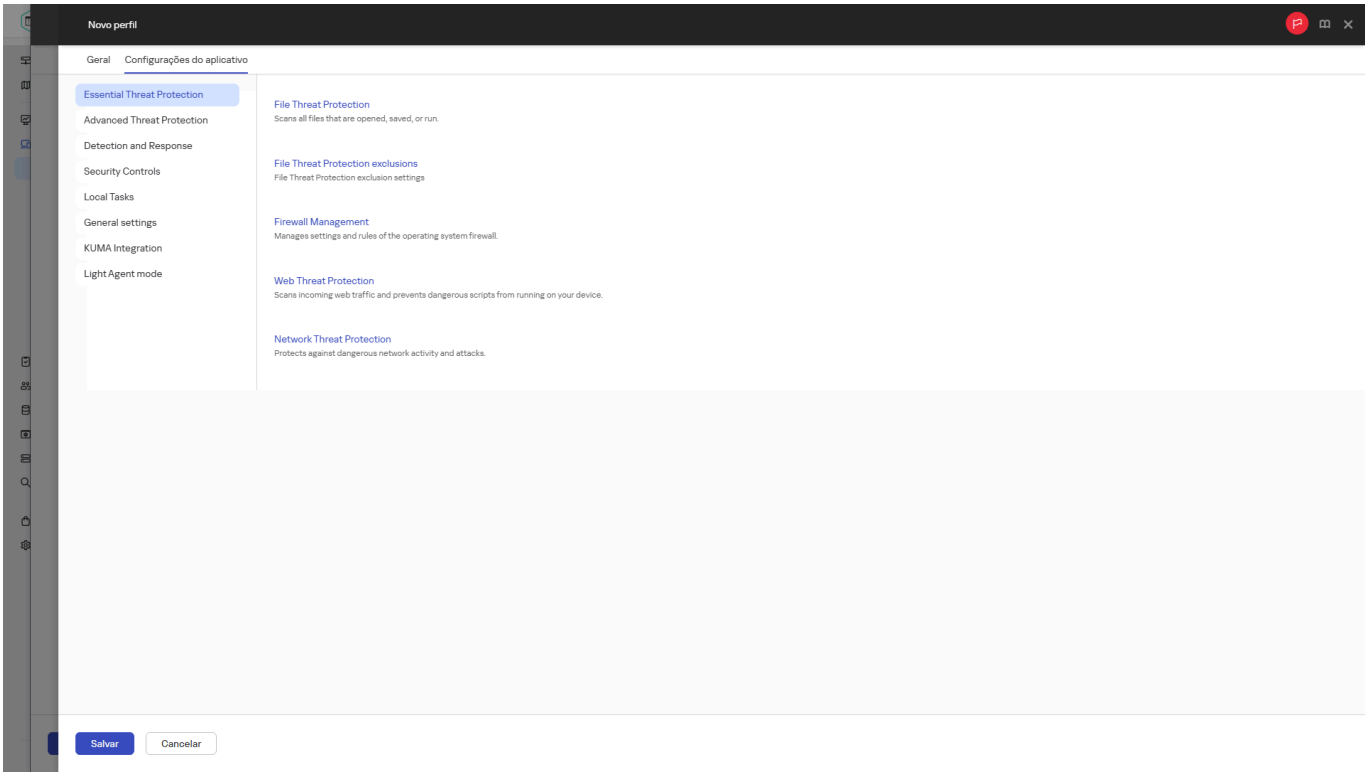
Criar um perfil da política

4. Selecione a guia **Configurações do aplicativo**.

   Ou então, é possível clicar em **Salvar** e sair. O perfil criado aparecerá na lista de perfis da política, e será possível editar as suas configurações depois.

5. Na guia **Configurações do aplicativo**, no painel esquerdo, selecione a categoria desejada e, no painel de resultados à direita, edite as configurações do perfil. Você pode editar as configurações do perfil da política em cada categoria (seção).

Ao editar as configurações, você pode clicar em **Cancelar** para cancelar a última operação.



Especificação das configurações do perfil de política

6. Clique em **Salvar** para salvar o perfil.

O perfil aparecerá na lista de perfis da política.

Copiar um perfil de política

Você pode copiar um perfil da política para política atual ou outra, por exemplo, se quiser ter perfis idênticos para políticas diferentes. Você também pode usar a cópia se quiser ter dois ou mais perfis que se diferenciam em apenas um pequeno número de configurações.

Para copiar um perfil de política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida. Se a política não tiver perfis, uma tabela vazia será exibida.

2. Na guia **Perfis de política**, selecione o perfil da política que deseja copiar.

3. Clique em **Copiar**.

4. Na janela exibida, selecione a política para a qual deseja copiar o perfil.

   É possível copiar um perfil da política para a mesma política ou uma política que você especificar.

5. Clique em **Copiar**.

O perfil da política é copiado para a política que você selecionou. O perfil recentemente copiado adquire a prioridade mais baixa. Se você copiar o perfil para a mesma política, o nome do perfil recentemente copiado será expandido com o índice (), por exemplo: (1), (2).

Você pode alterar posteriormente as configurações do perfil da política, incluindo o nome e a prioridade. Nesse caso, o perfil da política original não é alterado.

Criar uma regra de ativação do perfil da política

Para criar uma regra de ativação do perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.

2. Na guia **Perfis de política**, clique no perfil da política para o qual é preciso criar uma regra de ativação.

   Se a lista de perfis da política estiver vazia, você pode criar um perfil da política.

3. Na guia **Regras de ativação**, clique no botão **Adicionar**.

   A janela com as regras de ativação do perfil da política é aberta.

4. Especifique um nome para a regra.

5. Selecione as caixas junto as condições que devem afetar a ativação do perfil da política que você estiver criando:

   Regras gerais para a ativação do perfil de política

   Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo do status do modo offline de dispositivo, a regra para a conexão ao Servidor de Administração e as tags atribuídas ao dispositivo.

   Para esta opção, especifique na etapa seguinte:

   Status do dispositivo

   Define a condição da presença do dispositivo na rede:

   - **Online** – O dispositivo está na rede, portanto o Servidor de Administração está disponível.
   - **Offline** – O dispositivo está em uma rede externa, o que significa que o Servidor de Administração não está disponível.
   - **N/A** – O critério não será aplicado.

   Localização da rede do dispositivo

   Escolha a condição de ativação do perfil da política (se a regra está ou não sendo executada) e selecione o nome da regra.

   A regra define o local de rede do dispositivo para conexão ao Servidor de Administração, cujas condições devem ser atendidas (ou não devem ser atendidas) para a ativação do perfil da política.

   Uma descrição da localização da rede de dispositivos para conexão a um Servidor de Administração pode ser criada ou configurada em uma regra de troca de Agente de Rede.

   - **Regras para o proprietário do dispositivo específico**

     Para esta opção, especifique na etapa seguinte:

     Proprietário do dispositivo

Ative esta opção para configurar e ativar a regra para a ativação do perfil no dispositivo para seu proprietário. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

- O dispositivo pertence ao proprietário especificado (sinal "=").
- O dispositivo não pertence ao proprietário especificado (sinal "#").

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o proprietário do dispositivo se a opção estiver ativada. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

O proprietário do dispositivo está incluído em um grupo de segurança interno

Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pela associação do proprietário em um grupo de segurança interna do Kaspersky Security Center Linux. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

- O proprietário do dispositivo é um membro do grupo de segurança especificado (sinal "=").
- O proprietário do dispositivo não é um membro do grupo de segurança especificado (sinal "#").

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar um grupo de segurança do Kaspersky Security Center Linux. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **Regras para especificações de hardware**

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo do volume de memória e do número de processadores lógicos.

  Para esta opção, especifique na etapa seguinte:

  Tamanho da RAM, em MB

  Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pelo volume de RAM disponível naquele dispositivo. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

  - O tamanho da RAM do dispositivo é menos do que o valor especificado (sinal "<").
  - O tamanho de RAM de dispositivo é maior do que o valor especificado (sinal ">").

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o volume da RAM no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

  Número de processadores lógicos

  Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pelo número de processadores lógicos nesse dispositivo. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

  - O número de processadores lógicos no dispositivo é menor do que ou igual ao valor especificado (sinal "<").
  - O número de processadores lógicos no dispositivo é maior do que ou igual ao valor especificado (sinal ">").

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o número de processadores lógicos no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **Regras para atribuição de funções**

  Para esta opção, especifique na etapa seguinte:

  Ativar o perfil de política por função específica do proprietário do dispositivo

  Selecione esta opção para configurar e ativar a regra da ativação do perfil no dispositivo, dependendo da função do proprietário. Adicione a função manualmente da lista de funções existentes.

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados.

- **Regras para uso de tag**

  Marque esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo das tags atribuídas ao dispositivo. Você pode ativar o perfil da política para os dispositivos com ou sem tags selecionadas.

  Para esta opção, especifique na etapa seguinte:

  Lista de tags

  Na lista de tags, especifique uma regra para a inclusão do dispositivo no perfil da política, selecionando as caixas de seleção ao lado das tags relevantes.

  Você pode adicionar novas tags à lista inserindo-as no campo sobre a lista e clicando no botão **Adicionar**.

  O perfil da política inclui dispositivos com descrições que contêm todas as tags selecionadas. Se as caixas de seleção forem desmarcadas, o critério não é aplicado. Por padrão, estas caixas de seleção estão desmarcadas.

  Aplicar aos dispositivos sem tags especificadas

  Ative esta opção se tiver de inverter a seleção de tags.

  Se esta opção estiver selecionada, o perfil da política inclui dispositivos com descrições que não contêm nenhuma das tags selecionadas. Se esta opção estiver desativada, o critério não é aplicado.

  Por padrão, esta opção está desativada.

- **Regras para uso do Active Directory**

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo da presença do dispositivo em uma unidade organizacional (UO) do Active Directory ou em uma associação do dispositivo (ou seu proprietário) em um grupo de segurança do Active Directory.

  Para esta opção, especifique na etapa seguinte:

  Associação do proprietário do dispositivo em um grupo de segurança do Active Directory

  Se esta opção estiver ativada, o perfil da política será ativado no dispositivo cujo proprietário for um membro do grupo de segurança especificado. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

  Associação do dispositivo no grupo de segurança do Active Directory

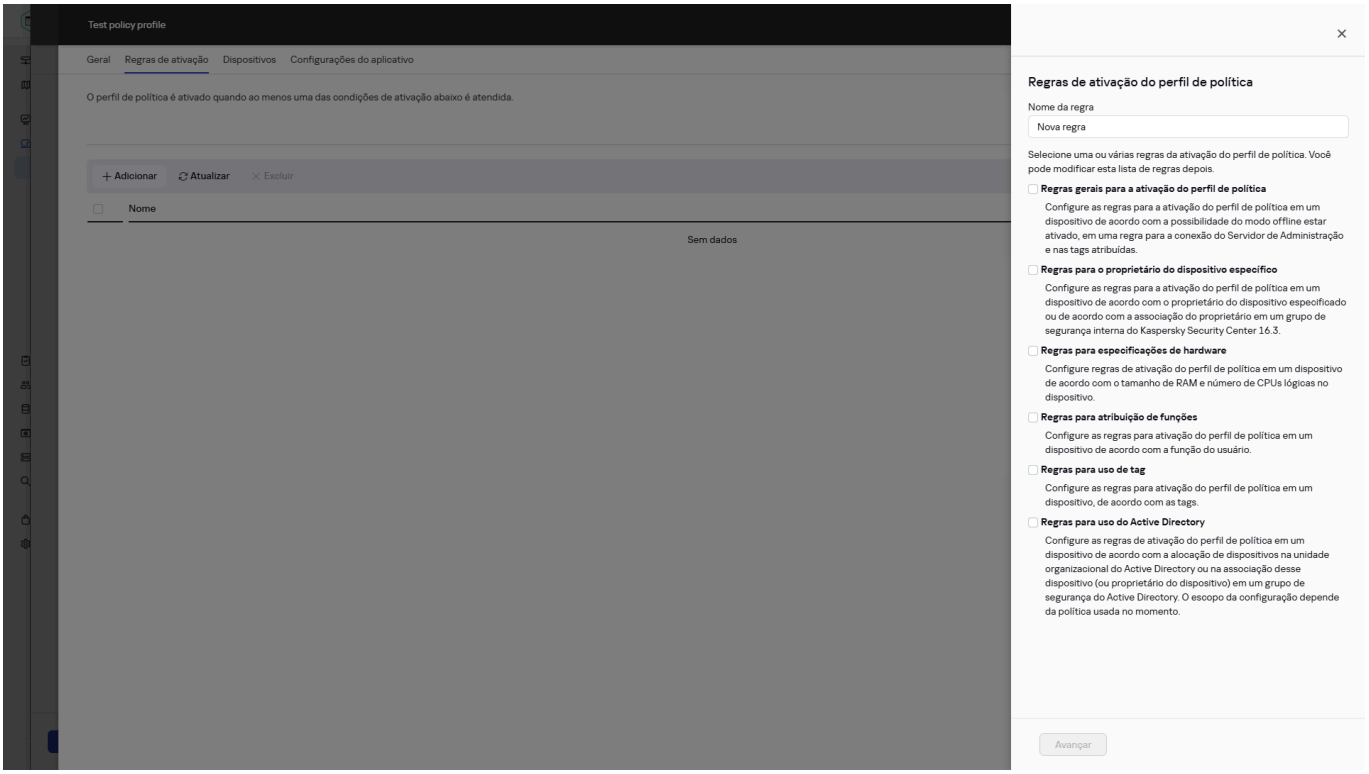
  Se esta opção estiver ativada, o perfil da política será ativado no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

  A alocação do dispositivo está na unidade organizacional do Active Directory

  Se esta opção estiver ativada, o perfil da política será ativado no dispositivo que estiver incluído na unidade organizacional (OU) do Active Directory especificada. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado.

  Por padrão, esta opção está desativada.

O número de páginas adicionais do assistente depende das configurações que você seleciona no primeiro passo. Você pode modificar as regras de ativação do perfil da política em outro momento.



Criar uma regra de ativação do perfil da política

6. Verifique a lista dos parâmetros configurados. Se a lista estiver correta, clique em **Criar**.

   O perfil será salvo. O perfil será ativado no dispositivo quando as regras de ativação forem acionadas.

As regras de ativação do perfil da política criadas para o perfil são exibidas nas propriedades do perfil da política na guia **Regras de ativação**. Você pode modificar ou remover qualquer regra de ativação do perfil da política.

Múltiplas regras de ativação podem ser acionadas simultaneamente.

Excluir um perfil de política

Para excluir um perfil de política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.

2. Na guia **Perfis de política**, marque a caixa de seleção ao lado do perfil de política que deseja excluir e clique em **Excluir**.

3. Na janela exibida, clique em **Excluir** novamente.

   O perfil da política é excluído. Se a política for herdada por um grupo de nível mais baixo, o perfil permanecerá nesse grupo, mas se tornará o perfil da política desse grupo. Isso é feito para eliminar a alteração significativa nas configurações dos aplicativos gerenciados instalados nos dispositivos de grupos de nível mais baixo.

Exportar e importar um perfil de política

Você pode salvar um perfil de política em um arquivo KLPROF sem exportar uma política e, em seguida, usar esse arquivo para importar o perfil salvo para a política.

Isso permite restaurar as configurações da política de perfil rapidamente em vez de configurá-las de novo.

Um perfil de política é importado para a política da mesma versão do aplicativo do qual você exportou o perfil. Para aplicativos compatíveis com versões anteriores de políticas (por exemplo, o Kaspersky Endpoint Security for Windows), você pode importar perfis de política para versões diferentes da política.

Para exportar um perfil de política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.

2. Na guia **Perfis de política**, selecione o perfil de política que você deseja exportar.

3. Na barra de ferramentas, clique no botão **Exportar**.

4. Na janela exibida, especifique o diretório no qual você deseja salvar o arquivo com o perfil de política.

   É possível alterar o nome do arquivo, se necessário.

5. Clique no botão **Salvar**.

Se a operação for concluída com êxito, uma mensagem apropriada será exibida na tela. Caso contrário, uma mensagem de erro será exibida.

Para importar um perfil de política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.

2. Na barra de ferramentas, clique no botão **Importar**.

3. Na janela exibida, selecione o arquivo KLPROF com o perfil de política necessário e clique no botão **Abrir**.

   O tamanho máximo do arquivo importado é de 4 MB.

Se a operação for concluída com êxito, uma mensagem apropriada será exibida na tela. Caso contrário, uma mensagem de erro será exibida.

O perfil de política é importado com o nome que tinha quando foi exportado, e não com o nome do arquivo KLPROF.
O arquivo é importado com o status **Desativado** e a prioridade mais baixa, independentemente da prioridade que o perfil de política tinha antes da exportação.

Não será possível fazer a importação:

- Se a política já tiver um perfil com o mesmo nome.
- Se o número de perfis na política for 100.

Configurações de política do Agente de Rede

Para configurar uma política do Agente de Rede:

1. No menu principal do aplicativo, acesse **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Agente de Rede.

   A janela de propriedades da política do Agente de Rede se abre. A janela de propriedades contém as guias e configurações descritas abaixo.

Veja a tabela de comparação detalhando como as configurações abaixo se aplicam, dependendo do tipo de sistema operacional usado.

Geral

Nesta guia, é possível modificar o nome e o status da política, além de especificar a herança das configurações da política:

- No campo **Nome**, você pode modificar o nome da política.
- No bloco **Status da política**, você poderá selecionar um dos modos de política:

  Ativo

  Se esta opção estiver selecionada, a política é habilitada.

  Por padrão, esta opção está selecionada.

  Inativo

  Se esta opção estiver selecionada, a política é habilitada, mas continua armazenada na pasta **Políticas**. Se necessário, a política pode ser habilitada.

- No grupo de configurações **Herança de configurações**, você pode configurar a herança de política:

  Herdar configurações da política principal

  Se esta opção estiver ativada, os valores das configurações de política são herdados da política de grupo de nível superior e, portanto são bloqueados.

  Por padrão, esta opção está ativada.

  Forçar herança de configurações nas políticas secundárias

Se esta opção estiver ativada, após a aplicação das alterações da política, as seguintes ações serão realizadas:

- Os valores das configurações da política serão propagados às políticas de subgrupos de administração, ou seja, às políticas secundárias.
- No bloco **Herança de configurações** da seção **Geral** na janela Propriedades de cada política secundária, a opção **Herdar configurações da política principal** será automaticamente ativada.

Se a opção estiver ativada, as configurações das políticas secundárias são bloqueadas.

Por padrão, esta opção está desativada.

Configuração de eventos

Nessa guia, é possível configurar o registro e a notificação de eventos. Os eventos são distribuídos de acordo com o nível de importância nas seguintes seções:

- **Falha funcional**
- **Advertência**
- **Informações**

Em cada seção, a lista exibe os tipos de eventos e o prazo de armazenamento de eventos padrão no Servidor de Administração (em dias). Após clicar no tipo de evento, é possível especificar as configurações do registro de eventos e as notificações sobre eventos selecionados na lista. Por padrão, as configurações de notificação comuns especificadas para todo o Servidor de Administração são usadas para todos os tipos de evento. Contudo, você pode alterar configurações específicas dos tipos de evento necessários.

Por exemplo, na seção **Advertência**, é possível configurar o tipo de evento **Ocorreu um problema de segurança**. Os eventos podem acontecer, por exemplo, quando o espaço livre em disco de um ponto de distribuição for inferior a 2 GB (pelo menos 4 GB são necessários para instalar aplicativos e baixar atualizações remotamente). Para configurar o evento **Ocorreu um problema de segurança**, clique nele e especifique onde armazenar os eventos ocorridos e como notificá-los.

Caso o Agente de Rede detecte um problema de segurança, será possível gerenciá-lo com o uso das configurações de um dispositivo gerenciado.

Configurações do aplicativo

Configurações

Na seção **Configurações**, você pode configurar a política do Agente de Rede:

Distribuir os arquivos somente através dos pontos de distribuição

Se essa opção for ativada, os Agentes de Rede em dispositivos gerenciados recuperam atualizações apenas de pontos de distribuição.

Se esta opção estiver desativada, os Agentes de Rede em dispositivos gerenciados recuperam atualizações de pontos de distribuição ou do Servidor de Administração.

Observe que os aplicativos de segurança em dispositivos gerenciados recuperam atualizações da fonte definida na tarefa de atualização para cada aplicativo de segurança. Caso a opção **Distribuir os arquivos somente através dos pontos de distribuição** seja ativada, verifique e confirme se o Kaspersky Security Center Linux está definido como uma fonte de atualização nas tarefas de atualização.

Por padrão, esta opção está desativada.

Tamanho máximo da fila de eventos, em MB

Neste campo, você pode especificar o espaço máximo na unidade que uma fila de eventos pode ocupar.

A configuração padrão é 2 MB.

O aplicativo tem permissão para recuperar os dados estendidos da política no dispositivo

O Agente de Rede instalado em um dispositivo gerenciado transfere informações sobre a política do aplicativo de segurança aplicada ao aplicativo de segurança (por exemplo, Kaspersky Endpoint Security for Linux). Você pode visualizar as informações transferidas na interface do aplicativo de segurança.

O Agente de Rede transfere as seguintes informações:

- Hora da entrega da política para o dispositivo gerenciado.
- Nome da política ativa no momento da entrega da política ao dispositivo gerenciado.
- Nome da política de ausência temporária no momento da entrega da política ao dispositivo gerenciado (indisponível para o Agente de Rede para Linux).
- Nome e caminho completo para o grupo de administração que continha o dispositivo gerenciado no momento da entrega da política para o dispositivo gerenciado.
- Lista de perfis de política ativos com seus nomes e prioridades no momento da entrega da política ao dispositivo gerenciado.

Você pode usar as informações para garantir que a política correta seja aplicada ao dispositivo e para fins de solução de problemas. Por padrão, esta opção está desativada.

Proteger serviço do Agente de Rede contra remoção ou interrupção não autorizada e impedir alterações nas configurações

Quando esta opção estiver ativado, após o Agente de Rede ter sido instalado em um dispositivo gerenciado, o componente não poderá ser removido ou reconfigurado sem os privilégios necessários. O serviço Agente de Rede não pode ser interrompido. Essa opção não tem efeito nos controladores de domínio.

Ative esta opção para proteger o Agente de Rede em estações de trabalho operadas com direitos de administrador local.

Por padrão, esta opção está desativada.

Usar senha de desinstalação

Caso esta opção esteja marcada, ao clicar no botão **Modificar**, será possível especificar a senha para o utilitário klmover e a desinstalação remota do Agente de Rede em dispositivos baseados no Windows.

Por padrão, esta opção está desativada.

Repositórios

Na seção **Repositórios**, é possível selecionar os tipos de objetos cujos detalhes serão enviados do Agente de Rede para o Servidor de Administração:

Detalhes dos aplicativos instalados

Se esta opção estiver ativada, as informações sobre os aplicativos instalados nos dispositivos clientes serão enviadas ao Servidor de Administração.

Por padrão, esta opção está ativada.

Incluir informações sobre patches

As informações sobre os patches para os aplicativos instalados nos dispositivos cliente são enviadas ao Servidor de Administração. A ativação desta opção pode aumentar a carga no Servidor de Administração e DBMS, assim como causar volume aumentado do banco de dados.

Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

Detalhes das atualizações do Windows Update

Se esta opção estiver ativada, as informações sobre as atualizações obrigatórias do Microsoft Windows Update que devem ser instaladas nos dispositivos clientes serão enviadas ao Servidor de Administração.

Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

Detalhes das vulnerabilidades de software e das atualizações correspondentes

Se essa opção estiver ativada, as informações sobre vulnerabilidades no software de terceiros (incluindo software da Microsoft), detectadas em dispositivos gerenciados e sobre atualizações de software para corrigir vulnerabilidades de terceiros (não incluindo o software da Microsoft) são enviadas ao Servidor de Administração.

Selecionando esta opção (**Detalhes das vulnerabilidades de software e das atualizações correspondentes)** aumenta a carga da rede, a carga do disco do Servidor de Administração e o consumo de recurso pelo Agente de Rede.

Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

Para gerenciar atualizações de software da Microsoft, use a opção **Detalhes das atualizações do Windows Update**.

Detalhes do registro de hardware

O Agente de Rede instalado em um dispositivo envia informações sobre o hardware do dispositivo para o Servidor de Administração. Você pode exibir os detalhes do hardware nas propriedades do dispositivo.

Verifique e confirme se o utilitário lshw está instalado nos dispositivos Linux a partir dos quais deseja buscar detalhes de hardware. Os detalhes de hardware obtidos de máquinas virtuais podem estar incompletos, dependendo do hipervisor usado.

Se a modificação de algumas configurações nesta seção estiver bloqueada pela política do Agente de Rede, você não pode modificá-las.

Atualizações e vulnerabilidades de software

Na seção **Atualizações e vulnerabilidades de software**, é possível ativar a verificação de arquivos executáveis quanto a vulnerabilidades:

Verificar a vulnerabilidade dos arquivos executáveis ao executá-los

Se essa caixa de seleção estiver selecionada, as vulnerabilidades serão verificadas quando os arquivos executáveis forem executados.

Por padrão, esta opção está ativada.

Gerenciamento de reinicialização

Na seção **Gerenciamento de reinicialização**, é possível especificar a ação a ser executada se o sistema operacional de um dispositivo gerenciado precisar ser reiniciado para uso correto, instalação ou desinstalação de um aplicativo:

Não reiniciar o sistema operacional

Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

Reiniciar o sistema operacional automaticamente se necessário

Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

Perguntar ao usuário o que fazer

O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

Por padrão, esta opção está selecionada.

Repetir aviso a cada (min)

Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

Forçar reinicialização após (min)

Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

Forçar fechamento de aplicativos em sessões bloqueadas

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

Gerenciar patches e atualizações

Na seção Gerenciar patches e atualizações, você poderá configurar o download e a distribuição das atualizações, assim como a instalação dos patches nos dispositivos gerenciados:

Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido

Se esta opção estiver ativada, os patches da Kaspersky com o status de aprovação *Indefinido* são automaticamente instaladas nos dispositivos gerenciados imediatamente após terem sido baixadas dos servidores de atualização.

Se esta opção estiver desativada, as correções da Kaspersky que foram baixadas e identificadas com o status *Indefinido* somente serão instaladas após você alterar o status para *Aprovado*.

Por padrão, esta opção está ativada.

Fazer antecipadamente o download das atualizações e dos bancos de dados de antivírus via Servidor de Administração (recomendado)

Se esta opção está ativada, o modelo offline do download da atualização é usado. Quando o Servidor de Administração recebe atualizações, ele notifica o Agente de Rede (nos dispositivos em que ele esteja instalado) sobre as atualizações que serão necessárias para os aplicativos gerenciados. Quando o Agentes de Rede recebe informações sobre essas atualizações, ele baixa dos arquivos relevantes do Servidor de Administração com antecedência. Na primeira conexão com o Agente de Rede, o Servidor de Administração inicia um download de atualizações. Após o Agente de Rede ter baixado todas as atualizações em um dispositivo cliente, as atualizações se tornam disponíveis para os aplicativos naquele dispositivo.

Quando um aplicativo gerenciado em um dispositivo cliente tentar acessar o Agente de Rede quanto a atualizações, o Agente de Rede verifica se ele tem todas as atualizações necessárias. Se as atualizações forem recebidas do Servidor de Administração até 25 horas antes de terem sido solicitadas pelo aplicativo gerenciado, o Agente de Rede não se conectará ao Servidor de Administração, mas fornecerá ao aplicativo gerenciado as atualizações do cache local. A conexão com o Servidor de Administração pode não ser estabelecida quando o Agente de Rede fornecer atualizações aos aplicativos em dispositivos cliente, mas a conexão não é necessária para a atualização.

Se esta opção está desativada, o modelo offline do download da atualização é usado. As atualizações são distribuídas de acordo com o agendamento da tarefa de download da atualização.

Por padrão, esta opção está ativada.

Conectividade

A seção **Conectividade** inclui três subseções:

- **Rede**
- **Perfis de conexão**
- **Agendamento de conexão**

Na subseção **Rede**, você pode configurar a conexão ao Servidor de Administração, ativar o uso de uma porta UDP e especificar o número da porta UDP.

- No grupo de configurações **Conectar-se ao Servidor de Administração**, você poderá configurar a conexão ao Servidor de Administração e especificar o intervalo de tempo para a sincronização entre os dispositivos cliente e o Servidor de Administração:

  Intervalo de sincronização (min)

  O Agente de Rede sincroniza o dispositivo gerenciado com o Servidor de Administração. Recomendamos definir o intervalo de sincronização (também conhecido como heartbeat) para 15 minutos a cada 10.000 dispositivos gerenciados.

  Compactar o tráfego de rede

  Se esta opção estiver ativada, a velocidade de transferência de dados pelo Agente de Rede é aumentada através da redução da quantidade de informação a ser transferida e consequente carga inferior sobre o Servidor de Administração.

  > A carga na CPU do computador cliente pode aumentar.

  Por padrão, esta caixa de seleção é marcada.

  Abrir portas do Agente de Rede no firewall do Microsoft Windows

  Se esta opção estiver ativada, as portas, necessárias para o funcionamento do Agente de Rede, serão adicionadas à lista de exclusões do Firewall do Microsoft Windows.

  Por padrão, esta opção está ativada.

  Usar conexão SSL

  Se esta opção estiver ativada, a conexão com o Servidor de Administração é estabelecida através de uma porta segura via SSL.

  Por padrão, esta opção está ativada.

  Usar o gateway de conexão em um ponto de distribuição (se disponível) com as configurações de conexão padrão

  Se esta opção estiver marcada, o gateway de conexão no ponto de distribuição é usado sob as configurações especificadas nas propriedades do grupo de administração.

  Por padrão, esta opção está ativada.

- **Usar porta UDP**

  Caso deseje que o Agente de Rede seja conectado com o Servidor de Administração por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de **Porta UDP**. Por padrão, esta opção está ativada. A porta UDP padrão para estabelecer conexão com o Servidor de Administração é 15000.

- **Número da porta UDP**

  Neste campo, é possível inserir o número da porta UDP. O número da porta padrão é 15000.

  É usado o sistema decimal para registros.

- **Usar ponto de distribuição para forçar conexão com o Servidor de Administração**

  Selecione esta opção se você selecionou a opção **Usar este ponto de distribuição como um servidor push** na janela de configurações do ponto de distribuição. Do contrário, o ponto de distribuição não atuará como um servidor push.

Na subseção **Perfis de conexão**, é possível especificar as configurações da localização da rede e ativar o modo ausente quando o Servidor de Administração não estiver disponível:

Configurações do local de rede

As configurações da localização da rede definem as características da rede à qual o dispositivo cliente está conectado e especifica as regras para o Agente de Rede alternando de um perfil de conexão do Servidor de Administração a outro quando aquelas características da rede forem alteradas.

Perfis de conexão do Servidor de Administração

É possível visualizar e adicionar perfis à conexão do Agente de Rede com o Servidor de Administração. Nesta seção, você também pode criar regras para alternar o Agente de Rede para diferentes Servidores de Administração quando os seguintes eventos ocorrem:

- Quando o dispositivo cliente se conectar a outra rede local
- Quando um dispositivo perde a conexão com a rede local da organização
- Quando o endereço do gateway de conexão for alterado ou o endereço do servidor DNS for modificado

Ativar modo ausente quando o Servidor de Administração não estiver disponível

Se esta opção estiver marcada, no caso da conexão com este perfil, os aplicativos instalados no dispositivo cliente irão usar as políticas do modo ausente, assim como as políticas de ausência de escritório. Se a política de ausência do escritório não estiver definida para o aplicativo, a política ativa será usada.

Se esta opção estiver desativada, os aplicativos usarão as políticas ativas.

Por padrão, esta opção está desativada.

Na subseção **Agendamento de conexão**, você pode especificar os intervalos de tempo durante os quais o Agente de Rede envia dados para o Servidor de Administração:

Conectar quando necessário

Se esta opção estiver selecionada, a conexão é estabelecida quando o Agente de Rede tem de enviar dados para o Servidor de Administração.

Por padrão, esta opção está selecionada.

Conectar-se nos intervalos de tempo especificados

Se esta opção estiver selecionada, o Agente de Rede se conecta ao Servidor de Administração numa hora específica. Você pode adicionar vários períodos de tempo de conexão.

Sondagem da rede por pontos de distribuição

Na seção **Sondagem da rede por pontos de distribuição**, você pode configurar a amostragem automática da rede. Você pode usar as seguintes opções para ativar a sondagem e definir a frequência:

Rede Windows

A opção está disponível somente para pontos de distribuição baseados em Windows.

Se a esta opção estiver ativada, o Servidor de Administração automaticamente efetua a sondagem da rede de acordo com o agendamento configurado ao clicar nos links **Definir agendamento da sondagem rápida** e **Definir agendamento da sondagem completa**.

Caso essa opção esteja desativada, o Servidor de Administração sonda a rede com o intervalo especificado no campo **Frequência de sondagens da rede (min)**.

O intervalo de descoberta de dispositivos para versões do Agente de Rede pode ser configurado nos campos **Frequência de sondagens de domínios Windows (min)** (para a sondagem rápida de rede do Windows) e **Frequência de sondagens da rede (min)** (para a sondagem completa de rede do Windows).

Por padrão, esta opção está desativada.

Intervalos de IPs

Caso a opção esteja ativada, o ponto de distribuição automaticamente realiza a sondagem dos intervalos de IP de acordo com o agendamento configurado ao clicar no link **Definir agendamento da sondagem**.

Se essa opção estiver desmarcada, o ponto de distribuição não faz a sondagem dos intervalos de IP.

A frequência de sondagem de conjuntos de IPs para versões do Agente de Rede anteriores a 10.2 pode ser configurada no campo **Intervalo de sondagem (min)**. O campo está disponível se a opção estiver ativada.

Por padrão, esta opção está desativada.

Zeroconf

Se esta opção for ativada, o ponto de distribuição sondará automaticamente a rede com dispositivos IPv6 usando a rede zero configuração (também referida como *Zeroconf*). Nesse caso, a sondagem de intervalo de IP ativada é ignorada, porque o ponto de distribuição sonda toda a rede.

Para começar a usar o Zeroconf, as seguintes condições devem ser atendidas:

- O ponto de distribuição deve executar Linux.
- Você deve instalar o utilitário avahi-browse no ponto de distribuição.

Se essa opção estiver desativada, o ponto de distribuição não faz a sondagem com dispositivos IPv6y.

Por padrão, esta opção está desativada.

Controladores de domínio

Caso a opção esteja ativada, o ponto de distribuição realiza automaticamente a sondagem dos controladores de domínio de acordo com o agendamento configurado ao clicar no botão **Definir agendamento da sondagem**.

Caso essa opção esteja desativada, o ponto de distribuição não faz a sondagem dos controladores de domínio.

A frequência de sondagem do controlador de domínio para as versões do Agente de Rede anteriores a 10.2 pode ser configurada no campo **Intervalo de sondagem (min)**. O campo está disponível caso a opção esteja ativada.

Por padrão, esta opção está desativada.

Configurações de rede para pontos de distribuição

Na seção **Configurações de rede para pontos de distribuição**, você pode especificar as configurações de acesso à Internet:

- **Usar o servidor proxy**

  Se esta opção estiver ativada, um servidor proxy da Internet será usado para conectar os pontos de distribuição aos servidores de atualização Kaspersky.

- **Endereço**

- **Número da porta**

- **Ignorar servidor proxy para endereços locais**

  Se esta opção estiver ativada, nenhum servidor proxy será usado para se conectar aos dispositivos na rede local.

  Por padrão, esta opção está desativada.

- **Autenticação do servidor proxy**

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

  Por padrão, esta caixa de seleção está desmarcada.

KSN Proxy (pontos de distribuição)

Na seção **KSN Proxy (pontos de distribuição)**, você pode configurar o aplicativo para usar o ponto de distribuição para encaminhar solicitações da Kaspersky Security Network (KSN) por meio dos dispositivos gerenciados:

Ativar o proxy da KSN no lado do ponto de distribuição

O serviço Proxy da KSN é executado no dispositivo que é usado como um ponto de distribuição. Use este recurso para redistribuir e otimizar o tráfego na rede.

O ponto de distribuição envia as estatísticas da KSN, que estão listadas na Declaração da Kaspersky Security Network, à Kaspersky.

Por padrão, esta opção está desativada. A ativação desta opção somente terá efeito caso as opções **Usar Servidor de Administração como um servidor proxy** e **Concordo em usar a Kaspersky Security Network** estejam ativadas na janela de propriedades do Servidor de Administração.

É possível atribuir um nó de um cluster ativo-passivo a um ponto de distribuição e habilitar o servidor proxy da KSN nesse nó.

Encaminhar solicitações da KSN para o Servidor de Administração

O ponto de distribuição encaminha solicitações do KSN dos dispositivos gerenciados para o Servidor de Administração.

Por padrão, esta opção está ativada.

Acessar a KSN Cloud/KPSN diretamente pela Internet

O ponto de distribuição encaminha solicitações da KSN de dispositivos gerenciados para a KSN Cloud ou KPSN. As solicitações da KSN geradas no próprio ponto de distribuição também são enviadas diretamente para a KSN Cloud ou para a KPSN.

Porta TCP

O número da porta TCP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. O número da porta padrão é 13111.

Porta UDP

Caso deseje que o Agente de Rede seja conectado com o Servidor de Administração por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de **Porta UDP**. Por padrão, esta opção está ativada. A porta UDP padrão para estabelecer conexão com o Servidor de Administração é 15000.

Porta HTTPS

Se você precisar que os dispositivos gerenciados se conectem ao servidor proxy da KSN por meio de uma porta HTTPS, ative a opção **Usar HTTPS** e especifique um número de porta no campo **Porta HTTPS**. Por padrão, esta opção está desativada. A porta HTTPS padrão para se conectar ao servidor proxy KSN é 17111.

Atualizações (pontos de distribuição)

Na seção **Atualizações (pontos de distribuição)**, é possível ativar o recurso de download de arquivos diff, para que os pontos de distribuição recebam atualizações na forma de arquivos diff dos servidores de atualização da Kaspersky.

Gerenciamento da conta local (apenas Linux)

A seção **Gerenciamento da conta local (apenas Linux)** inclui três subseções:

- **Gerenciamento de certificados do usuário**
- **Adicionar ou editar os grupos de administradores locais pertinentes**
- **Carregar um arquivo de referência para evitar alterações ao arquivo sudoers no dispositivo do usuário**

Na subseção **Gerenciamento de certificados do usuário**, você pode especificar quais certificados raiz instalar. Esses certificados podem ser usados, por exemplo, para verificar a autenticidade de sites ou servidores Web.

Instalar certificados raiz

Se esta opção estiver ativada, os certificados adicionados à tabela serão instalados nos dispositivos especificados.

Se esta opção estiver desativada, nenhum certificado será instalado nos dispositivos especificados.

Por padrão, esta opção está desativada.

Adicionar

Clicar nesse botão abre uma janela, na qual você pode adicionar um certificado.

O certificado deve ter menos de 10 MB.

O Kaspersky Security Center é compatível com certificados com as extensões CER, CRT, CERT, PEM e KEY.

Na subseção **Adicionar ou editar os grupos de administradores locais pertinentes**, você pode gerenciar grupos de administradores locais. Esses grupos são usados, por exemplo, ao revogar direitos de administrador local. Você também pode verificar a lista de contas de usuários privilegiados usando o **Relatório de usuários privilegiados dos dispositivos (apenas Linux)**.

Adicionar

Clicar nesse botão abre uma janela, onde você pode adicionar um grupo de administradores local.

Editar

Clicar nesse botão abre uma janela, onde você pode editar o grupo de administradores locais.

Este botão estará disponível se a caixa de seleção ao lado do grupo de administradores locais estiver marcada.

Excluir

Clicar nesse botão exclui o grupo de administradores locais selecionado da tabela.

Este botão estará disponível se a caixa de seleção ao lado do grupo de administradores locais estiver marcada.

Na subseção **Carregar um arquivo de referência para evitar alterações ao arquivo sudoers no dispositivo do usuário**, você pode configurar o controle do arquivo sudoers. Os grupos privilegiados e os usuários do dispositivo são definidos pelo arquivo sudoers no dispositivo. O arquivo sudoers está localizado em `/etc/sudoers`. Você pode carregar um arquivo sudoers de referência para proteger o arquivo sudoers contra alterações. Isso evitará alterações indesejadas no arquivo sudoers.

Um arquivo sudoers de referência inválido pode causar o mau funcionamento do dispositivo do usuário.

Controlar o arquivo sudoers

Se esta opção estiver ativada, o arquivo sudoers será substituído pelo arquivo sudoers de referência atual.

Se esta opção estiver desativada, o arquivo sudoers permanecerá inalterado.

Por padrão, esta opção está desativada.

Arquivo sudoers de referência

Este campo exibe o nome do arquivo sudoers de referência carregado.

Carregar

Clicar nesse botão abre uma janela, onde você pode carregar um arquivo sudoers de referência.

Arquivo sudoers de referência atual

Clicar nesse botão mostra o conteúdo do arquivo sudoers atual.

Histórico de revisões

Na guia **Histórico de revisões**, você pode:

- Visualizar e salvar o histórico de revisões de políticas.
- Reverter uma revisão de política.
- Adicionar e editar as descrições da revisão da política.
- Comparar revisões de política.

Uso do Agente de Rede para Windows, Linux e macOS: comparativo

O uso do Agente de Rede depende do sistema operacional do dispositivo. A política do Agente de Rede e as configurações do pacote de instalação também diferem, dependendo do sistema operacional. A tabela a seguir compara os recursos do Agente de Rede e os cenários de uso disponíveis para os sistemas operacionais Windows, Linux e macOS.

Comparativo de recursos do Agente de Rede

Recurso do Agente de Rede	Windows	Linux	macOS
Instalação			
Instalando por clonagem uma imagem do disco rígido do administrador com o sistema operacional e o Agente de Rede usando ferramentas de terceiros	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓	✓
Instalar com ferramentas de terceiros para a instalação remota de aplicativos	✓	✓	✓
Instalar manualmente, executando os instaladores do aplicativo em dispositivos	✓	✓	✓
Instalar o Agente de Rede em modo silencioso	✓	✓	✓
Conecte manualmente um dispositivo cliente ao Servidor de administração. Utilitário klmover	✓	✓	✓
Instalar as atualizações e patches para componentes do Kaspersky Security Center automaticamente	✓	✓	—
Distribuir uma chave automaticamente	✓	✓	✓
Sincronização forçada	✓	✓	✓ Exceção a um servidor push
Ponto de distribuição			

Recurso do Agente de Rede	Windows	Linux	macOS
Usar como ponto de distribuição	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓	✓
Calcular o número e a configuração de pontos de distribuição	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓ Sem usar o Reconhecimento de Local de Rede (NLA).	✓ Sem usar o Reconhecimento de Local de Rede (NLA).
Modelo offline de download da atualização	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓	✓
Sondagem da rede	✓ • Sondagem do conjunto de IPs • Sondagem do controlador de domínio (Microsoft Active Directory) Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓ Sondagem do conjunto de IPs Sondagem Zeroconf Sondagem do controlador de domínio (Microsoft Active Directory, Samba 4 Active Directory, FreeIPA, ALD Pro)	—
Execução do Serviço de Proxy da KSN no lado do ponto de distribuição	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓	—
Baixar atualizações via servidores de atualização Kaspersky para os repositórios de pontos de distribuição que distribuem atualizações para dispositivos gerenciados	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓	— (Se um ou mais dispositivos executando Linux ou macOS estiverem dentro do escopo da tarefa Baixar atualizações para os repositórios de pontos de distribuição, a tarefa será concluída com o status Falha, mesmo se for concluída com êxito em todos os dispositivos Windows.)
Instalação push de aplicativos	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	Restrito: não é possível realizar instalação push em dispositivos Windows usando pontos de distribuição Linux.	Restrito: não é possível realizar a instalação push em dispositivos Windows usando pontos de distribuição do macOS.
Usar como servidor push	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓	—
Gerenciamento de aplicativos de terceiros			
Instalação remota de aplicativos em dispositivos	✓	✓	✓ Consulte o seguinte artigo para obter informações: Instalação remota de aplicativos em dispositivos macOS.

Recurso do Agente de Rede	Windows	Linux	macOS
Configurar as atualizações do sistema operacional em uma política de Agente de Rede	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	—	—
Exibir informações sobre as vulnerabilidades do software	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	—	—
Verificar os aplicativos quanto a vulnerabilidades	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	—	—
Atualizações de software	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	—	—
Inventário de software instalado nos dispositivos	✓	✓	—
Máquinas virtuais			
Instalar o Agente de Rede em uma máquina virtual	✓	✓	✓
As configurações de optimização da infraestrutura de desktop virtual (VDI)	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓	✓
Suporte de máquinas virtuais dinâmicas	✓ Limitação: Não compatível com o Agente de Rede para Microsoft Windows on Arm.	✓	✓
Outro			
Auditoria de ações em um dispositivo cliente remoto usando o Windows Desktop Sharing	✓	—	—
Monitoramento do status de proteção antivírus	✓	✓	✓
Gerenciar reinícios de dispositivos	✓	—	—
Suporte da reversão do sistema	✓	✓	✓
Usar um Agente de Rede como um gateway de conexão	✓	✓	✓
Gerenciador de conexões	✓	✓	✓
Perfis de conexão para usuários ausentes	✓	✓	✓

Recurso do Agente de Rede	Windows	Linux	macOS
Agente de Rede alternando de um Servidor de Administração para outro (automaticamente pelo local da rede)	✓	✓	✓
Verificando a conexão entre um dispositivo cliente e o Servidor de Administração. Utilitário klnagchk	✓	✓	✓
Conexão remota à Área de trabalho de um dispositivo cliente	✓	✓	✓ Usando o sistema de computação de rede virtual (VNC).
Download de um pacote de instalação independente por meio do Assistente de migração	✓	✓	✓
Visualização de informações sobre o hardware dos dispositivos clientes	✓	✓ As informações sobre o hardware dos dispositivos Linux enviadas ao Servidor de Administração pelo Agente de Rede instalado nesses dispositivos são limitadas às informações especificadas na descrição das configurações do dispositivo gerenciado.	✓ As informações sobre o hardware dos dispositivos macOS enviadas ao Servidor de Administração pelo Agente de Rede instalado nesses dispositivos são limitadas às informações especificadas na descrição das configurações do dispositivo gerenciado.

Comparativo entre configurações de Agente de Rede por sistemas operacionais

A tabela abaixo mostra quais configurações da política do Agente de Rede estão disponíveis dependendo do sistema operacional do dispositivo gerenciado no qual o Agente de Rede foi instalado.

Configurações do Agente de Rede: comparativo entre sistemas operacionais

Seção Settings	Windows	Linux	macOS
Geral	✓	✓	✓
Configuração de eventos	✓	✓	✓
Configurações	✓	✓ As seguintes opções estão disponíveis: • **Distribuir os arquivos somente através dos pontos de distribuição** • **Tamanho máximo da fila de eventos, em MB** • **O aplicativo tem permissão para recuperar os dados estendidos da política no dispositivo**	✓
Repositórios	✓	✓ As seguintes opções estão disponíveis: • **Detalhes dos aplicativos instalados** • **Detalhes do registro de hardware**	✓ A opção **Detalhes do registro de hardware** está disponível.
Conectividade → Rede	✓	✓ Exceto a opção **Abrir portas do Agente de Rede no firewall do Microsoft Windows**.	✓
Conectividade → Perfis de conexão	✓	✓	✓

Seção Settings	Windows	Linux	macOS
Conectividade → Agendamento de conexão	✓	✓	✓
Sondagem da rede por pontos de distribuição	✓ As seguintes opções estão disponíveis: • **Rede Windows** • **Intervalos de IPs** • **Controladores de domínio**	✓ As seguintes opções estão disponíveis: • **Zeroconf** • **Intervalos de IPs** • **Controladores de domínio**	—
Configurações de rede para pontos de distribuição	✓	✓	✓
KSN Proxy (pontos de distribuição)	✓	✓	—
Atualizações (pontos de distribuição)	✓	✓	—
Histórico de revisões	✓	✓	✓

Ativar e desativar o modo de baixo consumo de recursos para o Agente de Rede

O modo de baixo consumo de recursos permite limitar o uso de RAM do Agente de Rede instalado no dispositivo cliente. Por padrão, o modo de baixo consumo de recursos está desativado.

No modo de baixo consumo de recursos, as seguintes funções não são executadas:

- O Agente de Rede não pode ser atribuído para atuar como um ponto de distribuição (manual ou automaticamente).
- O Agente de Rede não registra informações sobre o status do Agente de Rede em um arquivo de texto separado.
- O Agente de Rede não é compatível com o modelo offline de download da atualização.
- Os seguintes componentes e processos estão desativados:
  - Obter informações sobre atualizações e vulnerabilidades de terceiros.
  - Executar proxy da KSN no lado do ponto de distribuição.
  - Carregar atualizações para o repositório do ponto de distribuição.
  - Ignorar o bloco do servidor DNS.
  - Obtenção de informações sobre espaço livre em disco.

Componentes e processos retomam a operação depois de desativar o modo de baixo consumo de recursos.

Para ativar o modo de baixo consumo de recursos:

1. Execute o seguinte comando na linha de comando do dispositivo cliente:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Reinicie o Agente de Rede usando o seguinte comando:

   ```
   sudo service klnagent64 restart
   ```

3. No registro do sistema operacional, verifique se a entrada **O Agente de Rede do Kaspersky Security Center está funcionando no modo de baixo consumo de recursos** é exibida.

O modo de baixo consumo de recursos está ativado.

Para desativar o modo de baixo consumo de recursos:

1. Execute o seguinte comando na linha de comando do dispositivo cliente:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Reinicie o Agente de Rede usando o seguinte comando:

   ```
   sudo service klnagent64 restart
   ```

O modo de baixo consumo de recursos está desativado.

Você também pode ativar o modo de baixo consumo de recursos remotamente usando uma tarefa *Executar scripts remotamente*.

Definir as configurações de proteção de aplicativos gerenciados

Para definir as configurações de proteção de aplicativos gerenciados da Kaspersky, você pode usar políticas.

Para obter mais informações sobre a configuração de políticas do Kaspersky Endpoint Security, consulte a respectiva Ajuda:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux
- Ajuda do Kaspersky Endpoint Security for Mac

Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security

A opção de agendamento ideal e recomendada para o Kaspersky Endpoint Security é **Quando novas atualizações são baixadas no repositório** quando a caixa de seleção **Usar atraso aleatório automaticamente para início da tarefa** estiver marcada.

Configuração manual da tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security

O Assistente de início rápido cria uma tarefa de grupo para verificar um dispositivo. Caso o agendamento especificado automaticamente da tarefa de verificação de grupo não seja adequado para sua organização, é preciso configurar manualmente o agendamento mais conveniente para essa tarefa de acordo com as regras do local de trabalho adotadas na organização.

Por exemplo, é atribuído um agendamento para a tarefa **Executar às sextas-feiras as 19h** com aleatorização automática, e a caixa de seleção **Executar tarefas ignoradas** deve estar desmarcada. Isso significa que se os dispositivos em uma organização são desligados às sextas-feiras, por exemplo, às 18h30, a tarefa de verificação de dispositivo nunca será executada. Nesse caso, é necessário configurar a tarefa de verificação de grupo manualmente.

Kaspersky Security Network (KSN)

Essa seção descreve como usar uma infraestrutura de serviços on-line, denominada Kaspersky Security Network (KSN). A seção fornece os detalhes sobre a KSN, assim como instruções sobre como ativar a KSN, configurar o acesso à KSN e visualizar as estatísticas sobre o uso do Servidor proxy da KSN.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Sobre a KSN

A Kaspersky Security Network (KSN) é uma infraestrutura de serviços on-line que fornece o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software. O uso de dados a partir da Kaspersky Security Network garante uma resposta mais rápida dos aplicativos Kaspersky a ameaças, melhora a efetividade de alguns componentes de proteção e reduz o risco de falsos positivos. A KSN permite usar os bancos de dados de reputação da Kaspersky para obter informações sobre os aplicativos instalados nos dispositivos gerenciados.

Ao participar da Kaspersky Security Network, você concorda em fornecer automaticamente à Kaspersky informações sobre a operação dos aplicativos de segurança instalados em computadores e dispositivos móveis gerenciados por meio do Kaspersky Security Center Linux. As informações são transferidas de acordo com as configurações de acesso da KSN atuais.

O Kaspersky Security Center Linux oferece suporte às seguintes soluções de infraestrutura da KSN:

- *KSN Global* é uma solução que permite trocar informações com a Kaspersky Security Network. Ao participar da KSN, você concorda em enviar à Kaspersky informações no modo automático sobre a operação dos aplicativos da Kaspersky instalados nos dispositivos cliente gerenciados através do Kaspersky Security Center Linux. As informações são transferidas de acordo com as configurações de acesso da KSN atuais. Os analistas da Kaspersky também averiguam as informações recebidas e as incluem nos bancos de dados estatísticos e de reputação da Kaspersky Security Network. O Kaspersky Security Center Linux usa essa solução por padrão.

- A *Kaspersky Private Security Network (KPSN)* é uma solução que possibilita aos usuários de dispositivos com aplicativos da Kaspersky instalados obterem o acesso aos bancos de dados de reputação da Kaspersky Security Network, assim como a outros dados estatísticos, sem o envio de dados à KSN Global de seus próprios dispositivos. A KPSN foi projetada para clientes corporativos que não podem participar da Kaspersky Security Network por algum dos seguintes motivos:

  - Os dispositivos do usuário não estão conectados à Internet.

  - A transmissão de quaisquer dados fora do país ou da LAN corporativa é proibida pela lei ou por políticas de segurança corporativas.

  Você pode definir configurações de acesso da Kaspersky Private Security Network na seção **Proxy da KSN** da janela de propriedades do Servidor de Administração.

O aplicativo solicita a você participar da KSN durante a execução do Assistente de início rápido. É possível iniciar ou parar de usar a KSN em qualquer momento durante o uso do aplicativo.

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração da KSN for atualizada, ela será exibida quando você atualizar uma versão do Servidor de Administração. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Se recusar, continuará usando a KSN de acordo com a versão Declaração KSN aceita anteriormente.

Quando a KSN é ativada, o Kaspersky Security Center Linux verifica se os servidores da KSN estão acessíveis para garantir que o nível de segurança seja mantido para os dispositivos gerenciados. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos.

Os dispositivos cliente gerenciados pelo Servidor de Administração interagem com a KSN por meio do servidor proxy da KSN. O servidor proxy da KSN fornece os seguintes recursos:

- Os dispositivos clientes podem enviar solicitações à KSN, obter informações da KSN e transferir informações à KSN mesmo que não tenham acesso direto à Internet.

- O servidor proxy KSN armazena em cache os dados processados, o que reduz a carga de trabalho no canal de saída e o período de tempo despendido para aguardar por informações solicitadas por um dispositivo cliente.

Você pode configurar o Servidor Proxy KSN na seção **Proxy da KSN** da janela Propriedades do Servidor de Administração.

Configurar o acesso à KSN

Você pode configurar o acesso à Kaspersky Security Network (KSN) nas propriedades do Servidor de Administração, na política do Servidor de Administração e no ponto de distribuição.

Para configurar o acesso do Servidor de Administração à KSN nas propriedades do Servidor de Administração:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Proxy da KSN**.

3. Defina o botão de alternância **Ativar proxy da KSN no Servidor de Administração** como Ativado.

   Se esta opção estiver habilitada, o servidor proxy KSN enviará dados à KSN para aumentar a eficiência dos componentes do Kaspersky Security Center e melhorar o desempenho dos aplicativos da Kaspersky. Os dados são enviados dos dispositivos cliente para a KSN de acordo com a política do Kaspersky Endpoint Security que estiver ativa naqueles dispositivos cliente. Caso o botão de alternância esteja desativado, nenhum dado será enviado à KSN do Servidor de Administração e de dispositivos clientes por meio do Kaspersky Security Center Linux. No entanto, os dispositivos cliente podem enviar dados para a KSN diretamente (evitando o Kaspersky Security Center Linux), de acordo com suas respectivas configurações. A política do Kaspersky Endpoint Security, ativa nos dispositivos cliente, determina quais dados serão enviados diretamente (evitando o Kaspersky Security Center Linux) pelos dispositivos para a KSN.

4. Selecione a Solução de infraestrutura da KSN.

   Na subseção **Participação na KSN**, execute uma das seguintes ações:

   - Se estiver usando a KSN Global, defina o botão de alternância **Usar a Kaspersky Security Network** como Ativado.

     Ao ativar esta opção, certifique-se de ler e aceitar os termos da Declaração da KSN.

   - Se estiver usando a KPSN, defina o botão de alternância **Usar a Kaspersky Private Security Network** como Ativado e clique no botão **Selecionar arquivo com config. de proxy da KSN** para carregar as configurações da KPSN (arquivos com as extensões .pkcs7 e .pem). Após as configurações serem baixadas, a interface exibe o nome do provedor e os contatos, assim como a data de criação do arquivo com as configurações da KPSN.

   Quando você define o botão de alternância **Usar a Kaspersky Private Security Network** como Ativado, é exibida uma mensagem com informações detalhadas sobre a KPSN.

   Os seguintes aplicativos da Kaspersky são compatíveis com a KPSN:

   - Kaspersky Security Center Linux
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   Caso a opção KPSN seja ativada no Kaspersky Security Center Linux, esses aplicativos receberão as informações sobre a compatibilidade com a KPSN. Na janela de configurações do aplicativo, na subseção **Kaspersky Security Network** da seção **Advanced Threat Protection**, as informações sobre o provedor da KSN selecionado são exibidas: KSN ou KPSN.

O Kaspersky Security Center Linux não enviará dados estatísticos para a Kaspersky Security Network caso a KPSN esteja configurada na seção **Proxy da KSN** da janela de propriedades do Servidor de Administração.

5. Se você tiver as configurações do servidor proxy configuradas nas propriedades do Servidor de Administração, mas sua arquitetura de rede exigir que você use a KPSN diretamente, ative a opção **Ignorar as configurações do servidor proxy ao se conectar com a KPSN**. Caso contrário, as solicitações dos aplicativos gerenciados não chegarão à KPSN.

6. Configure a conexão do Servidor de Administração ao serviço de proxy da KSN:

   - Em **Conexão**, para a **Porta TCP**, especifique o número da porta TCP que será usada para se conectar ao Servidor proxy da KSN. A porta padrão para conectar-se ao servidor proxy da KSN é 13111.

   - Se desejar que o Servidor de Administração seja conectado ao servidor proxy da KSN por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de porta para **Porta UDP**. Por padrão, esta opção está desativada e a porta TCP é usada. Se essa opção estiver ativada, a porta UDP padrão para se conectar ao servidor proxy da KSN será 15111.

   - Se quiser que o Servidor de Administração se conecte com o servidor proxy da KSN por meio de uma porta HTTPS, ative a opção **Usar HTTPS** e especifique um número de porta para **Porta HTTPS**. Por padrão, esta opção está desativada e a porta TCP é usada. Se essa opção estiver ativada, a porta HTTPS padrão para se conectar ao servidor proxy da KSN será 17111.

     Se você selecionar essa opção, ative o HTTPS em todos os pontos de distribuição que atuam como proxy da KSN. Isso evita a sobrecarga do proxy.

7. Ative o botão de alternância **Conectar Servidores de Administração secundários à KSN através do Servidor de Administração Principal**.

   Se esta opção estiver ativada, Servidores de Administração secundários usam o Servidor de Administração principal como servidor proxy KSN. Se esta opção estiver desativada, os Servidores de Administração secundários conectam-se à KSN por conta própria. Neste caso, os dispositivos gerenciados usam Servidores de Administração secundários como servidores proxy KSN.

   Os Servidores de Administração secundários usam o Servidor de Administração principal como servidor proxy se, no painel direito da seção **Proxy da KSN**, nas propriedades dos Servidores de Administração secundários, o botão de alternância **Ativar Proxy da KSN no Servidor de Administração** também estiver definido como Ativado.

8. Clique no botão **Salvar**.

As configurações de acesso à KSN são salvas.

Para configurar o acesso do Servidor de Administração à KSN por meio da política do Servidor de Administração:

1. No menu principal, vá para **Gerenciamento de ativos → Políticas**.

2. Selecione uma política do Servidor de Administração.

3. Na janela de propriedades aberta, clique na guia **Configurações do aplicativo**.

4. Selecione a seção **Proxy da KSN** e siga as etapas 3 a 8 das instruções acima.

As configurações de acesso à KSN são salvas.

Você também pode configurar o acesso ao ponto de distribuição à KSN, por exemplo, se quiser reduzir a carga no Servidor de Administração. O ponto de distribuição que atua como um servidor proxy da KSN envia solicitações da KSN de dispositivos gerenciados para a Kaspersky diretamente, sem usar o Servidor de Administração.

Para configurar o acesso dos pontos de distribuição ao Kaspersky Security Network (KSN):

1. Certifique-se de que o ponto de distribuição seja atribuído manualmente.

2. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

3. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

4. Clique no nome do ponto de distribuição para abrir a janela de propriedades da tarefa.

5. Na janela de propriedades do ponto de distribuição, na seção **Proxy da KSN**, ative a opção **Ativar o proxy da KSN no lado do ponto de distribuição** e, em seguida, ative a opção **Acessar a KSN Cloud/KPSN diretamente pela Internet**.

6. Clique em **OK**.

O ponto de distribuição atuará como um servidor proxy da KSN.

Observe que o ponto de distribuição não é compatível com a autenticação do dispositivo gerenciado com o uso do protocolo NTLM.

Ativação e desativação do uso da KSN

Para ativar o uso da KSN:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Proxy da KSN**.

3. Defina o botão de alternância **Ativar proxy da KSN no Servidor de Administração** como Ativado.

O servidor proxy KSN é ativado e envia dados para a KSN para aumentar a eficiência dos componentes do Kaspersky Next XDR Expert e melhorar o desempenho dos aplicativos Kaspersky.

1. Dependendo da solução de infraestrutura da KSN que estiver sendo usando, ative os botões de alternância correspondentes.

   - Se estiver usando a KSN Global, defina o botão de alternância **Usar a Kaspersky Security Network** como Ativado.

     O envio de dados à KSN agora está disponível. Ao ativar esta opção, não se esqueça de ler e aceitar os termos da Declaração da KSN.

   - Se estiver usando a KPSN, defina o botão de alternância **Usar a Kaspersky Private Security Network** como Ativado e clique no botão **Selecionar arquivo com config. de proxy da KSN** para carregar as configurações da KPSN (arquivos com as extensões .pkcs7 e .pem). Após as configurações serem baixadas, a interface exibe o nome do provedor e os contatos, assim como a data de criação do arquivo com as configurações da KPSN.

     Quando você define o botão de alternância **Usar a Kaspersky Private Security Network** como Ativado, é exibida uma mensagem com informações detalhadas sobre a KPSN.

2. Clique no botão **Salvar**.

Para desativar o uso da KSN:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Proxy da KSN**.

3. Defina o botão de alternância **Ativar o proxy da KSN no Servidor de Administração** como Desativado para desativar o serviço de Proxy da KSN.

4. Clique no botão **Salvar**.

Visualizando a Declaração da KSN aceita

Ao ativar o Kaspersky Security Network (KSN), você deve ler e aceitar a Declaração da KSN. Você pode ver a Declaração da KSN aceita a qualquer momento.

Para visualizar a declaração KSN aceita:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Proxy da KSN**.

3. Clique no link **Ver Declaração da Kaspersky Security Network**.

Na janela aberta, você pode ver o texto da Declaração KSN aceita.

Aceitando uma declaração da KSN atualizada

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração da KSN for atualizada, ela será exibida quando você atualizar uma versão do Servidor de Administração. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Caso a declaração seja recusada, o usuário continuará usando a KSN de acordo com a versão Declaração da KSN aceita anteriormente.

Depois de atualizar uma versão do Servidor de Administração, a Declaração da KSN atualizada será exibida automaticamente. Se você recusar a declaração da KSN atualizada, você poderá ainda vê-la e aceitá-la posteriormente.

Para visualizar e aceitar ou recusar uma Declaração da KSN atualizada:

1. Clique no link **Exibir notificações** no canto superior direito da janela do aplicativo principal.

   A janela **Notificações** se abre.

2. Clique no link **Ver a Declaração da KSN atualizada**.

   A janela **Atualização da Declaração da Kaspersky Security Network** se abre.

3. Leia a Declaração da KSN e, em seguida, decida-se clicando em um dos seguintes botões:

   - **Eu aceito a declaração da KSN atualizada**
   - **Usar KSN sob as condições da Declaração anterior**

   Dependendo da sua escolha, a KSN continuará funcionando de acordo com os termos da Declaração da KSN em vigor ou atualizada. Você pode ver o texto da Declaração da KSN aceita nas propriedades do Servidor de Administração a qualquer momento.

Verificar se o ponto de distribuição funciona como servidor proxy da KSN

Em um dispositivo gerenciado atribuído como ponto de distribuição, é possível ativar o Proxy da Kaspersky Security Network (KSN). Um dispositivo gerenciado funciona como servidor proxy da KSN quando o serviço ksnproxy está sendo executado no dispositivo. É possível verificar, ativar ou desativar esse serviço localmente no dispositivo.

Você pode atribuir um dispositivo baseado em Windows ou Linux como um ponto de distribuição. O método de verificação do ponto de distribuição depende de seu sistema operacional.

Para verificar se o ponto de distribuição baseado em Linux funciona como servidor proxy da KSN:

1. No dispositivo de ponto de distribuição, execute o comando `ps aux` para exibir a lista de processos em execução.

2. Na lista de processos em execução, verifique se o processo `/opt/kaspersky/klnagent64/sbin/ksnproxy` está em execução.

Caso o processo `/opt/kaspersky/klnagent64/sbin/ksnproxy` esteja em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Para verificar se o ponto de distribuição baseado em Windows funciona como servidor proxy da KSN:

1. No dispositivo de ponto de distribuição, no Windows, abra **Serviços** (**Todos os programas** → **Ferramentas administrativas** → **Serviços**).

2. Na lista de serviços, verifique se o serviço ksnproxy está sendo executado.

   Se o serviço ksnproxy estiver em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Se desejar, você pode desativar o serviço ksnproxy. Nesse caso, o Agente de Rede no ponto de distribuição para de participar da Kaspersky Security Network. Isso requer direitos de administrador local.

Visualização das estatísticas do servidor proxy da KSN

O Kaspersky Security Center Web Console permite visualizar as estatísticas de uso do servidor proxy da KSN.

As estatísticas incluem os seguintes parâmetros:

- Status da conexão com a KSN
- Número de registros de cache
- Número de pacotes processados no cache
- Número de pacotes recebidos

Se você usar a KPSN como uma solução de infraestrutura, as estatísticas de uso da KPSN serão exibidas.

Para visualizar as estatísticas:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Proxy da KSN** e abra a guia **Estatísticas**.

   Esta guia exibe as estatísticas reais de uso do servidor proxy da KSN. As estatísticas são atualizadas a cada 15 segundos.

Você pode copiá-las clicando no botão **Copiar para transferência**.

Tarefas de gerenciamento

Esta seção descreve as tarefas utilizadas pelo Kaspersky Security Center Linux.

Sobre as tarefas

O Kaspersky Security Center Linux gerencia os aplicativos de segurança da Kaspersky instalados nos dispositivos cliente criando e executando *tarefas*. As tarefas são necessárias para a instalação, inicialização e interrupção de aplicativos, verificação de arquivos, atualização de bancos de dados e módulos de software e para a realização de outras ações em aplicativos.

As tarefas de um aplicativo específico podem ser criadas usando o Kaspersky Security Center Web Console apenas se o plugin de gerenciamento desse aplicativo estiver instalado no Kaspersky Security Center Web Console Server.

As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

As tarefas executadas no Servidor de Administração incluem o seguinte:

- Distribuição automática de relatórios
- Download de atualizações para o repositório
- Backup de dados do Servidor de Administração
- Manutenção do banco de dados

Os seguintes tipos de tarefas são executados nos dispositivos:

- *Tarefas locais* – Tarefas que são executadas em um dispositivo específico

  As tarefas locais podem ser modificadas pelo administrador por meio do uso do Kaspersky Security Center Web Console ou pelo usuário de um dispositivo remoto (por exemplo, por meio da interface do aplicativo de segurança). Se uma tarefa local tiver sido modificada simultaneamente pelo administrador e pelo usuário de um dispositivo gerenciado, as modificações feitas pelo administrador entrarão em vigor porque elas têm uma maior prioridade.

- *Tarefas de grupo* – Tarefas que são executadas em todos os dispositivos de um grupo específico

  Salvo de especificado de outra maneira nas propriedades de tarefa, uma tarefa de grupo também afeta todos os subgrupos do grupo selecionado. Uma tarefa de grupo também afeta (opcionalmente) os dispositivos que foram conectados aos Servidores de Administração secundários e virtuais implementados no grupo ou em algum dos seus subgrupos.

- *Tarefas globais* – Tarefas que são realizadas em um conjunto de dispositivos, independentemente se os mesmos estão incluídos em qualquer grupo

Para cada aplicativo, você pode criar qualquer número de tarefas de grupo, tarefas globais ou tarefas locais.

Você pode efetuar alterações nas configurações de tarefas, exibir o andamento das tarefas, copiar, exportar, importar e excluir tarefas.

Uma tarefa é iniciada em um dispositivo cliente somente se um aplicativo para o qual a tarefa foi criada estiver sendo executado.

Os resultados da execução das tarefas no log de eventos do sistema operacional em cada dispositivo, no log de eventos do sistema operacional: do Servidor de Administração e no banco de dados do Servidor de Administração.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Sobre o escopo de tarefa

O *escopo de uma tarefa* é o conjunto de dispositivos nos quais a tarefa é executada. Os tipos de escopo são os seguintes:

- Para uma *tarefa local*, o escopo é o próprio dispositivo.
- Para uma tarefa do *Servidor de Administração*, o escopo é o Servidor de Administração.
- Para uma *tarefa de grupo*, o escopo é a lista de dispositivos incluídos no grupo.

Ao criar uma *tarefa global*, você pode usar os seguintes métodos para especificar o escopo:

- Especificar determinados dispositivos manualmente.

  Você pode usar um endereço IP (ou uma faixa IP) ou nome DNS como o endereço do dispositivo. Também é possível selecionar dispositivos na rede detectados pelo Servidor de Administração.

- Importar uma lista de dispositivos de um arquivo .txt com os endereços dos dispositivos a serem adicionados (cada endereço deve ser colocado em uma linha individual).

  Se você importar uma lista de dispositivos a partir de um arquivo ou cria uma lista manualmente, e se os dispositivos cliente estão identificados pelos seus nomes, a lista deve conter somente os dispositivos cuja informação já foi adicionada ao banco de dados do Servidor de Administração. Além disso, as informações devem ter sido inseridas quando os dispositivos foram conectados ou durante a descoberta de dispositivos.

- Especificar uma seleção de dispositivos.

  Ao longo do tempo, o escopo de uma tarefa se modifica quando o conjunto de dispositivos incluídos na seleção são modificados. Uma seleção de dispositivos pode ser feita com base nos atributos do dispositivo, incluindo o software instalado em um dispositivo, e com base em tags atribuídas aos dispositivos. A seleção de dispositivos é o modo mais flexível para especificar o escopo de uma tarefa.

  As tarefas para seleções de dispositivos sempre são executadas de acordo com um agendamento pelo Servidor de Administração. Estas tarefas não podem ser executadas em dispositivos que não tenham uma conexão com o Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas diretamente nos dispositivos e, por isso, não dependem da conexão do dispositivo com o Servidor de Administração.

  As tarefas para Seleções de dispositivos não são executadas na hora local de um dispositivo; em vez disso, elas serão executadas na hora local do Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas na hora local de um dispositivo.

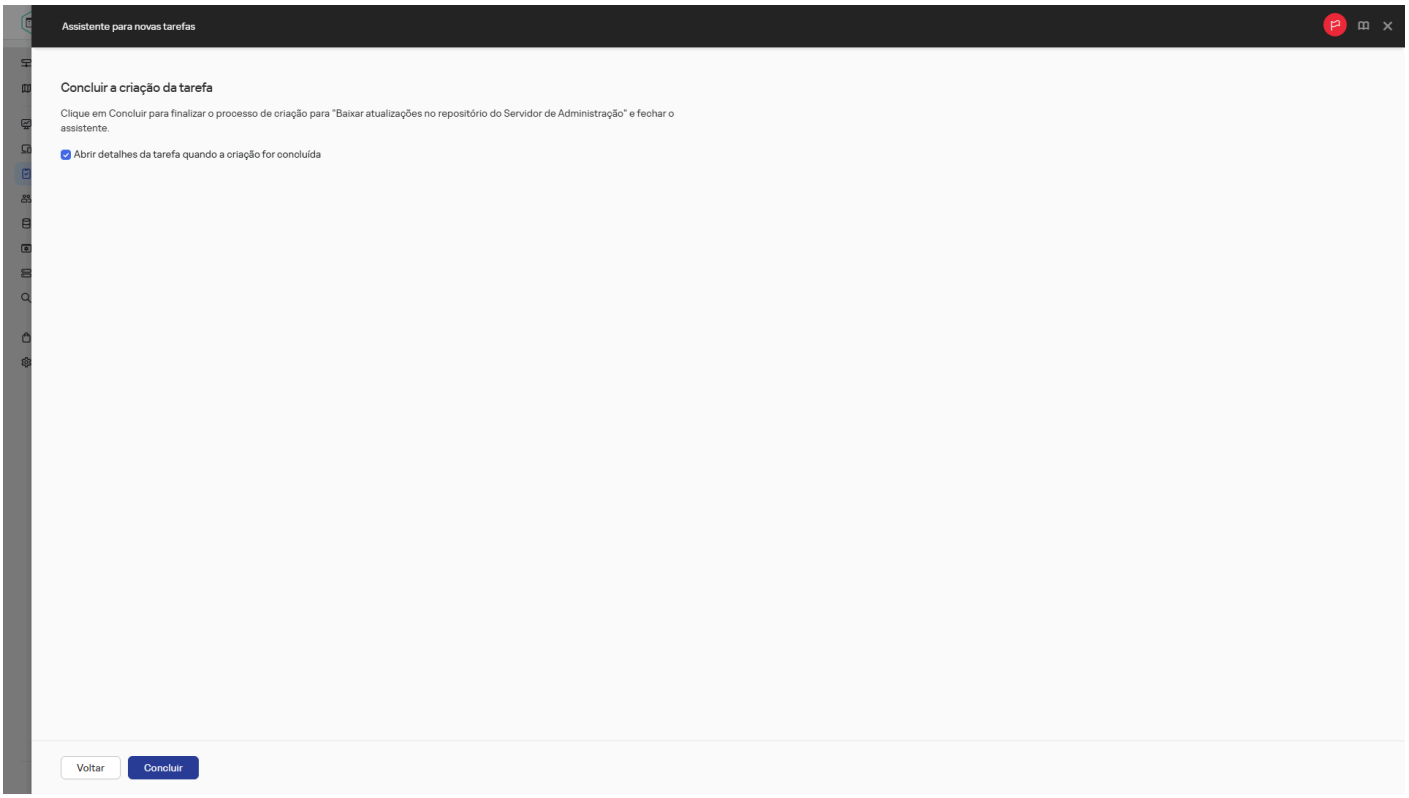
Criar uma tarefa

Para criar uma tarefa:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as instruções.
3. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode alterar as configurações padrão depois, a qualquer momento.
4. Clique no botão **Concluir**.

A tarefa é criada e exibida na lista de tarefas.



Finalização da criação da tarefa

Para criar uma nova tarefa atribuída aos dispositivos selecionados:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.
2. Na lista de dispositivos gerenciados, marque as caixas de seleção ao lado dos dispositivos para executar a tarefa para eles. Você pode usar as funções de pesquisa e filtro para encontrar os dispositivos que está procurando.
3. Clique no botão **Executar a tarefa** e selecione **Adicionar uma nova tarefa**.

O Assistente para novas tarefas inicia.

Na primeira etapa do assistente, você pode remover os dispositivos selecionados para incluir no escopo da tarefa. Siga as instruções do assistente.

4. Clique no botão **Concluir**.

A tarefa é criada para os dispositivos selecionados.

Como iniciar uma tarefa manualmente

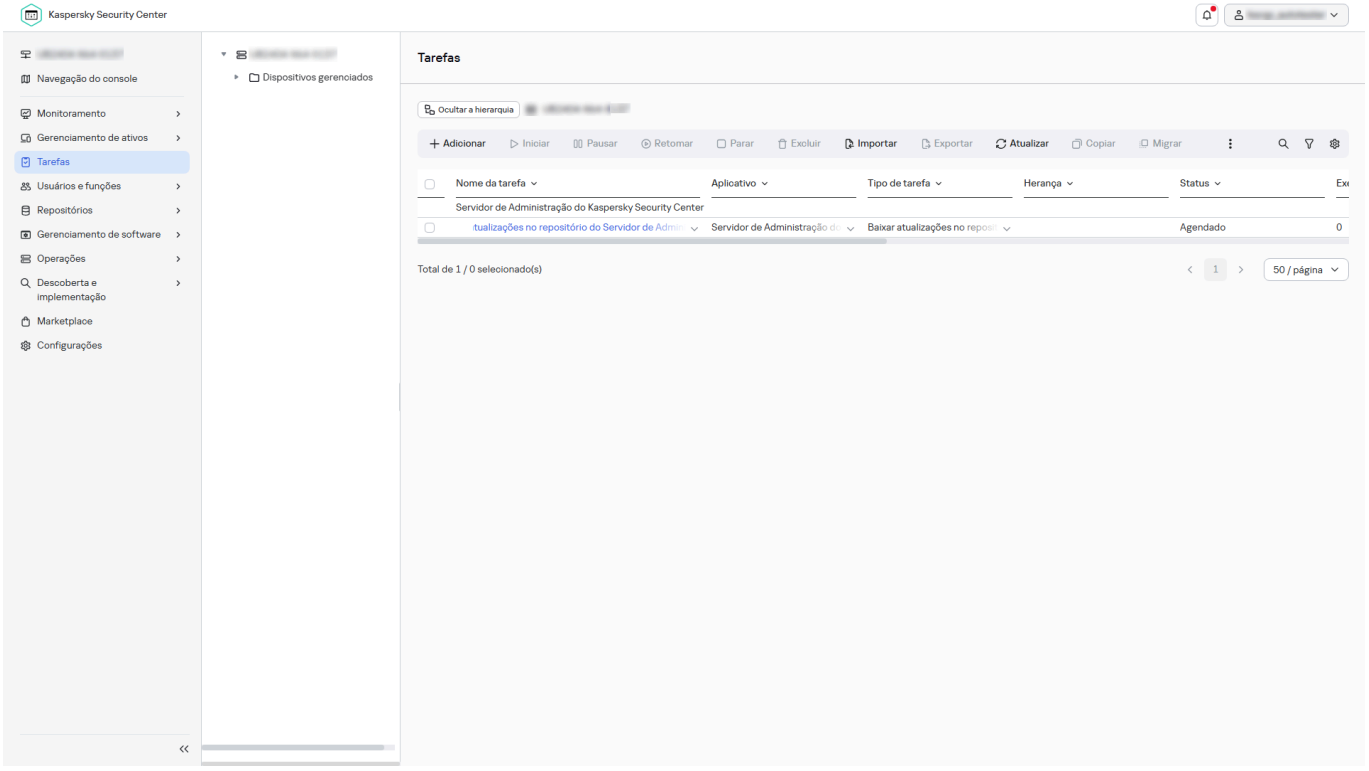
O aplicativo inicia as tarefas de acordo com as configurações de agendamento especificadas nas propriedades de cada tarefa. Você pode iniciar uma tarefa manualmente a qualquer momento por meio da lista de tarefas. Você também pode selecionar dispositivos na lista **Dispositivos gerenciados** e, em seguida, iniciar uma tarefa existente para eles.

Para iniciar uma tarefa manualmente:

1. No menu principal, vá para **Tarefas**.

2. Na lista de tarefas, selecione a caixa de seleção ao lado da tarefa que deseja iniciar.

3. Clique no botão **Iniciar**.



Iniciação de uma tarefa por meio da lista de tarefas

A tarefa é iniciada. Você pode verificar o status da tarefa na coluna **Status** ou clicando no botão **Resultado**.

Como iniciar uma tarefa para dispositivos selecionados

Você pode selecionar um ou mais dispositivos cliente na lista de dispositivos e iniciar uma tarefa criada anteriormente para eles. Isso permite executar tarefas criadas anteriormente para um conjunto específico de dispositivos.

Isso altera os dispositivos aos quais a tarefa foi atribuída para a lista de dispositivos que você seleciona ao executar a tarefa.
O escopo da tarefa anterior é excluído e substituído pelo escopo selecionado.

Para iniciar uma tarefa para dispositivos selecionados:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**. A lista de dispositivos gerenciados é exibida.
2. Na lista de dispositivos gerenciados, marque as caixas de seleção dos dispositivos para os quais você deseja executar a tarefa. Você pode usar as funções de pesquisa e filtro para encontrar os dispositivos que está procurando.
3. Clique no botão **Executar tarefa** e selecione **Usar a tarefa existente**.

   A lista de tarefas existentes é exibida.
4. Os dispositivos selecionados são exibidos acima da lista de tarefas. Se necessário, é possível remover um dispositivo dessa lista. Você pode excluir todos os dispositivos, exceto um.
5. Selecione a tarefa desejada na lista. Use a caixa de pesquisa acima da lista para pesquisar a tarefa desejada pelo nome. Apenas uma tarefa pode ser selecionada.
6. Salve as alterações clicando em um dos botões:

   - **Executar e fechar**

     A tarefa é executada para os dispositivos selecionados.

   - **Executar e abrir**

     A tarefa é executada para os dispositivos selecionados, e a janela de propriedades da tarefa é exibida. Nela, você pode consultar rapidamente os resultados da tarefa.

As configurações de início agendado na tarefa não são alteradas.

Visualizando a lista de tarefas

Você pode ver a lista de tarefas criadas no Kaspersky Security Center Linux.

Para visualizar a lista de tarefas,

No menu principal, vá para **Tarefas**.

A lista de tarefas é exibida. As tarefas são agrupadas pelos nomes dos aplicativos aos quais estão relacionados. Por exemplo, a tarefa *Instalar o aplicativo remotamente* está relacionada ao Servidor de Administração e a tarefa *Atualizar*, ao Kaspersky Endpoint Security.

Para visualizar as propriedades de uma tarefa,

Clique no nome da tarefa.

A janela de propriedades da tarefa é exibida com várias guias nomeadas. Por exemplo, **Tipo de tarefa** é exibido na guia **Geral** e o agendamento de tarefas - na guia **Agendamento**.

Configurações de tarefa gerais

Esta seção contém as configurações que podem ser definidas e especificadas para a maioria das tarefas. A lista de configurações disponíveis depende da tarefa que se está configurando.

Configurações especificadas durante a criação de tarefa

Você pode especificar as seguintes configurações ao criar uma tarefa. Algumas dessas configurações também podem ser modificadas nas propriedades da tarefa criada.

- Configurações para reiniciar o sistema operacional:

  Não reiniciar o dispositivo

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

  Reiniciar o dispositivo

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

  Forçar fechamento de aplicativos em sessões bloqueadas

  A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

  Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

  Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

  Por padrão, esta opção está desativada.

- Configurações de agendamento de tarefas:

Os tipos de agendamento podem variar dependendo da tarefa.

Alguns tipos de programação podem estar indisponíveis para outros aplicativos da Kaspersky.

- **Configuração Iniciar tarefa:**

  A cada N horas

  A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

  Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  A cada N dias

  A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

  Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  A cada N minutos

  A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

  Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  Por dias da semana

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

  Mensalmente

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

  Manualmente

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

  Uma vez

  A tarefa é executada uma vez, na data e hora especificadas (por padrão, no dia em que a tarefa foi criada).

  Imediatamente

  A tarefa é executada imediatamente após suas configurações serem salvas.

  Mensalmente em um dia da semana selecionado

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

Por padrão, a hora de início é 18:00 e nenhum dia do mês é selecionado.

> Observe que você não seleciona uma data específica no mês, nem o número da semana (primeira, segunda semana do mês), mas o número de sequência do dia da semana dentro de um mês. Por exemplo, se definir o cursor na célula **Ter** da **Primeiro(a)** linha, a tarefa será executada toda primeira terça-feira de cada novo mês.

É possível selecionar vários dias da semana.

Quando novas atualizações são baixadas no repositório

A tarefa é executada após as atualizações serem baixadas no repositório. Por exemplo, pode ser necessário usar esse agendamento para a tarefa *Atualizar*.

Na conclusão de outra tarefa

A tarefa atual inicia após outra tarefa ser concluída. Esta opção só funciona se ambas as tarefas estiverem atribuídas aos mesmos dispositivos. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus* com um tarefa de acionamento.

É necessário selecionar a tarefa de acionamento na tabela e o status com o qual a tarefa deve ser concluída (**Conclusão com êxito** ou **Falhou**).

Caso seja necessário, é possível pesquisar, classificar e filtrar as tarefas na tabela da seguinte maneira:

- Insira o nome da tarefa no campo de pesquisa para pesquisar a tarefa pelo nome.
- Clique no ícone de classificação para classificar as tarefas por nome.

  Por padrão, as tarefas são classificadas em ordem alfabética crescente.
- Clique no ícone de filtragem e, na janela exibida, filtre as tarefas por grupo e clique no botão **Aplicar**.

Se você estiver criando uma tarefa para um aplicativo gerenciado e o agendamento da tarefa puder ser pausado, essa tarefa terá as seguintes configurações de agendamento:

- **Hora de término**

  O agendamento da tarefa é interrompido à meia-noite da data especificada. Se a tarefa ainda estiver em execução quando chegar a hora de término do agendamento, ela não será encerrada.

  Por exemplo, suponha que uma tarefa seja executada às 23h todos os dias. Você especifica que o agendamento dessa tarefa será encerrado em 1º de janeiro. Em 31 de dezembro, a tarefa é iniciada às 23h e, à meia-noite de 1º de janeiro, seu agendamento é interrompido: a tarefa continua em execução até ser concluída e, após as 23h de 1º de janeiro, o agendamento não aciona mais a tarefa.

  Esta opção está disponível para todos os tipos de agendamento, exceto **Manualmente** e **Uma vez**.
- **Pausar tarefa**

  Se esta configuração estiver ativada, você poderá especificar um intervalo durante o qual uma tarefa iniciada anteriormente conforme o agendamento deverá ser pausada. Por exemplo, das 10h às 11h.

  Isso pode ser necessário durante períodos de pico de uso do dispositivo para reduzir o impacto do aplicativo gerenciado (por exemplo, o Kaspersky Endpoint Security) no desempenho.

  Esta opção está disponível para todos os tipos de agendamento.

- **Executar tarefas ignoradas**

  Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

  Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

  Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

  Por padrão, esta opção está ativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

  Por padrão, esta opção está ativada.

- **Usar atraso aleatório automaticamente para início de tarefa em um intervalo de**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

- Dispositivos aos quais a tarefa será atribuída:

  Selecionar os dispositivos na rede detectados pelo Servidor de Administração

  A tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

  Por exemplo, pode ser necessário usar esta opção em uma tarefa de instalação do Agente de Rede em dispositivos não atribuídos.

  Especificar os endereços do dispositivo manualmente ou importar os endereços da lista

  Você pode especificar nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

  Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

Atribuir a tarefa a uma seleção de dispositivos

A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

Atribuir uma tarefa a um grupo de administração

A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

- Configurações de conta:

  Conta padrão

  A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

  Por padrão, esta opção está selecionada.

  Especificar uma conta

  Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

  Login.

  Conta sob a qual a tarefa é executada.

  Senha

  Senha da conta sob a qual a tarefa será executada.

Configurações especificadas após a criação da tarefa

Você pode especificar as seguintes configurações após criar uma tarefa.

- Configurações de tarefa de grupo:

  Distribuir para subgrupos

  Essa opção só está disponível nas configurações das tarefas de grupo.

  Quando essa opção está habilitada, o escopo da tarefa inclui:

  - O grupo de administração selecionado ao criar a tarefa.
  - Os grupos de administração subordinados ao grupo de administração selecionado em qualquer nível abaixo da hierarquia do grupo.

  Quando essa opção está desabilitada, o escopo da tarefa inclui apenas o grupo de administração selecionado ao criar a tarefa.

  Por padrão, esta opção está ativada.

Distribuir em Servidores de Administração secundários e virtuais

Quando essa opção está habilitada, a tarefa efetiva no Servidor de Administração principal também é aplicada nos Servidores de Administração secundários (incluindo os virtuais). Caso já exista uma tarefa do mesmo tipo no Servidor de Administração secundário, ambas as tarefas serão aplicadas no Servidor de Administração secundário (a existente e a herdada do Servidor de Administração principal).

Essa opção só está disponível quando a opção **Distribuir para subgrupos** está habilitada.

Por padrão, esta opção está desativada.

- Configurações de agendamento avançado:

  Ligar dispositivos usando a função Wake-On-LAN antes de iniciar a tarefa

  O sistema operacional do dispositivo selecionado inicia na hora especificada, antes do início da tarefa. O período de tempo padrão é de cinco minutos.

  Ative esta opção se você quiser que a tarefa seja executada em todos os dispositivos clientes do escopo da tarefa, inclusive nos dispositivos que são desligados quando a tarefa está prestes a ser iniciada.

  Se você quiser que o dispositivo seja desativado automaticamente após a conclusão da tarefa, ative a opção **Desligar os dispositivos após concluir a tarefa**. Esta opção pode ser encontrada na mesma janela.

  Por padrão, esta opção está desativada.

  Desligar os dispositivos após concluir a tarefa

  Por exemplo, pode ser necessário ativar esta opção para uma tarefa que instala atualizações nos dispositivos clientes todas as sextas-feiras após o horário comercial e, em seguida, desliga esses dispositivos durante o fim de semana.

  Por padrão, esta opção está desativada.

  Interromper a tarefa se ela durar mais do que

  Após o final do período especificado, a tarefa é interrompida automaticamente, quer tenha sido concluída ou não.

  Ative esta opção se você quiser interromper (ou parar) tarefas que levam muito tempo para serem executadas.

  Por padrão, esta opção está desativada. O tempo predefinido de execução da tarefa é de 120 minutos.

- Configurações de notificação:

  - Bloco **Armazenar histórico de tarefas**:

    Armazenar no banco de dados do Servidor de Administração por (dias)

    Os eventos de aplicativo relacionados à execução da tarefa em todos os dispositivos clientes do escopo da tarefa são armazenados no Servidor de Administração durante o número de dias especificado. Quando esse período termina, as informações são excluídas do Servidor de Administração.

    Por padrão, esta opção está ativada.

    Armazenar no log de eventos do SO no dispositivo

    Os eventos de aplicativo relacionados à execução da tarefa são armazenados localmente no Log de Eventos do Syslog de cada dispositivo cliente.

    Por padrão, esta opção está desativada.

    Armazenar no log de eventos do SO no Servidor de Administração

Os eventos de aplicativo relacionados à execução da tarefa em todos os dispositivos clientes do escopo da tarefa são armazenados centralmente no Log de Eventos do Syslog do sistema operacional (SO) do Servidor de Administração.

Por padrão, esta opção está desativada.

Salvar todos os eventos

Se esta opção estiver selecionada, todos os eventos relacionados à tarefa serão salvos nos logs de eventos.

Salvar eventos relacionados ao progresso da tarefa

Se esta opção estiver selecionada, apenas os eventos relacionados à execução da tarefa serão salvos nos logs de eventos.

Salvar apenas os resultados da execução da tarefa

Se esta opção estiver selecionada, apenas os eventos relacionados aos resultados da tarefa serão salvos nos logs de eventos.

- **Notify administrator of task execution results**

  Você pode selecionar os métodos pelos quais os administradores recebem notificações sobre os resultados de execução da tarefa: por e-mail, por SMS e pela execução de um arquivo executável. Para configurar a notificação, clique em link **Configurações**.

  Por padrão, todos os métodos de notificação estão desativados.

- **Notificar somente erros**

  Se esta opção estiver ativada, os administradores serão notificados apenas quando uma execução de tarefa for concluída com um erro.

  Se esta opção estiver desativada, os administradores serão notificados após cada conclusão de execução de tarefa.

  Por padrão, esta opção está ativada.

- Configurações de segurança.

- Configurações do escopo da tarefa.

  Dependendo de como o escopo da tarefa é determinado, as seguintes configurações estão presentes:

  Dispositivos

  Se o escopo de uma tarefa for determinado por um grupo de administração, você pode exibir visualizar esse grupo. Nenhuma alteração está disponível nesse ponto. No entanto, você pode definir **Exclusões do escopo da tarefa**.

  Se o escopo de uma tarefa for determinado por uma lista de dispositivos, você pode alterar essa lista adicionando e removendo dispositivos.

  Seleção de dispositivos

  Você pode alterar a seleção de dispositivos aos quais a tarefa é aplicada.

  Exclusões do escopo da tarefa

Você pode especificar grupos de dispositivos aos quais a tarefa não é aplicada. Os grupos a serem excluídos podem somente ser subgrupos do grupo de administração ao qual a tarefa é aplicada.

- **Histórico de revisão**.

Exportação de tarefa

O Kaspersky Security Center Linux permite salvar uma tarefa e suas configurações em um arquivo KLT. Você pode usar este arquivo KLT para importar a tarefa salva tanto para o Kaspersky Security Center Windows quanto para o Kaspersky Security Center Linux.

Para exportar uma tarefa:

1. No menu principal, vá para **Tarefas**.
2. Marque a caixa de seleção ao lado da tarefa que deseja exportar.

   Você não pode exportar várias tarefas ao mesmo tempo. Se selecionar mais de uma tarefa, o botão **Exportar** será desabilitado. As tarefas do Servidor de Administração também ficam indisponíveis para exportação.
3. Clique no botão **Exportar**.
4. Na janela **Salvar como** que abrir, especifique o nome e o caminho do arquivo de tarefa. Clique no botão **Salvar**.

   A janela **Salvar como** é exibida apenas se você usar Google Chrome, Microsoft Edge ou Opera. Se usar outro navegador, o arquivo da tarefa será salvo automaticamente na pasta **Downloads**.

Importação de uma tarefa

O Kaspersky Security Center Linux permite importar uma tarefa de um arquivo KLT. O arquivo KLT contém a tarefa exportada e suas configurações.

Para a importação correta da tarefa do aplicativo Kaspersky, é necessário instalar o plug-in de gerenciamento adequado.

Para importar uma tarefa:

1. No menu principal, vá para **Tarefas**.
2. Clique no botão **Importar**.
3. Clique no botão **Procurar** para escolher um arquivo de tarefa que você deseja importar.
4. Na janela aberta, especifique o caminho para o arquivo de tarefa KLT e clique no botão **Abrir**. Observe que você pode selecionar apenas um arquivo de tarefa.

   O processamento da tarefa é iniciado.
5. Após o processamento com êxito da tarefa, selecione os dispositivos aos quais deseja atribuir a tarefa. Para fazer isso, selecione uma das seguintes opções:

   Atribuir tarefa a um grupo de administração

A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

Especificar endereços de dispositivos manualmente ou importar endereços de uma lista

Você pode especificar nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

Atribuir tarefa a uma seleção de dispositivos

A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

6. Especifique o escopo da tarefa.

7. Clique no botão **Concluir** para encerrar a importação da tarefa.

A notificação com os resultados da importação é exibida. Se a tarefa for importada com êxito, será possível clicar no link **Detalhes** para visualizar as propriedades da tarefa.

Após a importação com êxito, a tarefa será exibida na lista de tarefas. As configurações de tarefa e o agendamento também são importados. A tarefa será iniciada de acordo com seu agendamento.

Se a tarefa recém-importada tiver um nome idêntico a uma tarefa existente, o nome da tarefa importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Iniciar o Assistente para alterar a senha das tarefas

Para uma tarefa não local, você pode especificar uma conta na qual a tarefa deve ser executada. Você pode especificar a conta durante a criação da tarefa ou nas propriedades de uma tarefa existente. Se a conta especificada for usada de acordo com as instruções de segurança da organização, essas instruções poderão exigir a alteração periódica da senha da conta. Quando a senha da conta expirar e você definir uma nova, as tarefas não serão iniciadas até que você especifique a nova senha válida nas propriedades da tarefa.

O Assistente para alterar a senha das tarefas permite substituir automaticamente a senha antiga pela nova em todas as tarefas em que a conta esteja especificada. Como alternativa, você pode alterar esta senha manualmente nas propriedades de cada tarefa.

Para iniciar o Assistente para alterar a senha das tarefas:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Gerenciar as credenciais de contas para iniciar tarefas**.

Siga as etapas do Assistente.

Etapa 1. Especificar as credenciais

Especifique novas credenciais atualmente válidas em seu sistema. Quando o usuário passa para a próxima etapa do assistente, o Kaspersky Security Center Linux verifica se o nome da conta especificado corresponde ao nome da conta nas propriedades de cada tarefa não local. Se os nomes das contas corresponderem, a senha nas propriedades da tarefa será automaticamente substituída pela nova.

Para especificar a nova conta, selecione uma opção:

Usar a conta atual

O Assistente usa o nome da conta na qual você está conectado atualmente ao Kaspersky Security Center Web Console. Em seguida, especifique manualmente a senha da conta no campo **Senha atual para usar em tarefas**.

Especificar uma conta diferente

Especifique o nome da conta na qual as tarefas devem ser iniciadas. Em seguida, especifique a senha da conta no campo **Senha atual para usar em tarefas**.

Se o campo **Senha anterior (opcional; caso você deseje substituí-la pela atual)** for preenchido, o Kaspersky Security Center Linux substitui a senha apenas para as tarefas nas quais o nome da conta e a senha antiga são encontrados. A substituição é realizada automaticamente. Em todos os outros casos, você precisa escolher uma ação a ser executada na próxima etapa do Assistente.

Etapa 2. Selecionar uma ação a ser executada

Se você não especificou a senha antiga na primeira etapa do Assistente ou a senha antiga especificada não correspondeu às senhas nas propriedades da tarefa, deverá escolher uma ação a ser executada para as tarefas encontradas.

Para escolher uma ação para uma tarefa:

1. Marque a caixa de seleção ao lado da tarefa para a qual deseja escolher uma ação.
2. Execute uma das seguintes ações:

   - Para remover a senha nas propriedades da tarefa, clique em **Excluir as credenciais**.

     A tarefa é alternada para ser executada na conta padrão.

- Para substituir a senha por uma nova, clique em **Impor alteração da senha mesmo se a senha antiga esteja incorreta ou não foi fornecida**.
- Para cancelar a alteração da senha, clique em **Nenhuma ação está selecionada**.

As ações escolhidas são aplicadas depois que você passar para a próxima etapa do Assistente.

Etapa 3. Visualizar os resultados

Na última etapa do assistente, visualize os resultados para cada uma das tarefas encontradas. Para concluir o Assistente, pressione o botão **Concluir**.

Visualização de resultados da execução de tarefas armazenados no Servidor de Administração

O Kaspersky Security Center Linux permite visualizar resultados de execução para tarefas de grupo, tarefas para dispositivos específicos e tarefas do Servidor de Administração.

Para visualizar os resultados da tarefa:

Na janela de propriedades da tarefa, acesse a guia **Resultados**.

Para exibir os resultados da tarefa de um Servidor de Administração secundário:

1. Na janela de propriedades da tarefa, selecione a seção **Geral**.
2. Clique no link **Resultados** para abrir a janela **Resultados da tarefa**.
3. Clique em **Estatísticas de servidores secundários**.
4. Selecione o servidor secundário para o qual você deseja exibir a janela **Resultados da tarefa**.

Tags de aplicativo

Esta seção descreve as tags do aplicativo e fornece instruções para criá-los e modificá-los, bem como para aplicar tag em aplicativos de terceiros.

Tags de aplicativo

O Kaspersky Security Center Linux permite marcar os aplicativos pelo registro de aplicativos. Uma tag é o rótulo de um aplicativo que pode ser usada para agrupar ou encontrar dispositivos. Uma tag destinada a aplicativos pode servir como uma condição em seleções de dispositivos.

Por exemplo, você pode criar a tag `[Browsers]` e atribuí-la a todos os navegadores, como Microsoft Internet Explorer, Google Chrome, Mozilla Firefox etc.

Criando uma tag de aplicativo

Para criar um tag de aplicativo:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Tags de aplicativos**.
2. Clique em **Adicionar**.

   Uma nova janela de tag é exibida.
3. Insira o nome da tag.
4. Clique em **OK** para salvar as alterações.

A nova tag aparece na lista de tags de aplicativos.

Renomeando uma tag de aplicativo

Para renomear um identificador de aplicativos:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Tags de aplicativos**.
2. Marque a caixa de seleção ao lado do identificador que deseja renomear e clique em **Editar**.

   A janela de propriedades do identificador é exibida.
3. Altere o nome do identificador.
4. Clique em **OK** para salvar as alterações.

A tag atualizado aparece na lista de tags de aplicativos.

Atribuindo uma tag de aplicativos

Para atribuir uma ou várias tags a um aplicativo:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Registro de aplicativos**.
2. Clique no nome do aplicativo ao qual deseja atribuir tags.
3. Selecione a guia **Tags**.

   A guia exibe todos as tags de aplicativos existentes no Servidor de Administração. Para tags atribuídas ao aplicativo selecionado, a caixa de seleção na coluna **Tag atribuída** é selecionada.

4. Para as tags que deseja atribuir, marque as caixas de seleção na coluna **Tag atribuída**.
5. Clique em **Salvar** para salvar as alterações.

As tags são atribuídas ao aplicativo.

Removendo tags atribuídas de um aplicativo

Para remover uma ou várias tags de um aplicativo:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Registro de aplicativos**.
2. Clique no nome do aplicativo do qual deseja remover tags.
3. Selecione a guia **Tags**.

   A guia exibe todos as tags de aplicativos existentes no Servidor de Administração. Para tags atribuídas ao aplicativo selecionado, a caixa de seleção na coluna **Tag atribuída** é selecionada.
4. Para tags que deseja remover, desmarque as caixas de seleção na coluna **Tag atribuída**.
5. Clique em **Salvar** para salvar as alterações.

As tags são removidas do dispositivo.

> As tags de aplicativos removidas não são excluídas. Se quiser, você pode excluí-los manualmente.

Excluir uma tag de aplicativos

Para excluir um identificador de aplicativos:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Tags de aplicativos**.
2. Na lista, selecione o identificador de aplicativos que deseja excluir.
3. Em seguida, clique no botão **Excluir**.
4. Na janela que se abre, clique em **OK**.

O identificador de aplicativos é excluído. O identificador excluído é automaticamente removido de todos dos aplicativos aos quais foi atribuído.

Usando o utilitário klscflag para abrir a porta 13291

Você pode automatizar a operação do Kaspersky Security Center Linux usando o utilitário klakaut. O utilitário klakaut e seu sistema de Ajuda estão localizados na pasta de instalação do Kaspersky Security Center Linux. Se quiser usar o utilitário klakaut, abra a porta 13291 usando o utilitário klscflag.

O utilitário klscflag altera o valor do parâmetro KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Para abrir a porta 13291:

1. Execute o seguinte comando na linha de comando:
   ```
   /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
   KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
   \"SS_SETTINGS\";"
   ```

2. Reinicie o serviço do Servidor de Administração do Kaspersky Security Center executando o seguinte comando:
   ```
   sudo systemctl restart kladminserver_srv
   ```

   A porta 13291 está aberta.

Para verificar se a porta 13291 foi aberta com êxito:

Execute o seguinte comando na linha de comando:

```
/opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Este comando retorna o seguinte resultado:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

O valor `true` significa que a porta está aberta. Caso contrário, o valor `false` é exibido.

Registrar o aplicativo Kaspersky Industrial CyberSecurity for Networks no Kaspersky Security Center Web Console

Para começar a trabalhar com o aplicativo Kaspersky Industrial CyberSecurity for Networks por meio do Kaspersky Security Center Web Console, primeiro é necessário registrá-lo no Kaspersky Security Center Web Console.

Para registrar o aplicativo Kaspersky Industrial CyberSecurity for Networks:

1. Certifique-se de que o seguinte procedimento seja feito:

   - Ter baixado e instalado o plug-in da Web Kaspersky Industrial CyberSecurity for Networks.

     Você pode fazer isso mais tarde, enquanto aguarda a sincronização do Servidor Kaspersky Industrial CyberSecurity for Networks com o Servidor de Administração. Após baixar e instalar o plug-in, a seção **KICS for Networks** será exibida no menu principal do Kaspersky Security Center Web Console.

   - Na interface da Web do Kaspersky Industrial CyberSecurity for Networks, a interação com o Kaspersky Security Center Linux é configurada e ativada. Para saber mais detalhes, consulte a Ajuda do Kaspersky Industrial CyberSecurity for Networks.

2. Mova o dispositivo onde o Kaspersky Industrial CyberSecurity for Networks Server estiver instalado do grupo dispositivos não atribuídos para o grupo dispositivos gerenciados:

   a. No menu principal, vá para **Gerenciamento de ativos → Dispositivos não atribuídos**.

   b. Marque a caixa de seleção ao lado do dispositivo no qual o Kaspersky Industrial CyberSecurity for Networks Server está instalado.

   c. Clique no botão **Mover para o grupo**.

   d. Na hierarquia de grupos de administração, marque a caixa de seleção ao lado do grupo de **Dispositivos gerenciados**.

   e. Clique no botão **Mover**.

3. Abra a janela de propriedades do dispositivo no qual o Kaspersky Industrial CyberSecurity for Networks Server está instalado.

4. Na página de propriedades do dispositivo, na seção **Geral**, selecione a opção **Não desconectar do Servidor de Administração** e, em seguida, clique no botão **Salvar**.

5. Na página de propriedades do dispositivo, selecione a seção **Aplicativos**.

6. Na seção **Aplicativos**, selecione Agente de Rede do Kaspersky Security Center.

7. Caso o status atual do aplicativo seja *Interrompido*, espere até que mude para *Executando*.

   O processo leva até 15 minutos. Caso ainda não tenha instalado o plug-in da Web do Kaspersky Industrial CyberSecurity for Networks, é possível fazê-lo agora.

8. Caso queira visualizar as estatísticas do Kaspersky Industrial CyberSecurity for Networks, será possível adicionar os widgets no painel. Para adicionar os widgets, faça o seguinte:

   a. No menu principal, vá para **Monitoramento → Painel**.

   b. No painel, clique no botão **Adicionar ou restaurar widget da Web**.

   c. No widget do menu aberto, selecione **Outro**.

d. Selecione os widgets que deseja adicionar:

- Mapa de implementação do KICS for Networks
- Informações sobre o KICS for Networks Servers
- Eventos atualizados do KICS for Networks
- Dispositivos com problemas no KICS for Networks
- Eventos críticos no KICS for Networks
- Status no KICS for Networks

9. Para prosseguir para a interface da Web do Kaspersky Industrial CyberSecurity for Networks, faça o seguinte:

a. No menu principal, vá para **KICS for Networks** → **Pesquisar**.

b. Clique no botão **Encontrar eventos ou dispositivos**.

c. Na janela **Parâmetros de consulta** que é aberta, clique no campo **Servidor**.

d. Selecione o Kaspersky Industrial CyberSecurity for Networks Server na lista suspensa de servidores integrados com o Kaspersky Security Center Linux e clique no botão **Encontrar**.

e. Clique no link **Ir para o servidor** ao lado do nome do Kaspersky Industrial CyberSecurity for Networks Server.

A página de login do Kaspersky Industrial CyberSecurity for Networks é exibida.

Para fazer login na interface da Web do Kaspersky Industrial CyberSecurity for Networks, é necessário fornecer as credenciais da conta de usuário do aplicativo.

Gerenciamento de usuários e funções dos usuários

Esta seção descreve usuários e funções de usuário e fornece instruções para criá-los e modificá-los, atribuir funções e grupos a usuários e associar perfis de política a funções.

Sobre as contas de usuário

O Kaspersky Security Center Linux permite gerenciar as contas de usuário e grupos de segurança. O aplicativo é compatível com três tipos de contas:

- Contas dos funcionários da organização. O Servidor de Administração obtém dados das contas desses usuários de domínio ao fazer a sondagem da rede da organização.
- Contas de usuários locais. Contas locais em dispositivos gerenciados e em dispositivos em que o Servidor de Administração está instalado.
- Contas de usuários internos do Kaspersky Security Center Linux. É possível criar contas de usuários internos. As contas serão utilizadas apenas no Kaspersky Security Center Linux.

As contas de usuário locais e o grupo local kladmins no sistema operacional Linux não podem ser usados para acessar o Kaspersky Security Center Web Console no Kaspersky Security Center Linux. Ele só pode conter contas usadas para iniciar os serviços do Kaspersky Security Center Linux. Os funcionários da organização poderão usar suas contas de usuário para fazer login após configurar a autenticação do domínio.

Para exibir as tabelas de contas de usuário e grupos de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos**.
2. Selecione a guia **Usuários** ou **Grupos**.

A tabela de usuários ou grupos de segurança é aberta. Caso queira exibir a tabela apenas com os usuários ou grupos internos ou apenas com usuários ou grupos locais, defina os critérios de filtro **Tipo de conta** como **Interno** ou **Local**, respectivamente.

Se a tabela de usuários contiver mais de 50 mil usuários, somente os primeiros 50 mil serão exibidos e os restantes não serão exibidos.

Sobre as funções dos usuários

A *função de usuário* (também mencionada como uma *função*) é um objeto que contém um conjunto de direitos e privilégios. Uma função pode ser associada às configurações de aplicativos da Kaspersky instalados em um dispositivo de usuário. É possível atribuir uma função a um conjunto de usuários ou a um conjunto de grupos de segurança em qualquer nível na hierarquia de grupos de administração, Servidores de Administração, ou em nível de objetos específicos.

Caso gerencie dispositivos por meio de uma hierarquia de Servidores de Administração, a qual inclui Servidores de Administração virtuais, observe que é possível criar, modificar ou excluir as funções de usuário somente do Servidor de Administração físico. Em seguida, é possível propagar as funções de usuário para os Servidores de Administração secundários, incluindo os virtuais.

Você pode associar funções de usuário a perfis da política. Se uma função for atribuída a um usuário, esse usuário receberá as configurações de segurança necessárias para desempenhar suas funções profissionais.

Uma função de usuário pode ser associada a usuários de dispositivos em um grupo de administração específico.

Escopo da função do usuário

O *escopo da função do usuário* é uma combinação de usuários e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

Vantagem de usar funções

Uma vantagem de usar funções é que você não precisa especificar configurações de segurança para cada um dos dispositivos gerenciados ou cada um dos usuários separadamente. O número de usuários e dispositivos em uma empresa pode ser bastante grande, mas o número de descrições de cargos diferentes que necessitam de configurações de segurança diferentes é consideravelmente menor.

Diferenças do uso de perfis da política

Os perfis da política são as propriedades da política criada para cada aplicativo da Kaspersky separadamente. Uma função é associada a muitos perfis de política criados para aplicativos diferentes. Por isso, a função é um método da união de configurações para um determinado tipo de usuário em um lugar.

Configurar direitos de acesso aos recursos do aplicativo. Controle de acesso baseado em função

O Kaspersky Security Center Linux fornece meios de acesso baseado em função para os recursos do Kaspersky Security Center Linux e aplicativos gerenciados da Kaspersky.

Você pode configurar os direitos de acesso aos recursos do aplicativo para usuários do Kaspersky Security Center Linux de uma das seguintes maneiras:

- Configurando os direitos para cada usuário ou grupo de usuários individualmente.
- Criando funções de usuário padrão com um conjunto predefinido de direitos e atribuindo tais funções aos usuários dependendo do escopo de obrigações deles.

A aplicação de funções de usuário tem como objetivo simplificar e reduzir os procedimentos de rotina de configuração de direitos de acesso dos usuários aos recursos do aplicativo. Os direitos de acesso com em uma função são configurados de acordo com as tarefas "padrão" e o escopo de deveres do usuário.

As funções de usuários podem ter nomes que correspondem a suas finalidades respetivas. Você pode criar um número ilimitado de funções no aplicativo.

É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado ou criar novas funções e configurar os direitos necessários por conta própria.

Direitos de acesso aos recursos do aplicativo

A tabela abaixo mostra os recursos do Kaspersky Security Center Linux com os direitos de acesso para gerenciar as tarefas, relatórios e configurações associadas, bem como executar as ações do usuário associadas.

Para executar as ações do usuário listadas na tabela, o usuário deve ter o direito especificado ao lado da ação.

Os direitos de **Leitura**, **Gravação** e **Execução** são aplicáveis a qualquer tarefa, relatório ou configuração. Além desses direitos, o usuário deve ter o direito de **Executar operações nas seleções de dispositivos** para gerenciar tarefas, relatórios ou configurações nas seleções de dispositivos.

Todas as tarefas, relatórios, configurações e pacotes de instalação que estão faltando na tabela pertencem à área funcional **Recursos gerais: Funcionalidade básica**.

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Recursos gerais: **Gerenciamento de grupos de administração**	**Gravação**	• Adicionar dispositivo em um grupo de administração: **Gravação** • Excluir dispositivo a partir de um grupo de administração: **Gravação** • Adicionar um grupo de administração em outro grupo de administração: **Gravação** • Excluir um grupo de administração a partir de outro grupo de administração: **Gravação**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Recursos gerais: **Acessar objetos independentemente de suas ACLs**	**Ler**	Obter acesso de leitura a todos os objetos: **Leitura**	Nenhum	Nenhum	A área funcional **Recursos gerais: Acessar objetos independentemente de suas ACLs** destina-se a fins de auditoria. Uma permissão **Ler** nesta área funcional concede acesso total de **Ler** a todos os objetos. Recomendamos conceder esses direitos com cuidado e a um conjunto limitado de usuários que precisam deles para desempenhar suas funções oficiais. O acesso é concedido independentemente de outros direitos, mesmo se eles proibirem o acesso de leitura a objetos específicos.
Recursos gerais: **Funcionalidade básica**	• **Ler** • **Gravação** • **Execução** • **Executar operações nas seleções de dispositivos**	• Regras de migração de dispositivos (criar, modificar ou excluir) para o Servidor virtual: **Gravação**, **executar operações nas seleções de dispositivos** • Obter certificado personalizado do protocolo móvel (LWNGT): **Leitura** • Definir certificado personalizado do protocolo móvel (LWNGT): **Gravação** • Obter a lista de rede definida por NLA: **Ler** • Adicionar, modificar ou excluir a lista de rede definida por NLA: **Gravação** • Ver lista de controle de acesso de grupos: **Ler** • Exibir o log do sistema operacional: **Ler** • Visualize a chave de recuperação para restaurar o acesso a um disco rígido criptografado por BitLocker: **Executar**	• "Baixar atualizações no repositório do Servidor de Administração" • "Entregar relatórios" • "Distribuir pacote de instalação" • "Instalar aplicativos nos Servidores de Administração secundários remotamente"	• "Relatório do status de proteção" • "Relatório de ameaças" • "Relatório de dispositivos mais infectados" • "Relatório de status dos bancos de dados antivírus" • "Relatório de erros" • "Relatório de ataques de rede" • "Relatório resumido de aplicativos de proteção do sistema de e-mail instalados" • "Relatório resumido sobre aplicativos de proteção de estação de trabalho e do Windows Server" • "Relatório resumido de aplicativos de defesa de perímetro instalados" • "Relatório resumido dos tipos de aplicativos instalados" • "Relatório de usuários de dispositivos infectados"	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
				• "Relatório sobre problemas de segurança" • "Relatório de eventos" • "Relatório de atividade dos pontos de distribuição" • "Relatório de Servidores de Administração secundários" • "Relatório de eventos de Controle de Dispositivos" • "Relatório de vulnerabilidades" • "Relatório de aplicativos proibidos" • "Relatório de Controle da Web" • "Relatório de status da criptografia dos dispositivos gerenciados" • "Relatório de status da criptografia dos dispositivos de armazenamento em massa" • "Relatório de direitos de acesso aos dispositivos criptografados" • "Relatório de erros na criptografia de arquivos" • "Relatório de bloqueio de acesso aos arquivos criptografados" • "Relatório de permissões do usuário em vigor" • "Relatório de direitos"	
Recursos gerais: **Objetos excluídos**	• **Ler** • **Gravação**	• Ver os objetos excluídos na Lixeira: **Ler** • Excluir objetos a partir da lixeira: **Gravação**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Recursos gerais: **Processamento de eventos**	• **Excluir eventos** • **Editar configurações de notificação de eventos** • **Alterar configurações de log de eventos** • **Gravação**	• Alterar configurações de registro de eventos: **Editar configurações de log de eventos** • Alterar configurações de notificação de eventos: **Editar configurações de notificação de eventos** • Excluir eventos: **Excluir eventos**	Nenhum	Nenhum	Configurações: • O número máximo de eventos armazenados no banco de dados • Período para armazenar eventos dos dispositivos excluídos
Recursos gerais: **Operações no Servidor de Administração**	• **Ler** • **Gravação** • **Executar** • **Modificar ACLs de objetos** • **Executar operações nas seleções de dispositivos**	• Especificar as portas do Servidor de Administração para a conexão do agente de rede: **Gravação** • Especificar as portas do proxy de ativação iniciado no Servidor de Administração: **Gravação** • Especificar as portas do proxy de ativação para celular iniciado no Servidor de Administração: **Gravação** • Especificar as portas do Servidor Web para distribuição de pacotes independentes: **Gravação** • Especificar as portas do Servidor Web para distribuição de perfis MDM: **Gravação** • Especifique as portas SSL do Servidor de Administração para conexão via Web Console: **Gravação** • Especificar as portas do Servidor de Administração para conexão móvel: **Gravação** • Especificar o número máximo de eventos armazenados no banco de dados do Servidor de Administração: **Gravação**	• "Backup de dados do Servidor de Administração" • "Manutenção do banco de dados"	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
		• Especificar o número máximo de eventos que pode ser enviado pelo Servidor de Administração: **Gravação** • Especificar o período de tempo durante o qual os eventos podem ser enviados pelo Servidor de Administração: **Gravação**			
Recursos gerais: **Implementação de software da Kaspersky**	• **Gerenciar patches da Kaspersky** • **Ler** • **Gravação** • **Execução** • **Executar operações nas seleções de dispositivos**	Aprovar ou recusar a instalação do patch: **Gerenciar patches da Kaspersky**	Nenhum	• "Relatório de uso da chave de licença pelo Servidor de Administração virtual" • "Relatório de versões de software da Kaspersky" • "Relatório de aplicativos incompatíveis" • "Relatório de versões das atualizações dos módulos de software da Kaspersky" • "Relatório de implementação da proteção"	Pacote de instalação: "Kaspersky"
Recursos gerais: **Gerenciamento de chaves**	• **Exportar arquivo de chave** • **Gravação**	• Exportar arquivo de chave: **Exportar arquivo de chave** • Modificar as configurações de chave de licença do Servidor de Administração: **Gravação**	Nenhum	Nenhum	Nenhum
Recursos gerais: **gerenciamento de relatórios aplicado**	• **Ler** • **Gravação**	• Criar relatórios independentemente de suas ACLs: **Gravar** • Executar relatórios independentemente de suas ACLs: **Ler**	Nenhum	Nenhum	Nenhum
Recursos gerais: **Hierarquia de Servidores de Administração**	**Configurar uma hierarquia de Servidores de Administração**	• Registrar, atualizar ou excluir Servidores de Administração secundários: **Configurar a hierarquia de Servidores de Administração**	Nenhum	Nenhum	Nenhum
Recursos gerais: **Permissões do usuário**	**Modificar ACLs de objetos**	• Alterar as propriedades de "Segurança" de qualquer objeto: **Modificar ACLs de objetos** • Gerenciar funções de usuário:	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
		Modificar ACLs de objetos • Gerenciar usuários internos: **Alterar ACLs de objeto** • Gerenciar grupos de segurança: **Alterar ACLs de objeto** • Gerenciar codinomes: **Modificar ACLs de objetos**			
Recursos gerais: **Servidores de Administração Virtuais**	• **Gerenciar Servidores de Administração virtuais** • **Ler** • **Gravação** • **Execução** • **Executar operações nas seleções de dispositivos**	• Obter uma lista de Servidores de Administração virtuais: **Ler** • Obter informações sobre o Servidor de Administração virtual: **Ler** • Criar, atualizar ou excluir um Servidor de Administração virtual: **Gerenciar Servidores de Administração Virtuais** • Mover um Servidor de Administração virtual para outro grupo: **Gerenciar Servidores de Administração Virtuais** • Definir permissões de Servidor virtual de administração: **Gerenciar servidores de administração virtuais**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Recursos gerais: **Gerenciamento de Chaves de Criptografia**	**Gravação**	Importar as chaves de criptografia: **Gravação**	Nenhum	Nenhum	Nenhum
Gerenciamento de dispositivos móveis: **Geral**	• **Conectar novos dispositivos** • **Enviar somente comandos de informação a dispositivos móveis** • **Enviar comandos para dispositivos móveis** • **Gerenciar certificados** • **Leitura** • **Gravação**	• Obter dados de restauração do Serviço de gerenciamento de chaves: **Ler** • Excluir certificados de usuário: **Gerenciar certificados** • Obter a parte pública do certificado do usuário: **Ler** • Verificar se a infraestrutura da Chave Pública está ativada: **Ler** • Verificar a conta da infraestrutura da Chave Pública: **Ler** • Obter modelos de infraestrutura de Chave Pública: **Ler** • Obter modelos de infraestrutura de Chave Pública por certificado de uso estendido de chave: **Ler** • Verificar se o certificado de infraestrutura da chave pública foi revogado: **Ler** • Atualizar as configurações de emissão do certificado do usuário: **Gerenciar certificados** • Obter as configurações de emissão do certificado do usuário: **Ler** • Obter pacotes por nome e versão do produto: **Ler** • Definir ou cancelar certificado do usuário: **Gerenciar certificados** • Renovar certificado do usuário: **Gerenciar certificados** • Defina a tag de certificado do usuário: **Gerenciar certificados** • Executar a geração do pacote de instalação do MDM; cancelar a geração do pacote de instalação do MDM: **Conectar novos dispositivos**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Gerenciamento do sistema: **Conectividade**	• **Iniciar sessões RDP** • **Conectar-se a sessões RDP existentes** • **Iniciar tunelamento** • **Salvar arquivos de dispositivos na estação de trabalho do administrador** • **Ler** • **Gravação** • **Execução** • **Executar operações nas seleções de dispositivos**	• Criar sessão de compartilhamento de área de trabalho: **O direito de criar uma sessão de compartilhamento de área de trabalho** • Criar sessão RDP: **Conectar-se a sessões RDP existentes** • Criar túnel: **Iniciar o tunelamento** • Salvar lista de rede de conteúdo: **Salvar arquivos de dispositivos na estação de trabalho do administrador**	Nenhum	"Relatório de usuários dos dispositivos"	Nenhum
Gerenciamento de sistema: **Gerenciamento de patches e vulnerabilidades**	• **Ler** • **Gravação** • **Execução** • **Executar operações nas seleções de dispositivos**	• Ver propriedades de patch de terceiros: **Ler** • Alterar propriedades de patch de terceiros: **Gravação**	• "Corrigir vulnerabilidades" • "Instalar as atualizações necessárias e corrigir vulnerabilidades"	"Relatório de atualizações de software"	Nenhum
Gerenciamento do sistema: **Executar scripts remotamente**	• **Ler** • **Gravação** • **Execução** • **Executar operações nas seleções de dispositivos**	O usuário pode visualizar as propriedades da tarefa: **Leitura** O usuário pode criar, excluir ou modificar um pacote de instalação: **Gravação** O usuário pode executar uma tarefa: **Gravar**. Em dispositivos cliente Linux, os scripts são executados com privilégios de root. O usuário pode executar uma tarefa ou agendá-la para executar: **Executar** O usuário pode executar uma tarefa em uma seleção de dispositivos: **Executar operações em seleções de dispositivos**	"Executar scripts remotamente"	Nenhum	Nenhum

Funções de usuário predefinidas

As funções de usuário atribuídas aos usuários do Kaspersky Security Center Linux fornecem conjuntos de direitos de acesso aos recursos do aplicativo.

Os usuários criados em um servidor virtual não podem receber uma função no Servidor de Administração.

É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado ou criar novas funções. Ao criar uma nova função, defina o escopo da função e atribua direitos de acesso aos recursos da Kaspersky Security Center Linux. Algumas das funções de usuário predefinidas disponíveis no Kaspersky Security Center Linux podem ser associadas a cargos específicos, por exemplo, **Auditor**, **Técnico de segurança**, **Supervisor**. Os direitos de acesso dessas funções são pré-configurados de acordo com as tarefas padrão e o escopo das obrigações dos cargos associados. A tabela abaixo mostra como as funções podem ser associadas a cargos específicos.

Exemplos de funções para cargos específicos

Função	Comentário
Auditor	Permite realizar todas as operações de visualização e execução de qualquer tarefa em seleções de dispositivos conectados ao Servidor de Administração via Agente de Rede, com privilégios de administrador local (root no Linux). Recomendamos designar essa função com cautela, restrita a um grupo limitado de usuários que realmente necessitam dela para cumprir suas funções oficiais.
Supervisor	Permite a visualização de todas as operações; não permite outras operações. Você pode atribuir esta função a um diretor de segurança e a outros gerentes responsáveis pela segurança de TI em sua organização.
Diretor de segurança	Permite todas as operações de visualização, permite o gerenciamento de relatórios; concede permissões limitadas na área **Gerenciamento do sistema**: **Conectividade**. Você pode atribuir esta função a um diretor responsável pela segurança de TI em sua organização.

A tabela abaixo mostra os direitos de acesso atribuídos a cada função de usuário predefinida.

Direitos de acesso de funções de usuário predefinidas

Função	Descrição

Administrador do Servidor de Administração	Permite todas as operações nas seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Gerenciamento de chaves de criptografia**
	  • **Processamento de eventos**
	  • **Hierarquia de Servidores de Administração**
	  • **Servidores de Administração virtual**
	• **Gerenciamento do sistema**:
	  • **Conectividade**
	  • **Inventário de hardware**
	  • **Inventário de software**

Operador do Servidor de Administração	Concede os direitos de **Leitura** e **Execução** (quando aplicável) em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Gerenciamento de chaves de criptografia**
	  • **Servidores de Administração virtuais**
	• **Gerenciamento do sistema**:
	  • **Conectividade**
	  • **Inventário de hardware**
	  • **Inventário de software**

Auditor	Permite todas as operações nas seguintes áreas funcionais, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Objetos excluídos** • **Gerenciamento de relatórios aplicado** Você pode atribuir esta função a uma pessoa que realiza a auditoria da sua organização.

Função	Descrição

Administrador de instalação	Permite todas as operações nas seguintes áreas funcionais:
	• **Recursos gerais:**
	  • **Funcionalidade básica**
	  • **Implementação do aplicativo da Kaspersky**
	  • **Gerenciamento de chaves de licença**
	• **Gerenciamento do sistema:**
	  • **Implementação do sistema operacional**
	  • **Gerenciamento de patches e vulnerabilidades**
	  • **Instalação remota**
	  • **Inventário de software**
	Concede os direitos de **Ler** e **Executar** na área funcional **Recursos gerais: Servidores de Administração Virtuais**.

Operador de instalação	Concede os direitos de **Leitura** e **Execução** (quando aplicável) em todas as seguintes áreas funcionais:
	• **Recursos gerais:**
	  • **Funcionalidade básica**
	  • **Implementação de software da Kaspersky** (também concede o direito de **Gerenciar patches da Kaspersky** nesta área)
	  • **Servidores de Administração virtual**
	• **Gerenciamento do sistema:**
	  • **Implementação do sistema operacional**
	  • **Gerenciamento de patches e vulnerabilidades**
	  • **Instalação remota**
	  • **Inventário de software**

Administrador do Kaspersky Endpoint Security	Permite todas as operações nas seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • **Recursos gerais: Gerenciamento de chaves de criptografia** • Área do **Kaspersky Endpoint Security**, incluindo todos os recursos
Operador do Kaspersky Endpoint Security	Concede os direitos de **Leitura** e **Execução** (quando aplicável) em todas as seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • **Recursos gerais: Gerenciamento de chaves de criptografia** • Área do **Kaspersky Endpoint Security**, incluindo todos os recursos
Administrador geral	Permite todas as operações em áreas funcionais, *exceto* as seguintes áreas, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Gerenciamento de relatórios aplicado**

Operador Principal	Concede os direitos de **Leitura** e **Execução** (quando aplicável) em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Objetos excluídos**
	  • **Gerenciamento de chaves de criptografia**
	  • **Operações com o Servidor de Administração**
	  • **Tags de dispositivo**
	  • **Implementação do aplicativo da Kaspersky**
	  • **Integração de aplicativos**
	  • **Servidores de Administração virtual**
	• Área de **Gerenciamento de dispositivos móveis**, incluindo todos os recursos
	• Área de **Gerenciamento do sistema**, incluindo todos os recursos
	• Área do **Kaspersky Endpoint Security**, incluindo todos os recursos

Função	Descrição
Administrador do Gerenciamento de Dispositivos Móveis	Permite todas as operações nas seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • Área de **Gerenciamento de dispositivos móveis**, incluindo todos os recursos Concede o direito de **Exportar arquivo de chave** nos **Recursos gerais: Gerenciamento da chave de licença**. Concede o direito de **Ler** no **Gerenciamento do sistema: Gerenciamento de vulnerabilidades e patches**.
Operador do Gerenciamento de Dispositivos Móveis	Concede os direitos de **Ler** e **Executar** em **Recursos gerais: Funcionalidade básica**. Concede os direitos de **Ler** e **Enviar somente comandos de informações aos dispositivos móveis** no **Gerenciamento de dispositivos móveis**: • **Comum** • **Self Service Portal**
Diretor de segurança	Permite todas as operações nas seguintes áreas funcionais, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Gerenciamento de relatórios aplicado** Concede os seguintes direitos na área funcional **Gerenciamento do sistema: Conectividade**: **Ler**, **Gravar**, **Executar**, **Salvar arquivos de dispositivos na estação de trabalho do administrador** e **Executar operações em seleções de dispositivos**. Você pode atribuir esta função a um diretor responsável pela segurança de TI em sua organização.
Usuário do Self Service Portal	Permite todas as operações na área funcional **Gerenciamento de Dispositivos Móveis: Self Service Portal**.
Supervisor	Concede o direito de **Leitura** nas áreas funcionais **Recursos gerais**: **Acessar objetos independentemente de suas ACLs** e **Recursos gerais**: **Gerenciamento obrigatório de relatórios**. Você pode atribuir esta função a um diretor de segurança e a outros gerentes responsáveis pela segurança de TI em sua organização.
Administrador de gerenciamento de patches e vulnerabilidades	Permite todas as operações nas áreas funcionais **Recursos gerais**: **Funcionalidade básica** e **Gerenciamento do sistema** (incluindo todos os recursos, *exceto* o recurso **Executar scripts remotamente**).
Operador de gerenciamento de patches e vulnerabilidades	Concede os direitos de **Ler** e **Executar** (quando aplicável) nas áreas funcionais **Recursos gerais**: **Funcionalidade básica** e **Gerenciamento do sistema** (incluindo todos os recursos, *exceto* o recurso **Executar scripts remotamente**).

Atribuição de direitos de acesso a objetos específicos

Além de atribuir direitos de acesso no nível do servidor, é possível configurar o acesso a objetos específicos, por exemplo, a uma tarefa específica. O aplicativo permite especificar direitos de acesso aos seguintes tipos de objetos:

- Grupos de administração
- Tarefas
- Relatórios
- Seleções de dispositivos
- Seleções de eventos

Para atribuir direitos de acesso a um objeto específico:

1. Dependendo do tipo de objeto, no menu principal, vá para a seção correspondente:
   - **Gerenciamento de ativos → Hierarquia de grupos**
   - **Tarefas**

- **Monitoramento → Relatórios**
- **Gerenciamento de ativos → Seleções de dispositivos**
- **Monitoramento → Seleções de eventos**

2. Abra as propriedades do objeto para o qual deseja configurar os direitos de acesso.

   Para abrir a janela de propriedades de um grupo de administração ou de uma tarefa, clique no nome do objeto. As propriedades de outros objetos podem ser abertas usando o botão na barra de ferramentas.

3. Na janela de propriedades, abra a seção **Direitos de acesso**.

   A lista de usuários é aberta. Os usuários e grupos de segurança listados têm direitos de acesso ao objeto. Por padrão, se você usar uma hierarquia de grupos de administração ou Servidores, a lista e os direitos de acesso serão herdados do grupo de administração principal ou do Servidor principal.

4. Para poder modificar a lista, ative a opção **Usar permissões personalizadas**.

5. Configure os direitos de acesso:

   - Use os botões **Adicionar** e **Excluir** para modificar a lista.
   - Especifique os direitos de acesso para um usuário ou grupo de segurança. Execute uma das seguintes ações:
     - Caso queira especificar os direitos de acesso manualmente, selecione o usuário ou grupo de segurança, clique no botão **Direitos de acesso** e, em seguida, especifique os direitos de acesso.
     - Caso queira atribuir uma função de usuário ao usuário ou grupo de segurança, selecione o usuário ou grupo de segurança, clique no botão **Funções** e, em seguida, selecione a função a ser atribuída.

6. Clique no botão **Salvar**.

Os direitos de acesso ao objeto são configurados.

Atribuição de direitos de acesso a usuários e grupos de segurança

É possível conceder aos usuários e grupos de segurança direitos de acesso para usar diferentes recursos do Servidor de Administração, por exemplo, Kaspersky Endpoint Security for Linux.

Para atribuir direitos de acesso a um usuário ou grupo de segurança:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Direitos de acesso**, marque a caixa de seleção ao lado do nome do usuário ou do grupo de usuários ao qual os direitos serão atribuídos e clique no botão **Direitos de acesso**.

   Não é possível selecionar vários usuários ou grupos de segurança ao mesmo tempo. Caso mais de um item seja selecionado, o botão **Direitos de acesso** será desativado.

3. Configure o conjunto de direitos para o usuário ou grupo:

   a. Expanda o nó com recursos do Servidor de Administração ou outro aplicativo da Kaspersky.

   b. Marque a caixa de seleção **Permitir** ou **Negar** ao lado do recurso ou do direito de acesso desejado.

      Exemplo 1: marque a caixa de seleção **Allow** ao lado do nó **Application integration** para conceder todos os direitos de acesso disponíveis ao recurso Integração de aplicativos (**Read**, **Write** e **Execute**) para um usuário ou grupo.

      Exemplo 2: expanda o nó **Encryption key management** e marque a caixa de seleção **Allow** ao lado da permissão **Write** para conceder o direito de acesso de **Write** ao recurso de gerenciamento de chaves de criptografia para um usuário ou grupo.

4. Depois de configurar o conjunto de direitos de acesso, clique em **OK**.

O conjunto de direitos do usuário ou do grupo de usuários será configurado.

As permissões do Servidor de Administração (ou do grupo de administração) estão divididas nas seguintes áreas:

- Recursos gerais:
  - Gerenciamento de grupos de administração
  - Acessar objetos independentemente de suas ACLs
  - Funcionalidade básica
  - Objetos excluídos
  - Gerenciamento de chaves de criptografia
  - Processamento de eventos
  - Operações no Servidor de administração (somente na janela de propriedades do Servidor de Administração)
  - Tags de dispositivos
  - Implementação do aplicativo da Kaspersky
  - Gerenciamento de chaves de licença
  - Integração do aplicativo
  - Gerenciamento de relatórios forçado
  - Hierarquia de Servidores de Administração
  - Permissões do usuário
  - Servidores de Administração virtuais

- Gerenciamento de Dispositivos Móveis:
  - Geral
  - Self Service Portal
- Gerenciamento do sistema:
  - Conectividade
  - Executar scripts remotamente
  - Inventário de hardware
  - Controle de Acesso de Rede
  - Implementação do SO
  - Gerenciamento de Patches e Vulnerabilidades
  - Instalação remota
  - Inventário de software

Se nem **Permitir** nem **Negar** estiverem selecionados para uma permissão, a permissão será considerada como *indefinida*: será negada até que seja explicitamente negada ou permitida pelo usuário.

Os direitos de um usuário são a soma:

- Dos direitos do próprio usuário
- Dos direitos de todas as funções atribuídas a esse usuário
- Dos direitos de todo o grupo de segurança ao qual o usuário pertence
- Dos direitos de todas as funções atribuídas aos grupos de segurança aos quais o usuário pertence

Se pelo menos um desses conjuntos de direitos tiver **Negar** em uma permissão, a permissão será negada ao usuário, mesmo se outros conjuntos permitirem-na ou deixarem-na indefinida.

Também é possível adicionar usuários e grupos de segurança ao escopo de uma função do usuário para usar diferentes recursos do Servidor de Administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

Adicionar uma conta de usuário interno

Caso queira adicionar uma conta de usuário, verifique e confirme se sua conta tem o direito de Modificar ACLs do objeto na área funcional Recursos gerais: permissões do usuário.

Para adicionar uma nova conta de usuário interno ao Kaspersky Security Center Linux:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Usuários**.
2. Clique em **Adicionar**.
3. Na janela **Adicionar um usuário** que é aberta, especifique as configurações da nova conta de usuário:
   - **Nome**.
   - **Senha** para a conexão do usuário ao Kaspersky Security Center Linux.
     A senha deve estar em conformidade com as seguintes regras:
     - A senha deve ter de 8 a 256 caracteres.
     - A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
       - Letras maiúsculas (A–Z)
       - Letras minúsculas (a-z)
       - Números (0–9)
       - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - A senha não pode conter espaços em branco, caracteres Unicode nem a combinação de "." e "@" quando o "." preceder o "@".

     Para ver a senha inserida, clique em .
     É possível ativar a opção **O usuário deve alterar a senha no primeiro login** para forçar a alteração da senha na primeira autenticação do usuário.
4. Salve as alterações para concluir a criação da nova conta de usuário.

Uma nova conta de usuário é adicionada à lista de usuários.

Para usar uma conta de usuário interna previamente criada para fazer login no Kaspersky Security Center Web Console, você deve atribuir uma função a ela. Antes de fazer login, certifique-se de que a conta de usuário interna tenha uma função. Caso contrário, ocorrerá um erro de login.

Criação de um grupo de segurança

Para criar um grupo de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e selecione a guia **Grupos**.
2. Clique em **Adicionar**.

3. Na janela **Create security group** que é aberta, especifique as seguintes configurações para o novo grupo de segurança:

   - **Nome do grupo**
   - **Descrição**

4. Clique em **Salvar** para salvar as alterações.

Um novo grupo de segurança é adicionado à lista de grupos.

Editar uma conta de usuário interno

Caso queira editar uma conta de usuário, certifique-se de que sua conta tenha o direito de Modificar ACLs do objeto na área funcional Recursos gerais: permissões do usuário.

Para editar uma nova conta de usuário interno ao Kaspersky Security Center Linux:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Usuários**.
2. Clique no nome da conta de usuário que deseja editar.
3. Na janela de configurações do usuário exibida, na guia **Geral**, altere as configurações da conta de usuário:

   - **Conta de usuário**

     Se necessário, mude o botão de alternar para **Inativo** para impedir o usuário de se conectar ao aplicativo. Você pode desativar uma conta, por exemplo, depois que um funcionário sai da empresa.

   - Descrição
   - **Nome completo**
   - **Endereço de e-mail**
   - **Telefone principal**
   - **Senha**

     Caso necessário, é possível definir uma nova senha para a conexão do usuário com o Kaspersky Security Center Linux da seguinte forma:

     a. Clique no botão **Alterar senha** e defina uma nova senha para a conta de usuário.

     A senha deve estar em conformidade com as seguintes regras:

     - A senha deve ter de 8 a 256 caracteres.
     - A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
       - Letras maiúsculas (A–Z)
       - Letras minúsculas (a-z)

- Números (0–9)
- Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- A senha não pode conter espaços em branco, caracteres Unicode nem a combinação de "." e "@" quando o "." preceder o "@".

Para ver a senha inserida, clique em .

b. Caso necessário, ative a opção **O usuário deve alterar a senha no primeiro login** para forçar a alteração da senha na próxima autenticação do usuário.

c. Caso a conta de usuário esteja protegida contra modificação não autorizada, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da conta que tem o direito de Modificar ACLs do objeto na área funcional Recursos gerais: Permissões do usuário.

4. Na guia **Autenticação de dois fatores**, você pode especificar as configurações de segurança para esta conta.
5. Na guia **Grupos**, você pode adicionar o usuário a grupos de segurança.
6. Na guia **Dispositivos**, você pode atribuir dispositivos ao usuário.
7. Na guia **Funções**, você pode atribuir funções ao usuário.
8. Salve as alterações para concluir a edição da conta de usuário.

A conta de usuário atualizada aparece na lista de usuários.

Edição de um grupo de segurança

Para editar um grupo de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Grupos**.
2. Clique no nome do grupo de segurança que deseja editar.
3. Na janela de configurações do grupo que é aberta, altere as configurações do grupo de segurança:
   - Na guia **Geral**, é possível alterar as configurações de **Nome** e **Descrição**. Essas configurações estão disponíveis somente para os grupos de segurança internos.
   - Na guia **Usuários**, é possível adicionar usuários ao grupo de segurança. Essa configuração está disponível somente para usuários internos e grupos de segurança internos.
   - Na guia **Funções**, é possível atribuir uma função ao grupo de segurança.
4. Clique em **Salvar** para salvar as alterações.

As alterações são aplicadas ao grupo de segurança.

Atribuição de uma função a um usuário ou grupo de segurança

Para atribuir uma função a um usuário ou grupo de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e selecione a guia **Usuários** ou **Grupos**.
2. Selecione o nome do usuário ou grupo de segurança a quem deseja atribuir uma função.

   É possível selecionar múltiplos nomes.
3. Na linha do menu, clique no botão **Atribuir função**.

   O Assistente de Atribuição de Funções é iniciado.
4. Siga as instruções do assistente: selecione a função que deseja atribuir aos usuários selecionados ou grupos de segurança e selecione o escopo da função.

   O *escopo da função do usuário* é uma combinação de usuários e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

A função com um conjunto de direitos para uso com o Servidor de Administração será atribuída ao usuário (ou aos usuários ou ao grupo de segurança). Na lista de usuários ou grupos de segurança, uma caixa de seleção aparece na coluna **Tem funções atribuídas**.

Adição de contas de usuário em um grupo de segurança interno

É possível adicionar somente as contas de usuários internos em um grupo de segurança interno.

Para adicionar as contas de usuários em um grupo de segurança interno:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Usuários**.
2. Marque as caixas de seleção ao lado das contas de usuário que deseja adicionar a um grupo de segurança.
3. Clique no botão **Atribuir grupo**.
4. Na janela exibida **Atribuir grupo**, selecione o grupo de segurança ao qual deseja adicionar contas de usuário.
5. Clique no botão **Salvar**.

As contas de usuário são adicionadas ao grupo de segurança. Também é possível adicionar usuários internos a um grupo de segurança usando as configurações do grupo.

Atribuir um usuário como um proprietário de dispositivo

Para obter informações sobre como atribuir um usuário como proprietário de um dispositivo móvel, consulte a Ajuda do Kaspersky Secure Mobility Management.

Para atribuir um usuário como proprietário do dispositivo:

1. Caso queira atribuir um proprietário de um dispositivo conectado a um Servidor de Administração virtual, primeiro alterne para o Servidor de Administração virtual:
   a. No menu principal, clique no ícone de Sinalização (▶) à direita do nome atual do Servidor de Administração.
   b. Selecione o Servidor de Administração necessário.
2. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Usuários**.
   A lista de usuários é aberta. Caso você esteja conectado a um Servidor de Administração virtual, a lista incluirá usuários do Servidor de Administração virtual atual e do Servidor de Administração principal.
3. Clique no nome da conta de usuário que deseja atribuir como proprietário do dispositivo.
4. Na janela aberta de configurações do usuário, clique na guia **Dispositivos**.
5. Clique em **Adicionar**.
6. Na lista de dispositivos, selecione o dispositivo que deseja atribuir ao usuário.
7. Clique em **OK**.

O dispositivo selecionado é adicionado à lista de dispositivos atribuídos ao usuário.

Você pode executar a mesma operação em **Gerenciamento de ativos** → **Dispositivos gerenciados**, clicando no nome do dispositivo que deseja atribuir e clicando no link **Gerenciar proprietário do dispositivo**.

Atribuir um usuário como proprietário do dispositivo durante a instalação do Agente de Rede

Para atribuir um usuário como proprietário do dispositivo ao instalar o Agente de Rede por meio de um pacote de instalação, adicione as variáveis especificadas na tabela abaixo às configurações do pacote de instalação do Agente de Rede.

Nome da variável	Necessário	Descrição	Valores possíveis
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Não	Permite executar o utilitário para registrar o usuário como proprietário do dispositivo após a instalação do Agente de Rede. Caso esteja desativado, o registro como proprietário do dispositivo não estará disponível para o usuário.	1 - O utilitário para registrar o usuário como proprietário do dispositivo será iniciado após a instalação do Agente de Rede. Outro - O utilitário não está disponível.
KLNAGENT_DEVICEOWNER_LOGIN	Não Sim, se você inserir a senha	Contém o login de um usuário que será registrado como proprietário do dispositivo.	O login do usuário conforme especificado na lista de usuários no Kaspersky Security Center Linux.
KLNAGENT_DEVICEOWNER_PASSWORD	Não Sim, se você inserir o login	Contém a senha criptografada de um usuário que será registrado como proprietário do dispositivo.	A senha do usuário.

O Agente de Rede irá descriptografar o login e a senha especificados durante a instalação do Kaspersky Security Center Linux e o usuário será registrado como proprietário do dispositivo.

Você também pode atribuir um usuário como proprietário do dispositivo ao instalar o Agente de Rede no modo silencioso com um arquivo de resposta.

Para atribuir um usuário como proprietário do dispositivo ao instalar o Agente de Rede no modo silencioso com um arquivo de resposta:

1. Adicione o parâmetro KLNAGENT_DEVICEOWNER_REGISTRATION_START ao arquivo de resposta e defina-o como 1.

   O utilitário para registrar o usuário como proprietário do dispositivo será iniciado após a instalação do Agente de Rede.

2. Insira o login e a senha na linha de comando no dispositivo cliente.

   O usuário será atribuído como um proprietário do dispositivo.

Se o usuário estiver incluído em um grupo de segurança interno, o login deve conter o nome do usuário.

Se o usuário estiver incluído em um grupo de segurança do Active Directory, o login deve conter o nome de usuário e o nome de domínio.

Você deve inserir a senha avulsa por tempo limitado (TOTP) do aplicativo para a autenticação de dois fatores.

Atribuir um usuário como proprietário do dispositivo Linux após a instalação do Agente de Rede

Para permitir que o usuário se registre como proprietário do dispositivo Linux:

1. No Kaspersky Security Center Web Console, vá para **Gerenciamento de software → Pacotes de instalação**.

   A lista de pacotes de instalação é aberta.

2. Clique no pacote de instalação do Agente de Rede.

   A janela Propriedades do pacote de instalação é aberta.

3. Na janela de propriedades do pacote de instalação, clique em **Configurações** → **Avançado**.

4. Na seção **Registro de usuário como um proprietário do dispositivo (apenas Linux)**, ative a opção **Permitir a execução do utilitário de registro do usuário após a instalação do Agente de Rede** e clique em **Salvar**.

O utilitário para registrar o usuário como proprietário do dispositivo pode ser executado usando a linha de comando no dispositivo cliente.

Para registrar um usuário como proprietário do dispositivo Linux no dispositivo cliente:

1. Execute o seguinte comando na linha de comando no dispositivo cliente:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Insira o login e a senha, se solicitados.

   Se o login e a senha estiverem incluídos no arquivo de resposta ou no pacote de instalação do Agente de Rede, execute o seguinte comando na linha de comando no dispositivo cliente:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Se o usuário estiver incluído em um grupo de segurança interno, o login deve conter o nome do usuário.

Se o usuário estiver incluído em um grupo de segurança do Active Directory, o login deve conter o nome de usuário e o nome de domínio.

Você deve inserir a senha avulsa por tempo limitado (TOTP) do aplicativo para a autenticação de dois fatores.

O usuário será registrado como proprietário do dispositivo.

Remover um usuário como proprietário do dispositivo

Para remover um usuário como proprietário do dispositivo no dispositivo cliente:

1. Execute o seguinte comando na linha de comando do dispositivo cliente:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner
   ```

2. Digite o nome de usuário e senha.

Se o usuário estiver incluído em um grupo de segurança interno, o login deve conter o nome do usuário.

Se o usuário estiver incluído em um grupo de segurança do Active Directory, o login deve conter o nome de usuário e o nome de domínio.

Você deve inserir a senha avulsa por tempo limitado (TOTP) do aplicativo para a autenticação de dois fatores.

O usuário será removido como proprietário do dispositivo.

Ativando a proteção da conta contra modificações não autorizadas

Você pode ativar uma opção adicional para proteger uma conta de usuário contra modificações não autorizadas. Se essa opção for ativada, a modificação das configurações da conta do usuário requer autorização do usuário com direitos para modificação.

Para ativar ou desativar a proteção da conta contra modificações não autorizadas:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Usuários**.
2. Clique no nome da conta de usuário interno para a qual você deseja especificar a proteção da conta contra modificações não autorizadas.
3. Na janela aberta de configurações do usuário, clique na guia **Autenticação de dois fatores**.
4. Na guia **Autenticação de dois fatores**, selecione a opção **Solicite a autenticação para verificar a permissão para alterar as contas de usuário** caso queira solicitar credenciais e um código de segurança de uso único para a autenticação de dois fatores sempre que as configurações de conta forem alteradas ou modificadas. Caso contrário, selecione a opção **Permitir que usuários modifiquem esta conta sem autenticação adicional**.
5. Salve as alterações.

Configuração da autenticação de dois fatores

A partir do Servidor de Administração versão 16.1, a autenticação de dois fatores é ativada automaticamente. A opção global para desativar a autenticação de dois fatores não é compatível. Este cenário fornece etapas para configurar a autenticação em duas etapas no primeiro login e definir as configurações da autenticação de dois fatores no Servidor de Administração.

Fases

A configuração da autenticação de dois fatores ocorre em etapas:

1. **Instalação de um app autenticador em um dispositivo**

   É possível instalar qualquer aplicativo compatível com o Algoritmo de Senha Avulsa por Tempo Limitado (TOTP).

   Disponível na Rússia:

   - Kaspersky Password Manager for Business (recomendado)
   - Bitrix24 OTP
   - ID Yandex
   - Autenticador da Avanpost

- Aladdin 2FA
- Rutoken OTP

Disponível em todo o mundo (incluindo a Rússia):

- Autenticador do Google
- Autenticador da Microsoft

Para verificar se o Kaspersky Security Center Linux é compatível com o app autenticador que deseja usar, ative a autenticação de dois fatores para todos os usuários ou para um usuário específico.

Uma das etapas sugere a especificação do código de segurança gerado pelo app autenticador. Caso haja êxito, o Kaspersky Security Center Linux será compatível com o autenticador selecionado.

> É altamente recomendável não instalar o app autenticador no mesmo dispositivo no qual o Servidor de Administração é gerenciado.

2. **Sincronização da hora no dispositivo com o app autenticador com a hora do dispositivo no qual o Servidor de Administração está instalado**

   Certifique-se de que a hora no dispositivo com o app autenticador e a hora no dispositivo com o Servidor de Administração estejam sincronizadas com o UTC. Para uma melhor precisão, recomendamos utilizar os mesmos servidores NTP em toda a infraestrutura. Caso contrário, podem ocorrer falhas ao configurar a autenticação de dois fatores.

3. **Configuração da autenticação de dois fatores para contas de usuário ao fazer login no Web Console**

   Faça login no Web Console e configure a autenticação de dois fatores.

   Se a configuração da autenticação de dois fatores não estiver disponível para você, entre em contato com um usuário que tenha o direito Modificar ACLs de objetos da área funcional **Recursos gerais: Permissões do usuário** e tenha configurado a autenticação de dois fatores, a fim de adicionar sua conta à lista de permissão da autenticação de dois fatores.

4. **Definição das configurações de autenticação de dois fatores no Servidor de Administração**

   Se você configurou a autenticação de dois fatores e o direito Modificar ACLs de objetos da área funcional **Recursos gerais**: **Permissões do usuário**, você pode definir as configurações da autenticação de dois fatores no Servidor de Administração da seguinte forma:

   1. Revisão da lista de usuários que podem configurar a autenticação em duas etapas no login:

      - Para instalar o Servidor de Administração 16.1 a partir do zero: adicione os usuários necessários à lista de permissão da autenticação de dois fatores para permitir que eles configurem a autenticação de dois fatores ao fazer login pela primeira vez.
      - Para atualizar ou restaurar para o Servidor de Administração 16.1: revise a lista de permissão da autenticação de dois fatores e exclua as contas que não devem ter acesso ao Servidor de Administração.

   2. Exclusão de contas de usuário para as quais você não precisa ativar a autenticação de dois fatores (opcional)

      Exclua contas de usuário da autenticação de dois fatores para permitir que os usuários façam login no Servidor de Administração mesmo sem terem configurado a autenticação de dois fatores. A exclusão de contas da autenticação de dois fatores pode ser necessária para as contas de serviço que não conseguem fornecer um código de segurança durante a autenticação. As contas de integração são usadas para executar scripts por meio da OpenAPI.

3. Redefinição ou exclusão de uma chave secreta de autenticação de dois fatores (opcional)

   Você pode redefinir uma chave secreta de autenticação de dois fatores quando um usuário perder o acesso ao dispositivo de autenticação de dois fatores ou precisar configurá-la em um novo dispositivo. Você também pode redefinir uma chave secreta para a sua própria conta.

   Você pode excluir uma chave secreta para impedir completamente que um usuário faça login no Web Console, bem como acessar o Servidor de Administração.

4. Edição do nome de um emissor de código de segurança (opcional)

   Caso você tenha vários Servidores de Administração com nomes semelhantes, pode ser necessário alterar os nomes do emissor do código de segurança para uma melhor identificação dos diferentes Servidores de Administração.

Resultados

Após a conclusão deste cenário:

- A autenticação de dois fatores é configurada para a sua própria conta e para outra conta de usuário que precisa acessar o Servidor de Administração.
- As contas de integração são excluídas da autenticação de dois fatores.

Sobre a autenticação de dois fatores para uma conta

O Kaspersky Security Center Linux fornece a autenticação de dois fatores aos usuários do Kaspersky Security Center Web Console. A autenticação de dois fatores baseia-se no padrão RFC 6238 (TOTP: Algoritmo de Senha Avulsa por Tempo Limitado).

Sempre que você fizer login no Kaspersky Security Center Web Console, insira seu nome de usuário, senha e um código de segurança de uso único adicional. Para receber um código de segurança de uso único, é necessário ter um app autenticador no dispositivo móvel ou computador.

> Qualquer software de autenticação compatível com o Algoritmo de Senha Avulsa por Tempo Limitado (TOTP) pode ser usado como um app autenticador, como o Google Authenticator, por exemplo. Para gerar o código de segurança de uso único, você deve sincronizar a hora definida no dispositivo com o app autenticador com a hora definida no dispositivo do Servidor de Administração. Para uma melhor precisão, recomendamos utilizar os mesmos servidores NTP em toda a infraestrutura.

Para verificar se o Kaspersky Security Center Linux é compatível com o app autenticador que você deseja usar, tente configurar a autenticação de dois fatores com esse app autenticador.

Uma das etapas sugere especificar o código de segurança de uso único gerado pelo app autenticador. Caso haja êxito, o Kaspersky Security Center Linux será compatível com o autenticador selecionado.

Geração de um código secreto usando um aplicativo de autenticação

Um app autenticador gera o código de segurança da seguinte maneira:

1. O Servidor de Administração gera uma chave secreta especial e um código QR.
2. A chave secreta gerada ou o código QR é passado para o app autenticador.
3. O app autenticador gera um código de segurança de uso único que deve ser passado para a janela de autenticação do Servidor de Administração.

Um código de segurança possui um identificador conhecido como *nome do emissor*. O nome do emissor do código de segurança é usado como um identificador do Servidor de Administração no app autenticador. Você pode alterar o nome do emissor do código de segurança. O nome do emissor do código de segurança possui um valor padrão que é igual ao nome do Servidor de Administração. Um novo nome de emissor do código de segurança será atribuído ao Servidor de Administração após o próximo login. Um código de segurança é de uso único e válido por até 30 segundos (o tempo exato pode variar).

É altamente recomendável salvar a chave secreta (ou código QR) e mantê-la em um lugar seguro. Isso ajudará a restaurar o acesso ao Kaspersky Security Center Web Console caso você perca o acesso ao dispositivo com o app autenticador.

A autenticação de dois fatores tem os seguintes recursos:

- A partir do Servidor de Administração versão 16.1, a autenticação de dois fatores é ativada automaticamente e a opção de configurá-la ao fazer login é desativada por padrão. A configuração da autenticação de dois fatores no login está disponível somente para os usuários que estão incluídos na lista de permissão da autenticação de dois fatores.
- Um usuário pode configurar a autenticação de dois fatores somente para a sua própria conta.
- Um usuário pode excluir contas da autenticação de dois fatores. Isso pode ser necessário para contas de integração que não podem receber um código de segurança de uso único para autenticação. As contas de integração são usadas para executar scripts por meio da OpenAPI.
- Para gerar novamente uma chave secreta de autenticação de dois fatores, um usuário deve redefinir a chave secreta da sua própria conta.
- Para redefinir ou excluir uma chave secreta de autenticação de dois fatores para a conta de outro usuário, um usuário deve ter uma conta com a autenticação de dois fatores configurada e ter o direito Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário**.
- Para excluir contas de outros usuários da autenticação de dois fatores ou modificar a lista de permissão da autenticação de dois fatores, um usuário deve ter uma conta com esta autenticação configurada e com o direito de Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário**.
- Sempre deve haver pelo menos um usuário com a autenticação de dois fatores configurada para que ele possa gerenciar a lista de permissão da autenticação de dois fatores e a lista de exclusão.
- A autenticação de dois fatores é ativada automaticamente somente na versão 16.1 do Servidor de Administração. Se outros Servidores de Administração principais ou secundários estiverem executando a versão 16 ou anterior, suas configurações de autenticação de dois fatores permanecerão inalteradas.

- Um Servidor de Administração virtual herda as configurações de autenticação de dois fatores do Servidor de Administração físico para que, se a autenticação de dois fatores estiver ativada no servidor físico, ela também seja ativada em um servidor virtual. Você não pode definir as configurações de autenticação de dois fatores em um Servidor de Administração virtual.
- Para que a autenticação de dois fatores funcione corretamente, você precisa atualizar o Servidor de Administração e o Web Console para a versão 16.1 ou posterior.

Para garantir uma proteção abrangente usando a autenticação de dois fatores, é necessário proteger não apenas o Servidor de Administração, mas também o dispositivo no qual ele está instalado. Para fazer isso, siga as recomendações do Guia de proteção.

Configuração de uma chave secreta de autenticação de dois fatores ao fazer login no Kaspersky Security Center Web Console

Na primeira vez que você fizer login no Kaspersky Security Center Linux 16.1 ou posterior, a janela para configurar a autenticação de dois fatores será aberta.

Para configurar a autenticação de dois fatores para sua conta:

1. Instale qualquer aplicativo que seja compatível com o Algoritmo de Senha Avulsa por Tempo Limitado (TOTP) no dispositivo móvel ou computador.

   Disponível na Rússia:

   - Kaspersky Password Manager for Business (recomendado)
   - Bitrix24 OTP
   - ID Yandex
   - Autenticador da Avanpost
   - Aladdin 2FA
   - Rutoken OTP

   Disponível em todo o mundo (incluindo a Rússia):

   - Autenticador do Google
   - Autenticador da Microsoft

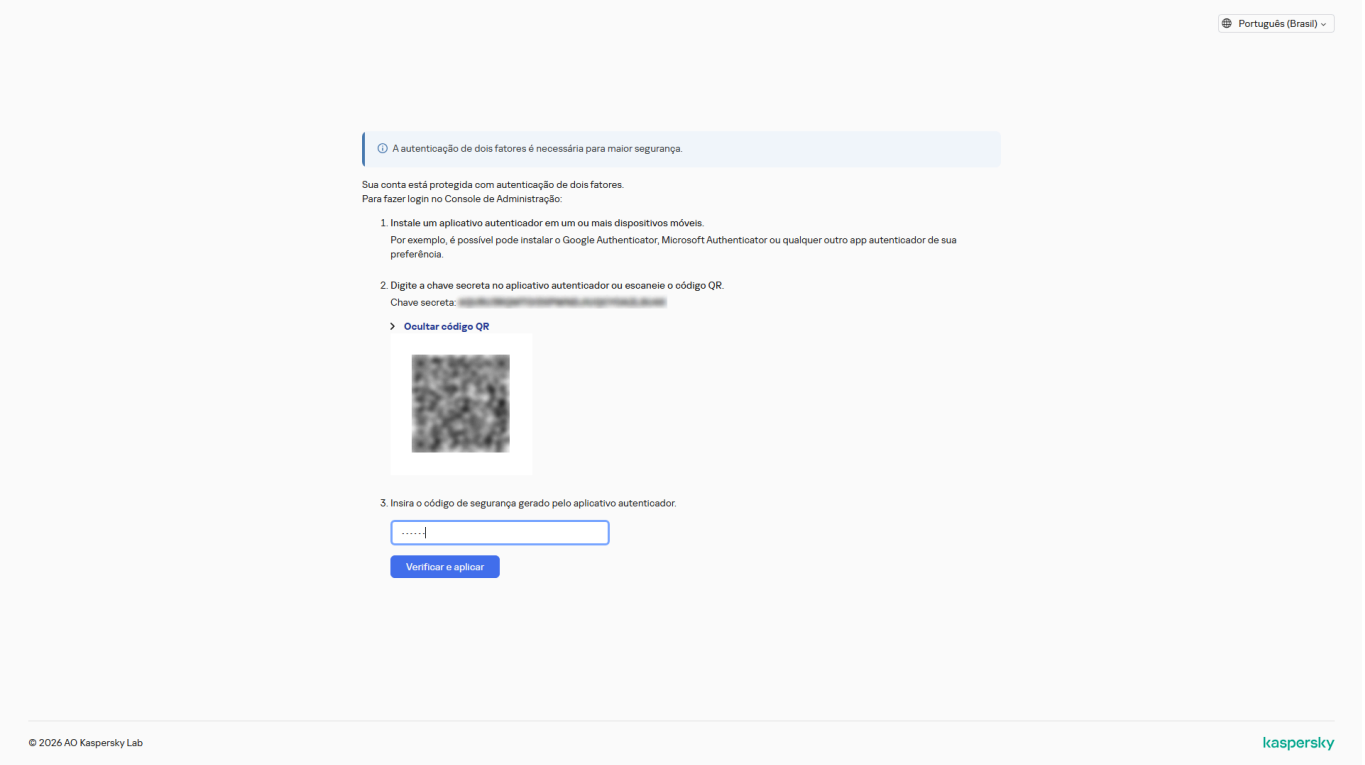
   É altamente recomendável não instalar o app autenticador no mesmo dispositivo no qual o Servidor de Administração é gerenciado.

2. Certifique-se de que a hora no dispositivo com o app autenticador e a hora no dispositivo com o Servidor de Administração estejam sincronizadas com o UTC. Para uma melhor precisão, recomendamos utilizar os mesmos servidores NTP em toda a infraestrutura.

3. Gere um código de segurança de uso único usando o app autenticador no dispositivo móvel ou computador. Para fazer isso, siga uma destas etapas:

   - Insira manualmente a chave secreta de autenticação de dois fatores no app autenticador.
   - Clique em **Ver código QR** e leia o código QR usando o app autenticador.

   Um código de segurança de uso único de 6 dígitos será exibido no dispositivo móvel.



Configuração de uma chave secreta de autenticação de dois fatores ao fazer login no Kaspersky Security Center Web Console

4. Na janela da **Autenticação de dois fatores**, especifique o código de segurança de uso único gerado pelo app autenticador e clique no botão **Verificar e aplicar**.

   Configuração do Rutoken OTP

   Se você utilizar o Rutoken OTP, será necessário um dispositivo móvel Android com o aplicativo Rutoken OTP instalado. O dispositivo móvel Android deve ter os seguintes requisitos:

   - Sistema operacional Android 7 ou mais recente.
   - Módulo NFC disponível e ativado.

   No aplicativo Rutoken OTP, você deve configurar os seguintes parâmetros:

   - Escaneie o código QR exibido no assistente de configuração da autenticação em duas etapas.
   - Defina o intervalo de tempo para 30 segundos.
   - Selecione SHA1 como algoritmo.

   Para configurar o Rutoken OTP:

   1. Coloque o dispositivo Rutoken OTP ao lado do dispositivo móvel com o módulo NFC.
   2. No aplicativo Rutoken OTP, pressione **Conectar token**.

3. No aplicativo Rutoken OTP, pressione **Definir configurações** e, em seguida, pressione **Salvar chave secreta.**

   Se o token estiver conectado com sucesso ao dispositivo móvel, o aplicativo Rutoken OTP mostra as seguintes mensagens de status:

   - **O token está conectado.**
   - **As configurações estão definidas.**
   - **A chave secreta está salva.**

4. No dispositivo Rutoken OTP, clique no botão.

   Um código de segurança é exibido no dispositivo.

5. No Kaspersky Security Center Web Console, na janela de verificação em duas etapas, insira o código de segurança.

A autenticação de dois fatores está configurada para sua conta. É possível acessar o Servidor de Administração de acordo com seus direitos.

Se a configuração da autenticação de dois fatores não estiver disponível, entre em contato com um usuário que tenha o direito Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário** e tenha configurado a autenticação de dois fatores, a fim de adicionar sua conta à lista de permissão da autenticação de dois fatores.

Permitir que os usuários configurem a autenticação de dois fatores

A lista de permissão da autenticação de dois fatores é uma lista de usuários que têm permissão para configurar inicialmente a autenticação de dois fatores ao fazer login no Web Console. Essa lista contém contas de usuário sem autenticação de dois fatores configurada. Por padrão, as novas contas de usuário não são incluídas na lista de permissão da autenticação de dois fatores e devem ser adicionadas por um administrador. Se uma conta nova for uma conta de integração usada para executar scripts OpenAPI, ela deve ser excluída da autenticação de dois fatores.

Uma conta de usuário será automaticamente excluída da lista de permissão da autenticação de dois fatores quando ela tiver configurado a autenticação de dois fatores ou for excluída da autenticação de dois fatores.

A modificação manual da lista de permissão da autenticação de dois fatores está disponível para contas que configuraram a autenticação de dois fatores e que têm o direito de Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário**.

Para adicionar uma conta de usuário à lista de permissão da autenticação de dois fatores manualmente:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Autenticação de dois fatores** da janela de propriedades, na tabela **Usuários autorizados a gerar chaves secretas**, clique no botão **Adicionar**.

3. Na janela aberta:

   a. Selecione as contas de usuário que deseja adicionar.

      Somente usuários que não estão excluídos da autenticação de dois fatores e não têm uma chave secreta de autenticação de dois fatores podem ser adicionados à lista de permissão.

   b. Caso a conta esteja protegida contra modificações não autorizadas, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da sua própria conta e o código de segurança de uso único para a autenticação de dois fatores.

   c. Salve as alterações.

A conta de usuário selecionada é adicionada à lista de permissão da autenticação de dois fatores. No próximo login, o usuário poderá gerar uma chave secreta.

Uma conta de usuário pode ser excluída da lista de permissão da autenticação de dois fatores até que a autenticação de dois fatores seja configurada para essa conta.

Para excluir contas de usuário da lista de permissão da autenticação de dois fatores manualmente:

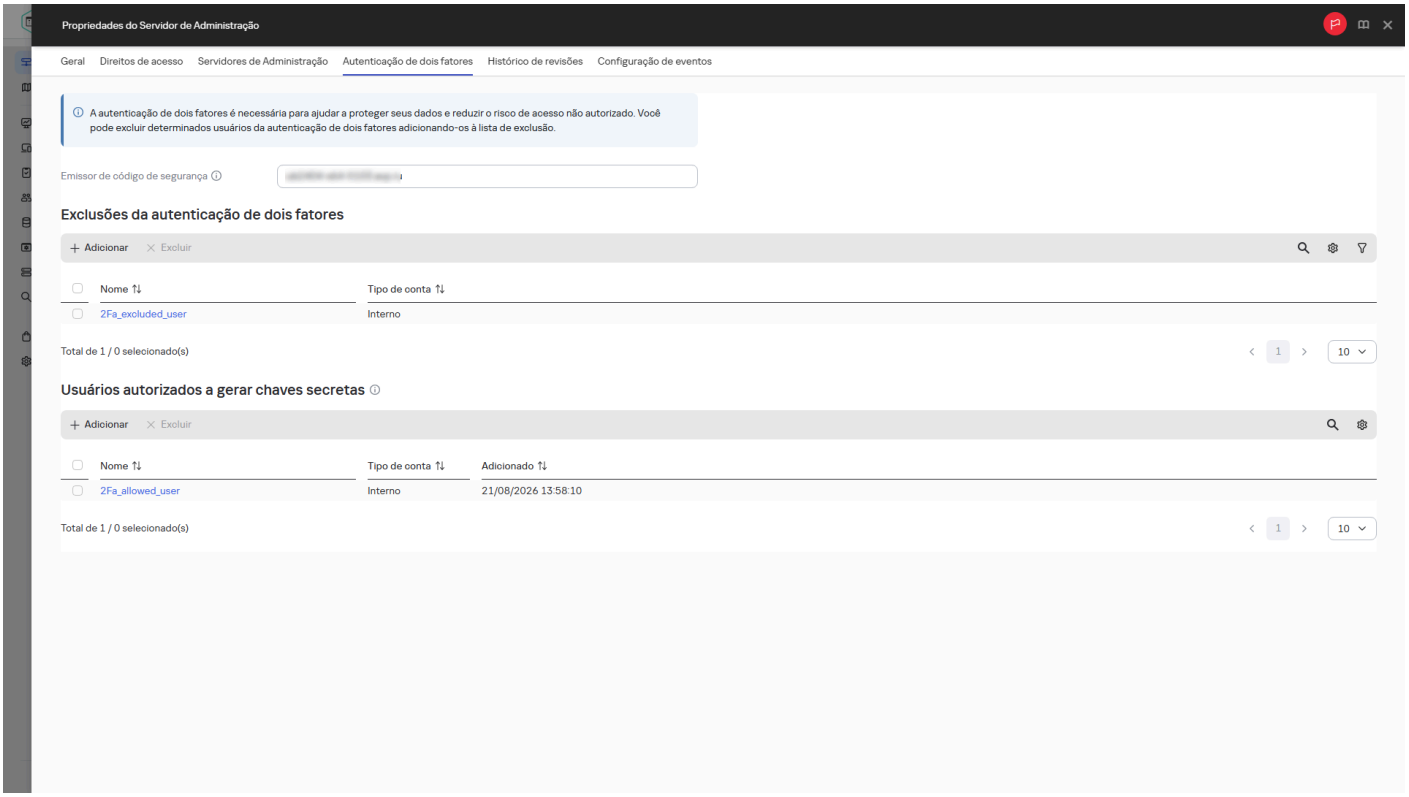
1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Autenticação de dois fatores** da janela de propriedades, na tabela **Usuários autorizados a gerar chaves secretas**, selecione as contas de usuário que deseja excluir e clique em **Excluir**.

3. Caso a conta esteja protegida contra modificações não autorizadas, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da sua própria conta e o código de segurança de uso único para a autenticação de dois fatores.

As contas de usuário selecionadas serão excluídas da lista de permissão da autenticação de dois fatores.



Configurar a lista de permissão de autenticação de dois fatores

Se, durante uma sessão ativa no Servidor de Administração, sua chave secreta de autenticação de dois fatores for excluída por outro usuário ou você mesmo redefinir a chave, mas não criar uma nova, a capacidade de modificar a lista de permissão será bloqueada.

As contas de usuário também podem ser adicionadas e excluídas automaticamente da lista de permissão da autenticação de dois fatores.

Ao redefinir a chave secreta de autenticação de dois fatores para outras contas, essas contas são automaticamente adicionadas à lista de permissão da autenticação de dois fatores, para que possam gerar uma nova chave secreta.

Ao atualizar o Servidor de Administração da versão 16 ou anterior para a versão 16.1 ou posterior, bem como ao criar um backup de dados no Servidor de Administração 16 ou anterior e restaurá-lo no Servidor de Administração 16.1 ou posterior, as contas de usuário serão automaticamente adicionadas à lista de permissão da autenticação de dois fatores, desde que todas as seguintes condições sejam atendidas:

- O usuário tem a permissão Ler na área funcional *Recursos gerais: Funcionalidade básica* atribuída diretamente a ele (não por meio de um grupo de segurança). O escopo da função do usuário com esta permissão deve incluir todos os dispositivos gerenciados e não atribuídos, e deve ser definido no nível do Servidor de Administração.
- O usuário não é excluído da autenticação de dois fatores.
- O usuário não tem uma chave secreta de autenticação de dois fatores.
- A autenticação de dois fatores não foi ativada para todos os usuários na versão anterior do Servidor de Administração.

O não atendimento de apenas uma das condições resultará na não inclusão do usuário na lista de permissão da autenticação de dois fatores.

Após uma atualização ou restauração, recomendamos garantir que a lista de permissão da autenticação de dois fatores contenha apenas as contas de usuário que precisam ter acesso ao Servidor de Administração. Revise a lista de permissão da autenticação de dois fatores e remova quaisquer outras contas dela. Adicione contas de integração usadas para executar scripts por meio do OpenAPI à lista de exclusão para evitar falhas de script.

As contas de usuário perderão o acesso ao Servidor de Administração após uma atualização ou restauração se todas as seguintes condições forem atendidas:

- O usuário tem a permissão Ler na área funcional *Recursos gerais: Funcionalidade básica* atribuída por meio de um grupo de segurança (não diretamente ao usuário) ou não tem essa permissão.
- O usuário não é excluído da autenticação de dois fatores.
- O usuário não tem uma chave secreta de autenticação de dois fatores.
- A autenticação de dois fatores não foi ativada para todos os usuários na versão anterior do Servidor de Administração.

Essas contas podem ser adicionadas manualmente à lista de permissão da autenticação de dois fatores, se necessário.

Redefinição e exclusão de uma chave secreta de autenticação de dois fatores

Você pode redefinir uma chave secreta quando um usuário perde o acesso ao dispositivo de autenticação de dois fatores ou precisa configurá-la em um dispositivo novo. A redefinição da chave secreta permite que o usuário entre no Web Console novamente e gere uma nova chave secreta.

Você pode redefinir ou excluir uma chave secreta de autenticação de dois fatores para contas de outros usuários somente se tiver configurado a autenticação de dois fatores e tiver o direito Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário**. Você também pode gerar novamente sua própria chave secreta.

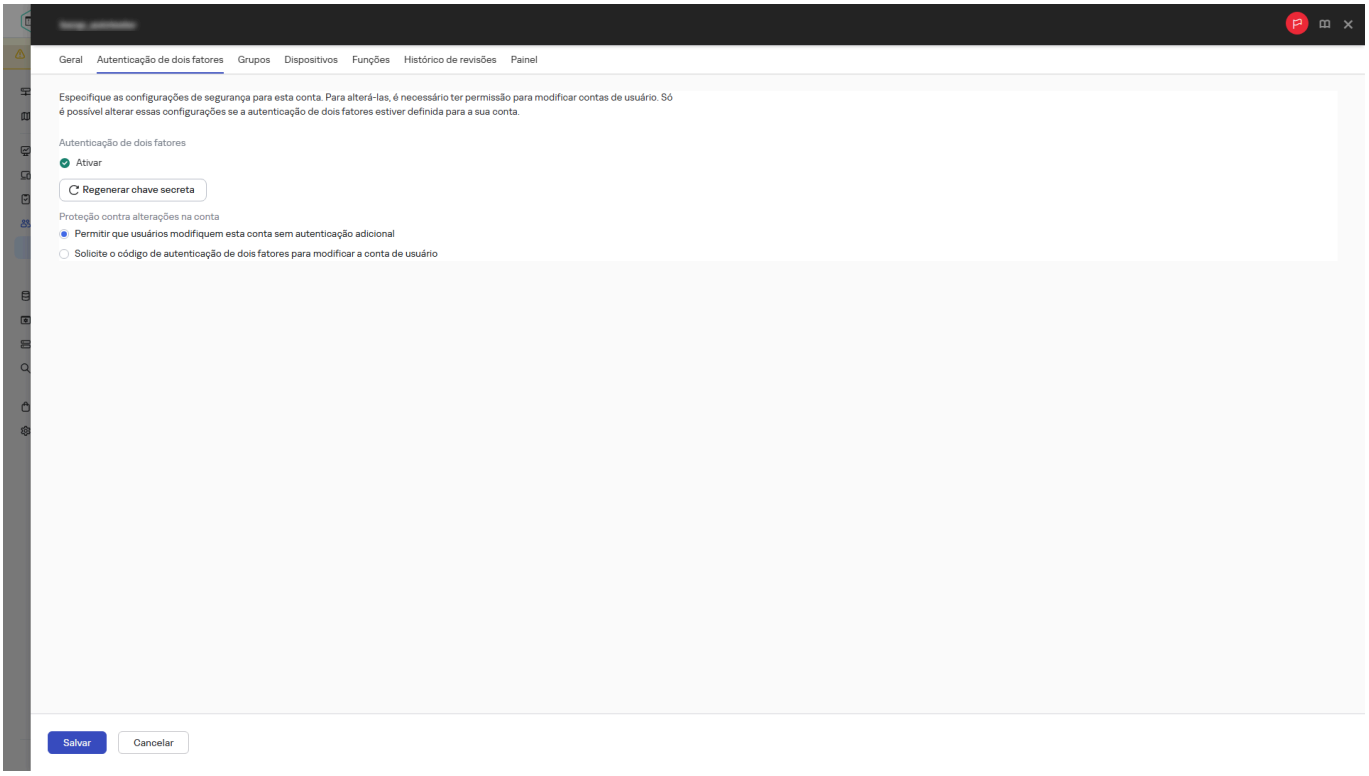
Para redefinir uma chave secreta para uma conta:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Usuários**.

2. Clique no nome da conta de usuário para a qual você deseja redefinir uma chave secreta.

3. Se você quiser redefinir uma chave secreta para sua conta:

a. Na guia **Autenticação de dois fatores**, clique no botão **Regenerar chave secreta**.

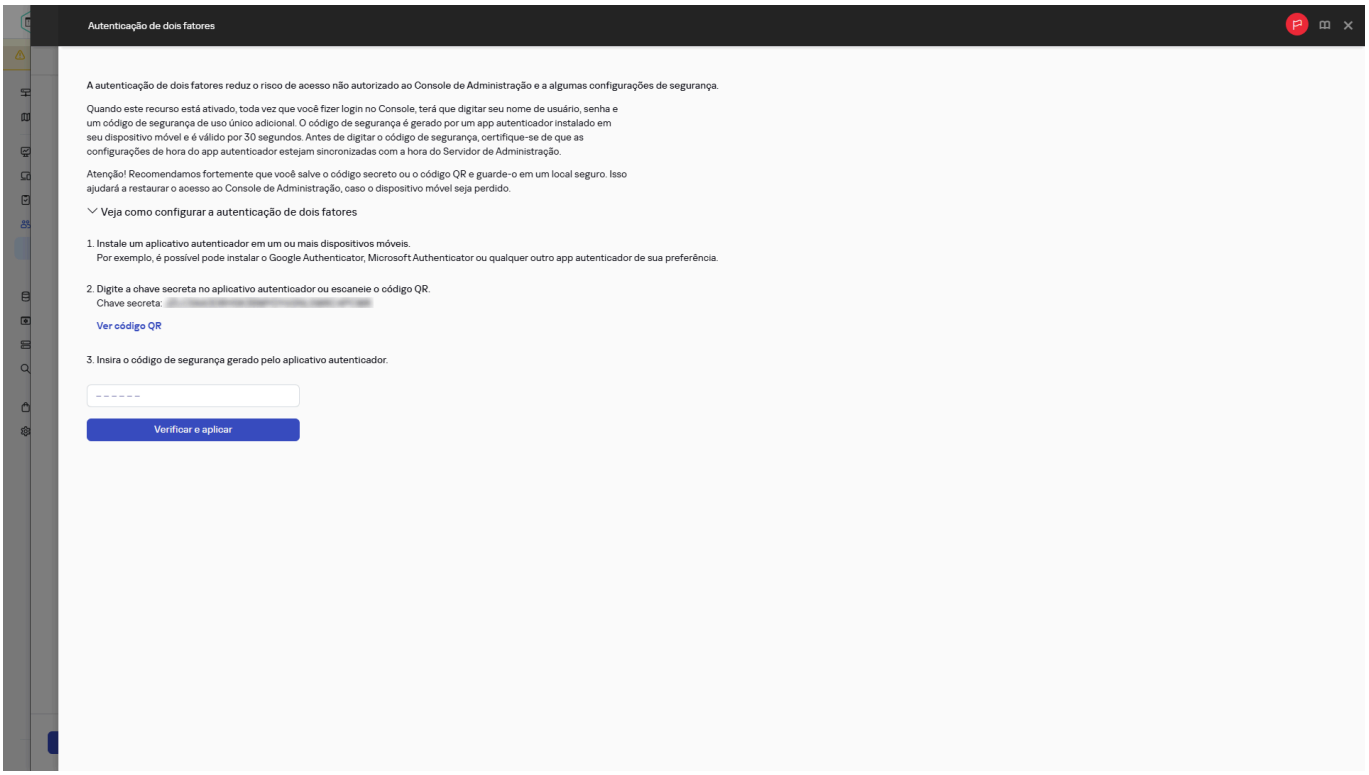


Regenerar a chave secreta de autenticação de dois fatores para a conta de usuário atual

a. Caso sua conta esteja protegida contra modificações não autorizadas, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da sua própria conta e o código de autenticação de dois fatores.

b. Na janela **Autenticação de dois fatores**, clique em **Veja como configurar a autenticação de dois fatores** e depois clique em **Ver código QR**.

c. Use o app autenticador no dispositivo móvel para ler o código QR e receber um código de segurança de uso único.



Configurar uma nova chave secreta de autenticação de dois fatores para a conta de usuário atual

a. Na janela **Autenticação de dois fatores**, especifique o código de segurança de uso único gerado pelo app autenticador, clique no botão **Verificar e aplicar** e salve as alterações.

Configuração do Rutoken OTP

Se você utilizar o Rutoken OTP, será necessário um dispositivo móvel Android com o aplicativo Rutoken OTP instalado. O dispositivo móvel Android deve ter os seguintes requisitos:

- Sistema operacional Android 7 ou mais recente.
- Módulo NFC disponível e ativado.

No aplicativo Rutoken OTP, você deve configurar os seguintes parâmetros:

- Escaneie o código QR exibido no assistente de configuração da autenticação em duas etapas.
- Defina o intervalo de tempo para 30 segundos.
- Selecione SHA1 como algoritmo.

Para configurar o Rutoken OTP:

1. Coloque o dispositivo Rutoken OTP ao lado do dispositivo móvel com o módulo NFC.
2. No aplicativo Rutoken OTP, pressione **Conectar token**.
3. No aplicativo Rutoken OTP, pressione **Definir configurações** e, em seguida, pressione **Salvar chave secreta.**

Se o token estiver conectado com sucesso ao dispositivo móvel, o aplicativo Rutoken OTP mostra as seguintes mensagens de status:

- **O token está conectado.**
- **As configurações estão definidas.**
- **A chave secreta está salva.**

4. No dispositivo Rutoken OTP, clique no botão.

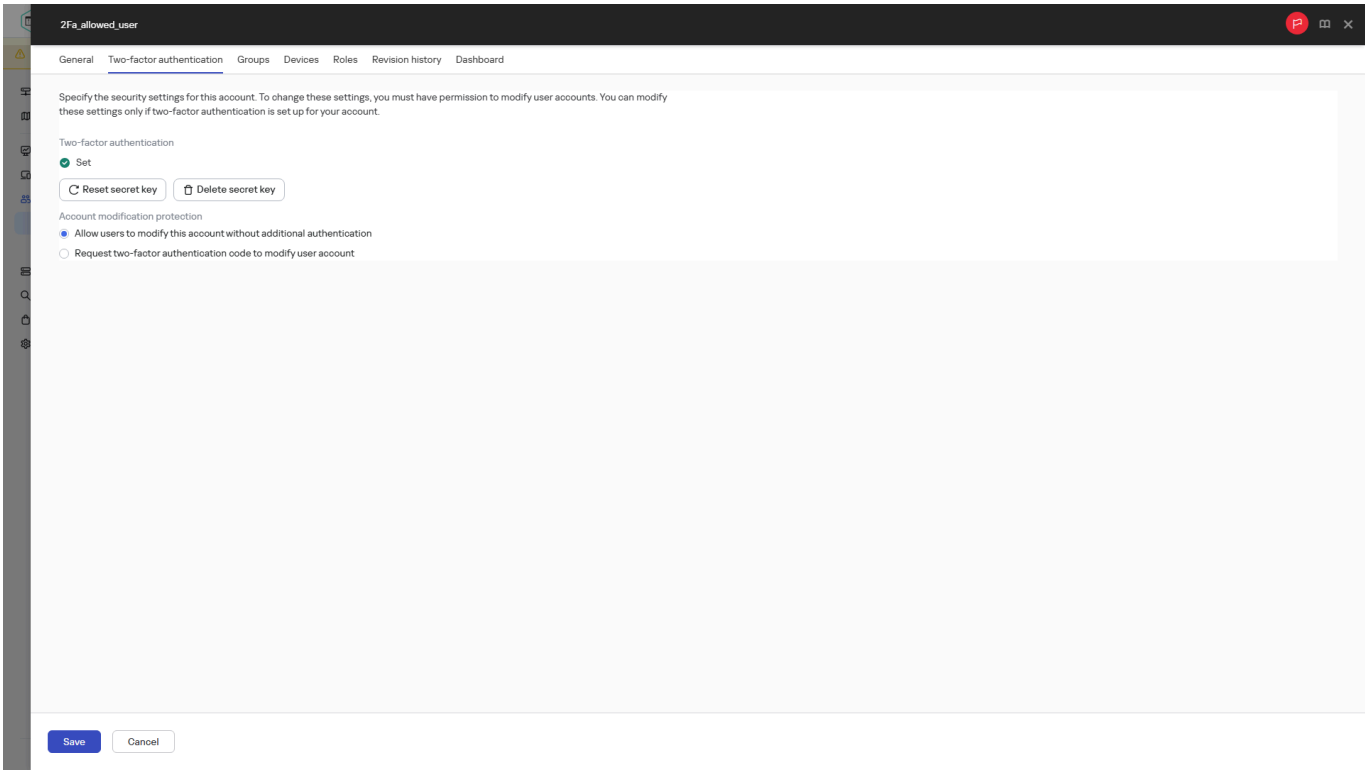
   Um código de segurança é exibido no dispositivo.

5. No Kaspersky Security Center Web Console, na janela de verificação em duas etapas, insira o código de segurança.

A chave secreta de sua conta é alterada.

4. Se você quiser redefinir uma chave secreta para outra conta:

   a. Na guia **Autenticação de dois fatores**, clique no botão **Redefinir a chave secreta**.



Redefinir a chave secreta de autenticação de dois fatores para outra conta de usuário

   a. Caso a conta esteja protegida contra modificações não autorizadas, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da sua própria conta e o código de segurança de uso único para a autenticação de dois fatores.

   b. Confirme a redefinição da chave secreta e salve as alterações.

Ao redefinir uma chave secreta para outra conta, a chave secreta existente é excluída e a conta de usuário é adicionada à lista de permissão de autenticação de dois fatores nas propriedades do Servidor de Administração. No próximo login, o usuário poderá gerar uma nova chave secreta.

A chave secreta de uma conta de usuário é redefinida.

Você pode excluir uma chave secreta para impedir completamente que um usuário faça login no Web Console, bem como acessar o Servidor de Administração.

Para excluir uma chave secreta:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Usuários**.
2. Clique no nome da conta de usuário interna para a qual deseja excluir uma chave secreta.

   Você não pode excluir uma chave secreta da sua própria conta.

3. Na guia **Autenticação de dois fatores**, clique no botão **Excluir a chave secreta**.
4. Caso a conta esteja protegida contra modificações não autorizadas, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da sua própria conta e o código de segurança de uso único para a autenticação de dois fatores.
5. Confirme a exclusão da chave secreta e salve as alterações.

A chave secreta de uma conta de usuário é excluída.

É possível restaurar o acesso ao adicionar o usuário à lista de permissão da autenticação de dois fatores nas propriedades do Servidor de Administração. Nesse caso, no próximo login, o usuário poderá gerar uma nova chave secreta.

Excluir contas da autenticação de dois fatores

É possível excluir contas de usuário da autenticação de dois fatores para permitir que os usuários façam login no Servidor de Administração mesmo sem terem configurado a autenticação de dois fatores. A exclusão de contas da autenticação de dois fatores pode ser necessária para as contas de integração que não conseguem fornecer um código de segurança de uso único durante a autenticação. As contas de integração são usadas para executar scripts por meio da OpenAPI.

Você pode modificar a lista de exclusão se a autenticação de dois fatores estiver configurada para a sua conta e você tiver o direito Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário**.

Para excluir uma conta de usuário da autenticação de dois fatores:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Autenticação de dois fatores** da janela de propriedades, clique no botão **Adicionar** na tabela **Exclusões da autenticação de dois fatores**.

3. Na janela aberta:

   a. Selecione a conta de usuário que deseja excluir.

   b. Caso a conta esteja protegida contra modificações não autorizadas, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da sua própria conta e o código de segurança de uso único para a autenticação de dois fatores.

   c. Salve as alterações.

   As contas de usuário selecionadas são excluídas da autenticação de dois fatores e suas chaves secretas são excluídas, caso existam. A lista de contas excluídas não é alterada quando você restaura um backup no Servidor de Administração 16.1 ou atualiza o Servidor de Administração para a versão 16.1 ou posterior. Se as contas da lista de exclusão tinham segredos na versão anterior do Servidor de Administração, essas chaves secretas serão excluídas na versão 16.1.

Você pode excluir contas de usuário da lista de exclusão para impedir completamente que os usuários façam login no Web Console, bem como acessar o Servidor de Administração.

Para excluir contas de usuário da lista de exclusão:

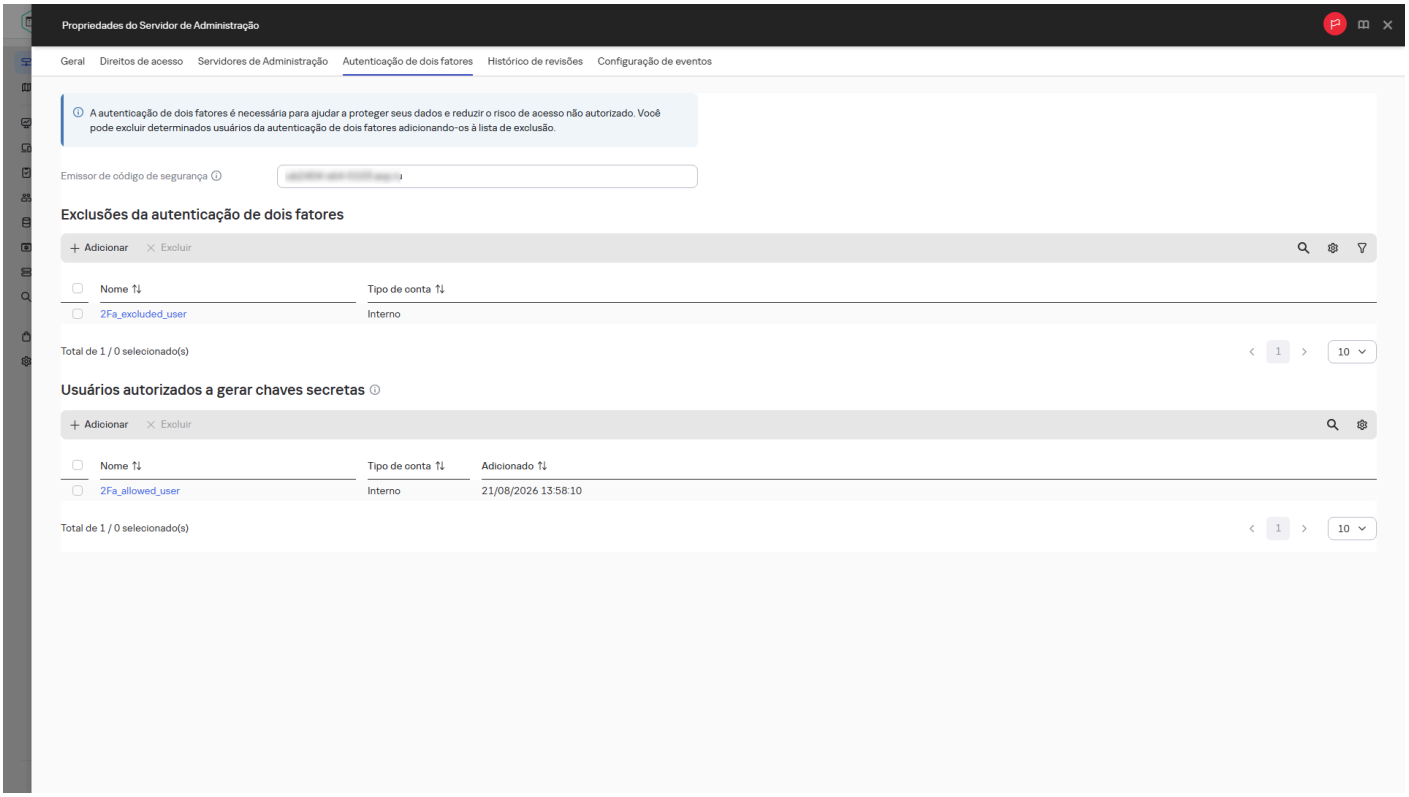
1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Autenticação de dois fatores** da janela de propriedades, na tabela **Exclusões da autenticação de dois fatores**, selecione as contas de usuário que deseja excluir e clique em **Excluir**.

3. Caso a conta esteja protegida contra modificações não autorizadas, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da sua própria conta e o código de segurança de uso único para a autenticação de dois fatores.

As contas de usuário selecionadas são excluídas da lista de exclusão.



Configurar a lista de exclusão de autenticação de dois fatores

Editando o nome de um emissor do código de segurança

Você pode ter vários identificadores (chamados de emissores) para diferentes Servidores de Administração. Você pode alterar o nome de um emissor de código de segurança caso, por exemplo, o Servidor de Administração já utilize um nome semelhante de emissor para outro Servidor de Administração. Por padrão, o nome de um emissor de código de segurança é igual ao nome do Servidor de Administração.

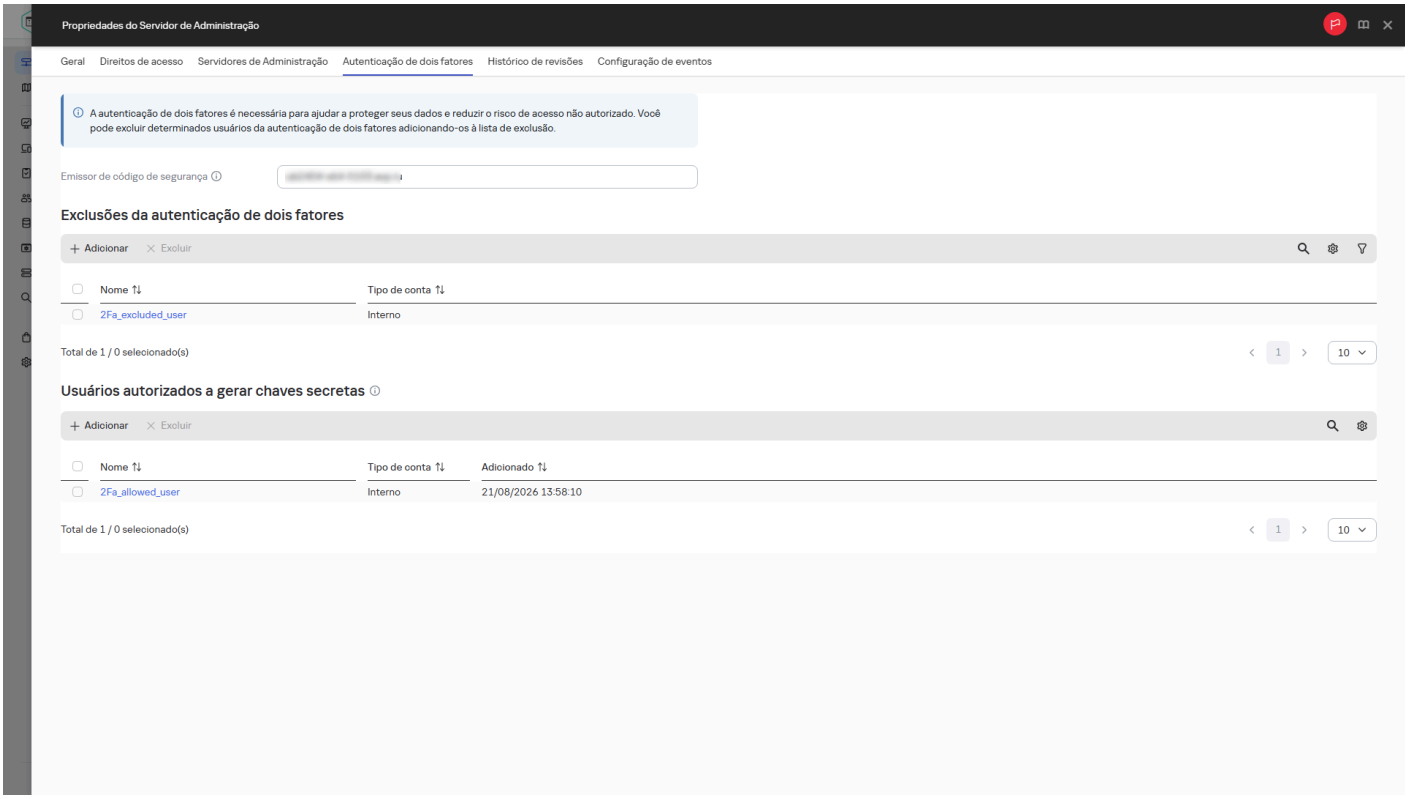
Para especificar um novo nome de um emissor do código de segurança:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Autenticação de dois fatores** da janela de propriedades, insira um novo nome no campo **Emissor de código de segurança** e salve as alterações.

Um novo nome de emissor do código de segurança será atribuído ao Servidor de Administração após o próximo login.



Especificar o nome de um emissor do código de segurança

Alterar o número permitido de tentativas de entrada de senha

O usuário do Kaspersky Security Center Linux pode inserir uma senha inválida um número limitado de vezes. Depois que o limite é atingido, a conta de usuário é bloqueada por uma hora.

Por padrão, o número máximo de tentativas permitidas de entrada da senha é de 10. Você pode alterar o número permitido de tentativas de entrada de senha, como descrito nesta seção.

Para alterar o número permitido de tentativas de entrada de senha:

1. No dispositivo do Servidor de Administração, execute uma linha de comando do Linux.

2. Para o utilitário klscflag, execute o seguinte comando:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

onde N é o número de tentativas de inserir uma senha.

3. Para aplicar as alterações, reinicie o serviço do Servidor de Administração.

O número máximo de tentativas permitidas de entrada da senha é alterado.

Excluir um usuário ou um grupo de segurança

Você pode excluir apenas usuários internos ou grupos de segurança internos.

Para excluir um usuário ou um grupo de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e selecione a guia **Usuários** ou **Grupos**.
2. Marque a caixa de seleção ao lado do usuário ou do grupo de segurança que deseja excluir.

   Sempre deve haver pelo menos um usuário com a autenticação de dois fatores configurada para que ele possa gerenciar a lista de permissão da autenticação de dois fatores e a lista de exclusão.

3. Clique no botão **Excluir**.
4. Na janela que se abre, clique em **OK**.

O usuário ou o grupo de segurança é excluído.

Alterar a senha de uma conta de usuário

Pode ser necessário alterar a senha de sua própria conta ou de outra conta de usuário caso a senha atual esteja prestes a expirar ou caso você queira alterá-la para uma mais segura.

A senha deve estar em conformidade com as seguintes regras:

- A senha deve ter de 8 a 256 caracteres.
- A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
  - Letras maiúsculas (A–Z)
  - Letras minúsculas (a-z)
  - Números (0–9)
  - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- A senha não pode conter espaços em branco, caracteres Unicode nem a combinação de "." e "@" quando o "." preceder o "@".

Alterar a senha da sua conta

Para editar a senha de sua conta:

1. No painel superior, acesse o menu da conta clicando no nome da conta.
2. Na lista suspensa, selecione **Alterar senha**.
3. No painel exibido à direita, insira a senha atual e especifique a nova senha para conectar ao Kaspersky Security Center Linux.

   Para ver a senha inserida, clique em .
4. Caso sua conta esteja protegida contra modificações não autorizadas, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da sua própria conta ou da conta que tem o direito Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário**.
5. Insira o código de segurança de uso único gerado pelo app autenticador no dispositivo móvel.

Alteração da senha de uma conta de usuário interna

Para editar a senha de uma conta de usuário interna:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e, em seguida, selecione a guia **Usuários**.
2. Clique no nome da conta de usuário que deseja editar.
3. Na janela de configurações do usuário que é aberta, na guia **Geral**, clique no botão **Alterar senha**.
4. Defina a nova senha para a conexão do usuário com o Kaspersky Security Center Linux.

   Para ver a senha inserida, clique em .
5. Caso necessário, ative a opção **O usuário deve alterar a senha no primeiro login** para forçar a alteração da senha na próxima autenticação do usuário.
6. Caso a conta de usuário esteja protegida contra modificações não autorizadas, será necessário confirmar que você tem as permissões para alterar essa conta. Na janela **Proteção da conta**, especifique as credenciais da conta que tem o direito Modificar ACLs de objetos na área funcional **Recursos gerais**: **Permissões do usuário**.
7. Insira o código de segurança de uso único gerado pelo app autenticador no dispositivo móvel.

Configuração das opções para alteração da senha usando sinalizadores do servidor

Execute a linha de comando e, em seguida, altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado no diretório onde o Agente de Rede está instalado. O diretório de instalação padrão é `/opt/kaspersky/ksc64/sbin`. Execute os seguintes comandos:

- Configuração do período de rotação da senha (o sinalizador `LP_SplPwdChangePeriodDays`)

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <período_de_rotação>`

  Em que `<período_de_rotação>` é um período em dias após o qual a senha do usuário expira. Valores possíveis: 0 a 730. Caso o valor do parâmetro seja 0, a rotação de senha será desativada.

- Configuração do tempo de aviso anterior sobre a necessidade de alterar a senha (o sinalizador `LP_SplPwdChangeNotificationHours`)

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <tempo_de_advertência>`

  Em que `<tempo_de_aviso>` é um período em horas antes que a senha do usuário expire. Durante esse tempo, a notificação sobre a necessidade de alteração da senha será exibida. Valores possíveis: 0 a 17520. Se o valor do parâmetro for 0, o tempo de advertência será de 25% do período de rotação da senha.

- Especificação do valor padrão da opção o **O usuário deve alterar a senha no primeiro login** (o sinalizador `LP_SplPwdForceChange`)

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <valor>`

  Em que os valores possíveis de `<valor>` do sinalizador:

  `1` - A opção **O usuário deve alterar a senha no primeiro login** está ativada.

  `0` - A opção **O usuário deve alterar a senha no primeiro login** está desativada.

Para visualizar o valor do sinalizador atual, execute o seguinte comando:

`./klscflag -fget -pv .core/.independent -s KLLIM -n <sinalizador> -t d`

Em que `<sinalizador>` é o `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` ou o sinalizador `LP_SplPwdForceChange`.

Criar uma função de usuário

Para criar uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique em **Adicionar**.
3. Na janela **Nome da nova função** exibida, digite o nome da nova função.
4. Clique em **OK** para aplicar as alterações.

5. Na janela de propriedades da função exibida, altere as configurações da função:

   - Na guia **Geral**, edite o nome da função.
     Você não pode editar o nome de uma função predefinida.
   - Na guia **Configurações**, edite o escopo da função e as políticas e os perfis associados à função.
   - Na guia **Direitos de acesso**, edite os direitos de acesso a aplicativos da Kaspersky.

6. Clique em **Salvar** para salvar as alterações.

A nova função aparece na lista de funções de usuário.

Editar uma função de usuário

Para editar uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função que deseja editar.
3. Na janela de propriedades da função exibida, altere as configurações da função:

   - Na guia **Geral**, edite o nome da função.
     Você não pode editar o nome de uma função predefinida.
   - Na guia **Configurações**, edite o escopo da função e as políticas e os perfis associados à função.
   - Na guia **Direitos de acesso**, edite os direitos de acesso a aplicativos da Kaspersky.

4. Clique em **Salvar** para salvar as alterações.

A função atualizada aparece na lista de funções de usuário.

Editar o escopo de uma função de usuário

O *escopo da função do usuário* é uma combinação de usuários e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

Para adicionar usuários, grupos de segurança e grupos de administração ao escopo de uma função de usuário, você pode usar qualquer dos seguintes métodos:

Método 1:

1. No menu principal, vá para **Usuários e funções** → **Usuários e grupos** e selecione a guia **Usuários** ou **Grupos**.
2. Marque as caixas de seleção ao lado dos usuários ou grupos de segurança que deseja adicionar ao escopo da função de usuário.
3. Clique no botão **Atribuir função**.

   O Assistente de Atribuição de Funções é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
4. Na etapa **Selecionar função**, selecione a função de usuário que deseja atribuir.
5. Na etapa **Definir escopo**, selecione o grupo de administração que deseja adicionar ao escopo da função de usuário.
6. Clique no botão **Atribuir função** para fechar a janela.

Os usuários ou os grupos de segurança selecionados e o grupo de administração selecionado são adicionados ao escopo da função de usuário.

Método 2:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função para a qual deseja definir o escopo.
3. Na janela de propriedades da função exibida, selecione a guia **Configurações**.
4. Na seção **Escopo da função**, clique em **Adicionar**.

   O Assistente de Atribuição de Funções é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
5. Na etapa **Definir escopo**, selecione o grupo de administração que deseja adicionar ao escopo da função de usuário.
6. Na etapa **Selecionar usuários**, selecione os usuários e os grupos de segurança que deseja adicionar ao escopo da função de usuário.
7. Clique no botão **Atribuir função** para fechar a janela.
8. Clique no botão **Fechar** (⨯) para fechar a janela de propriedades da função.

Os usuários ou os grupos de segurança selecionados e o grupo de administração selecionado são adicionados ao escopo da função de usuário.

Método 3:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Direitos de acesso**, marque a caixa ao lado do nome do usuário ou grupo de segurança que você deseja adicionar ao escopo da função do usuário e clique no botão **Funções**.

   Não é possível selecionar vários usuários ou grupos de segurança ao mesmo tempo. Caso mais de um item seja selecionado, o botão **Funções** será desativado.

3. Na janela **Funções**, selecione a função de usuário que deseja atribuir e, em seguida, aplique e salve as alterações.

   Os usuários ou os grupos de segurança selecionados são adicionados ao escopo da função de usuário.

Excluir uma função de usuário

Para excluir uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Marque a caixa de seleção ao lado do nome da função que deseja excluir.
3. Clique no botão **Excluir**.
4. Na janela que se abre, clique em **OK**.

A função de usuário é excluída.

Associação de perfis da política a funções

Você pode associar funções de usuário a perfis da política. Nesse caso, a regra de ativação desse perfil da política é baseada na função: o perfil da política fica ativo para um usuário com a função especificada.

Por exemplo, a política proíbe qualquer software de navegação de GPS em todos os dispositivos em um grupo de administração. O software de navegação de GPS é necessário em um dispositivo único no grupo de administração de Usuários, notadamente que for de propriedade do courier. Nesse caso, você pode atribuir uma função "Courier" ao seu proprietário e criar um perfil da política, permitindo que o software de navegação de GPS seja executado apenas nos dispositivos a cujos proprietários é atribuída a função "Courier". Todas as outras configurações de política são preservadas. Somente o usuário com a função "Courier" poderá executar o software de navegação de GPS. Depois, se outro funcionário receber a função "Courier", o novo funcionário também poderá executar o software de navegação no dispositivo da sua organização. Executar o software de navegação de GPS ainda será proibido em outros dispositivos no mesmo grupo de administração.

Para associar uma função a um perfil da política:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função que deseja associar a um perfil da política.

   A janela de propriedades da função é exibida com a guia **Geral** selecionada.

3. Selecione a guia **Configurações** e role para baixo até a seção **Políticas**.
4. Clique em **Editar**.

5. Para associar a função a:

   - **Um perfil da política existente** – Clique no ícone de insígnia (>) ao lado do nome de política necessário e marque a caixa de seleção ao lado do perfil ao qual você deseja associar a função.
   - **Um novo perfil da política**:

     a. Marque a caixa de seleção ao lado da política para a qual deseja criar um perfil.

     b. Clique em **Novo perfil de política**.

     c. Especifique um nome para o novo perfil e defina as configurações de perfil.

     d. Clique no botão **Salvar**.

     e. Selecione a caixa de seleção junto ao novo perfil.

6. Clique em **Atribuir à função**.

   O perfil é associado à função e aparece nas propriedades da função. O perfil se aplica automaticamente a qualquer dispositivo cujo proprietário seja atribuído à função.

Propagando funções de usuário aos Servidores de Administração secundários

Por padrão, as listas de funções de usuário dos Servidores de Administração principal e secundários são independentes. Você pode configurar o aplicativo para propagar automaticamente as funções de usuário criadas no Servidor de Administração principal a todos dos Servidores de Administração secundários. As funções de usuário também podem ser propagadas de um Servidor de Administração secundário para seus próprios Servidores de Administração secundários.

Para propagar funções de usuário do Servidor de Administração principal aos Servidores de Administração secundários:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Vá para a seção **Hierarquia de Servidores de Administração**.

3. Ative a opção **Retransmitir lista de funções para Servidores de Administração secundários** e depois clique no botão **Salvar**.

   O aplicativo copia as funções de usuário do Servidor de Administração principal para os Servidores de Administração secundários.

Quando a opção **Retransmitir lista de funções para Servidores de Administração secundários** for ativada e as funções do usuário forem propagadas, elas não poderão ser editadas nem excluídas nos Servidores de Administração secundários. Ao criar uma nova função ou editar uma função existente no Servidor de Administração principal, as modificações são automaticamente copiadas para os Servidores de Administração secundários. Ao excluir uma função de usuário no Servidor de Administração principal, essa função permanece nos Servidores de Administração secundários posteriormente, mas pode ser editada, nem excluída.

As funções propagadas do Servidor de Administração principal para o Servidor de Administração secundário serão exibidas com marcas de seleção verdes (✓). Você não pode editar essas funções no Servidor de Administração secundário.

Se você criar uma função no Servidor de Administração principal e existir uma função com o mesmo nome no Servidor de Administração secundário, a nova função será copiada para o Servidor de Administração secundário com o índice adicionado ao nome, por exemplo, ~~1, ~~2 (o índice pode ser aleatório).

Se você desativar a opção **Retransmitir lista de funções para Servidores de Administração secundários**, todas as funções do usuário permanecerão nos Servidores de Administração secundários, mas serão independentes das que estão no Servidor de Administração principal. Após se tornarem independentes, as funções de usuário nos Servidores de Administração secundários podem ser editadas ou excluídas.

Alterar a senha da conta

Você pode alterar a senha da conta local, por exemplo, quando o usuário esquece a senha da conta local ou para executar uma alteração de senha agendada.

A alteração da senha será aplicada mesmo se o usuário não tiver feito login na conta. Você também pode alterar a senha da conta raiz local.

Esta tarefa pode ser executada somente em dispositivos Linux.

Para alterar a senha da conta local em dispositivos específicos:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.
3. No campo **Tipo de tarefa**, selecione **Alterar a senha da conta (apenas Linux)**.
4. Escolha uma das seguintes opções:

   Atribuir tarefa a um grupo de administração

   A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

   Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

   Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

   Especificar endereços de dispositivos manualmente ou importar endereços de uma lista

   Você pode especificar nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

   Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

Atribuir tarefa a uma seleção de dispositivos

A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

A tarefa *Alterar senha da conta (somente Linux)* é criada para os dispositivos especificados. Se você selecionou a opção **Atribuir tarefa a um grupo de administração**, a tarefa será de grupo.

5. Na etapa **Escopo da tarefa**, especifique um grupo de administração, dispositivos com endereços específicos ou uma seleção de dispositivos gerenciados.

   As configurações disponíveis dependem da opção selecionada na etapa anterior.

6. Na etapa **Insira o nome da conta e a nova senha**, especifique as seguintes configurações:

   - No campo **Nome da conta**, especifique o nome da conta para a qual você deseja alterar a senha.
   - No campo **Nova senha**, especifique a senha que será definida para a conta especificada no campo anterior.

     Para ver os caracteres digitados, clique e pressione o botão **Mostrar**.
   - Se necessário, marque a caixa de seleção **Definir como uma senha única (o usuário deve alterar a senha após o primeiro login)**.

     Definir como uma senha única (o usuário deve alterar a senha após o primeiro login)

     Se esta caixa de seleção estiver marcada, o usuário será solicitado a definir uma nova senha após o primeiro login.

     Se esta caixa de seleção estiver desmarcada, o usuário não será solicitado a definir uma nova senha após o primeiro login.

     Por padrão, esta caixa de seleção está desmarcada.

7. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

   Se você ativou a opção **Abrir detalhes da tarefa quando a criação for concluída**, a janela de configurações da tarefa é aberta. Nesta janela, é possível verificar os parâmetros da tarefa, modificá-los ou configurar um cronograma de início da tarefa, caso necessário.

8. Na lista de tarefas, selecione a tarefa criada e clique em **Começar**.

   Como alternativa, aguarde que a tarefa seja inicializada de acordo com o agendamento especificado nas configurações da tarefa.

Quando a tarefa de alteração da senha da conta for concluída, a senha será alterada para a conta local especificada nos dispositivos especificados.

Para assegurar a operação correta das tarefas de alteração de senha da conta, o SELinux deve ser desativado no dispositivo do usuário.

Revogação de direitos de administrador local

Você pode revogar os direitos de administrador local das contas. Isso fornece uma camada extra de controle de contas de usuário. Por exemplo, você pode revogar os direitos de administrador local após a conclusão de uma atribuição única.

Quando esta tarefa é executada, a conta local especificada é verificada para ver se ela pertence a grupos de administradores locais. Esses grupos são definidos nas configurações da política do Agente de Rede. Você pode personalizar a lista de grupos de administradores locais nas configurações da política do Agente de Rede. Você também pode verificar a lista de contas de usuários privilegiados usando o **Relatório de usuários privilegiados dos dispositivos (apenas Linux)**.

Esta tarefa pode ser executada somente em dispositivos Linux.

Para revogar direitos de administrador local em dispositivos específicos:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.
3. No campo **Tipo de tarefa**, selecione **Revogar direitos do administrador local (apenas Linux)**.
4. Escolha uma das seguintes opções:

   Atribuir tarefa a um grupo de administração

   A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

   Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

   Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

   Especificar endereços de dispositivos manualmente ou importar endereços de uma lista

   Você pode especificar nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

   Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

   Atribuir tarefa a uma seleção de dispositivos

   A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

   Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

   A tarefa *Revogar direitos de administrador local (somente Linux)* é criada para os dispositivos especificados. Se você selecionou a opção **Atribuir tarefa a um grupo de administração**, a tarefa será de grupo.
5. Na etapa **Escopo da tarefa**, especifique um grupo de administração, dispositivos com endereços específicos ou uma seleção de dispositivos gerenciados.

   As configurações disponíveis dependem da opção selecionada na etapa anterior.
6. Nesta etapa do assistente, especifique as seguintes configurações:

   - No grupo de configurações **Modo de operação**, selecione o modo de operação:

Revogar os direitos do administrador local de contas listadas

Se esta opção for selecionada, os direitos de administrador local serão revogados das contas locais especificadas.

Por padrão, esta opção está selecionada.

Excluir contas listadas da revogação de direitos do administrador local

Se esta opção for selecionada, os direitos de administrador local serão revogados de todas as contas locais, exceto as especificadas.

Por padrão, esta opção não está selecionada.

- Especifique as contas locais:
  - Clique em **Adicionar**.
  - Na janela que se abre, execute uma das seguintes ações:
    - No campo **Nome da conta**, especifique o nome da conta local.
    - No grupo de configurações **Ação na conta** (disponível somente se a opção **Revogar os direitos do administrador local de contas listadas** estiver marcada), selecione a ação.
    - **Manter conta**

      Se esta opção for selecionada, a conta local não será excluída depois que os direitos de administrador local forem revogados.

      Por padrão, esta opção está selecionada.

    - **Excluir conta**

      Se esta opção for selecionada, a conta local será excluída independentemente de ter direitos de administrador local.

      Por padrão, esta opção não está selecionada.

7. Na etapa **Concluir a criação da tarefa**, clique no botão **Concluir** para criar a tarefa e fechar o assistente.

   Se você ativou a opção **Abrir detalhes da tarefa quando a criação for concluída**, a janela de configurações da tarefa é aberta. Nesta janela, é possível verificar os parâmetros da tarefa, modificá-los ou configurar um cronograma de início da tarefa, caso necessário.

8. Na lista de tarefas, selecione a tarefa criada e clique em **Começar**.

   Como alternativa, aguarde que a tarefa seja inicializada de acordo com o agendamento especificado nas configurações da tarefa.

Quando a tarefa Revogar direitos de administrador local for concluída, os direitos de administrador local serão revogados das contas locais especificadas nos dispositivos especificados.

Configuração da autenticação do domínio Kerberos

A Kaspersky Security Center Linux permite utilizar a autenticação do domínio por meio do protocolo Kerberos. A utilização da autenticação do domínio permite a autenticação segura no Kaspersky Security Center Web Console sem precisar inserir a senha novamente na rede corporativa (conexão única).

Você deve primeiro configurar o controlador de domínio para utilizar Kerberos e gerar um arquivo keytab. Para mais informações, consulte a documentação do controlador de domínio.

A configuração SCRIL (Smart Card Is Required for Interactive Logon) é compatível com o Microsoft Active Directory.

Gerar um arquivo keytab para FreeIPA e AldPro

Para gerar um arquivo keytab:

1. Crie uma conta de usuário a ser usada pelo IAM para acessar o controlador de domínio.

2. Se o Servidor de Administração estiver fora do domínio FreeIPA/AldPro, adicione a entrada do registro DNS e a entrada do host:

   ```
   ipa dnsrecord-add <zoneName> <recordName> --a-rec < endereço IP do Servidor de Administração >
   ```

   ```
   ipa host-add --password=<password> < endereço do host do Servidor de Administração >
   ```

3. Especifique o tipo de PAC ao criar o serviço HTTP para o Servidor de Administração:

   ```
   ipa service-add HTTP/< FQDN do host do Servidor de Administração >@< DOMÍNIO ESCRITO EM LETRAS MAIÚSCULAS > --ok-to-auth-as-delegate=true --pac-type PAD
   ```

4. Especifique a conta de usuário para autenticação:

   ```
   ipa service-allow-retrieve-keytab HTTP/< endereço do host do Servidor de Administração >@< DOMÍNIO ESCRITO EM LETRAS MAIÚSCULAS > --user=<user>
   ```

5. Exporte o arquivo keytab:

   ```
   ipa-getkeytab -s < endereço do controlador de domínio > -p HTTP/< endereço do host do Servidor de Administração >@< DOMÍNIO ESCRITO EM LETRAS MAIÚSCULAS > -k /tmp/h.keytab
   ```

Gerar um arquivo keytab para o Microsoft Active Directory

Para gerar um arquivo keytab:

1. Crie uma conta de usuário a ser usada pelo IAM para se comunicar com o controlador de domínio.

2. Ative as seguintes opções para a conta de usuário:

   - **O usuário não pode alterar a senha**
   - **Criptografia Kerberos AES de 256 bits**

   Você pode ativar a opção **A senha nunca expira** para evitar que o arquivo keytab seja emitido novamente sempre que a senha expirar.

3. Adicione um Nome Principal de Serviço (SPN) à conta de usuário:

   ```
   setspn -S HTTP/<FQDN do host do Servidor de Administração> <DOMÍNIO ESCRITO EM LETRAS MAIÚSCULAS>\<user>
   ```

4. Exporte o arquivo keytab:

   ```
   ktpass -out C:\<folder>\<nome do arquivo keytab> -princ HTTP/<FQDN do host do Servidor de Administração>@<DOMÍNIO ESCRITO EM LETRAS MAIÚSCULAS> -mapuser <DOMÍNIO ESCRITO EM LETRAS MAIÚSCULAS>\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <password> -mapop set
   ```

Gerar um arquivo keytab para o Samba

Para gerar um arquivo keytab:

1. Crie uma conta de usuário a ser usada pelo IAM para se comunicar com o controlador de domínio:

   ```
   samba-tool user add <user>
   ```

2. Adicione o SPN à conta de usuário:

   ```
   samba-tool spn add HTTP/<FQDN do host do Servidor de Administração> <user>
   ```

3. Exporte o arquivo keytab:

   ```
   samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/<FQDN do host do Servidor de Administração>
   ```

Configurar a autenticação do domínio Kerberos

Para ativar a autenticação do domínio Kerberos:

1. Fazer a sondagem do controlador de domínio.
2. No menu principal, vá para a seção **Configurações** → **Conexão única**.
3. Ative a opção **Autenticação Kerberos**.
4. Carregue o arquivo keytab.
5. Atribua uma função aos usuários do domínio que dê acesso ao Kaspersky Security Center Web Console.

   A autenticação do domínio Kerberos é ativada para os usuários do domínio.

Atualização dos bancos de dados e dos aplicativos da Kaspersky

Esta seção descreve as etapas que você deve seguir para atualizar regularmente o seguinte:

- Bancos de dados e módulos de software da Kaspersky
- Aplicativos Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center Linux

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Cenário: Atualização regular dos bancos de dados e dos aplicativos Kaspersky

Esta seção fornece um cenário para a atualização regular de bancos de dados, módulos de software e aplicativos da Kaspersky. Após ter concluído o Cenário de configuração de proteção da rede, você precisará manter a confiabilidade do sistema de proteção para ter certeza de que os Servidores de Administração e os dispositivos gerenciados estejam permanentemente protegidos contra várias ameaças, incluindo vírus, ataques à rede e ataques de phishing.

A proteção da rede é mantida atualizada por atualizações regulares dos seguintes:

- Bancos de dados e módulos de software da Kaspersky
- Aplicativos Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center Linux

Quando concluir este cenário, você poderá ter certeza do seguinte:

- A sua rede está protegida pelo software da Kaspersky mais recente, inclusive aplicativos de segurança e componentes do Kaspersky Security Center Linux.
- Os bancos de dados de antivírus e outros bancos de dados da Kaspersky críticos para a segurança de rede são sempre atualizados.

Pré-requisitos

Os dispositivos gerenciados devem ter uma conexão com o Servidor de Administração. Se eles não tiverem uma conexão, considere atualizar os bancos de dados da Kaspersky e módulos do software manualmente ou diretamente dos servidores de atualização Kaspersky.

O Servidor de Administração deve ter uma conexão com a Internet.

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

1. Implementado os aplicativos de segurança da Kaspersky nos dispositivos gerenciados de acordo com o cenário de implementação de aplicativos Kaspersky através do Kaspersky Security Center Web Console.
2. Criado e configurado todos os perfis da política, políticas e tarefas necessários segundo o cenário de configuração da proteção de rede.
3. Atribuído um volume apropriado de pontos de distribuição conforme o número de dispositivos gerenciados e a topologia de rede.

A atualização dos bancos de dados e dos aplicativos da Kaspersky prossegue em estágios:

1. **Seleção de um esquema de atualização**

   Há vários esquemas que você pode usar para instalar atualizações para aplicativos de segurança. Selecione o esquema ou vários esquemas que atendem aos requisitos de sua melhor rede.

2. **Criar a tarefa para baixar as atualizações no repositório do Servidor de Administração**

   Essa tarefa é criada automaticamente pelo assistente de início rápido do Kaspersky Security Center. Se você não tiver executado o assistente, crie a tarefa agora.

   Essa tarefa é necessária para baixar atualizações de servidores de atualização da Kaspersky para o repositório do Servidor de Administração e para atualizar os bancos de dados e módulos do software da Kaspersky para o Kaspersky Security Center Linux. Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

   Se a rede tiver pontos de distribuição atribuídos, as atualizações serão baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Nesse caso, os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.

   Instruções: Como criar a tarefa para baixar as atualizações para o repositório do Servidor de Administração

3. **Criar a tarefa para baixar as atualizações para os repositórios de pontos de distribuição (opcional)**

   Por padrão, as atualizações são baixadas para os pontos de distribuição do Servidor de Administração. É possível configurar o Kaspersky Security Center Linux para baixar as atualizações para os pontos de distribuição diretamente dos servidores de atualização Kaspersky. Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.

   Quando a rede tiver atribuído pontos de distribuição e a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for criada, os pontos de distribuição baixarão atualizações dos servidores de atualização da Kaspersky e não do repositório do Servidor de Administração.

   Instruções: Como criar a tarefa para baixar atualizações nos repositórios dos pontos de distribuição

4. **Configurar os pontos de distribuição**

   Quando a sua rede tem pontos de distribuição atribuídos, certifique-se de que a opção **Ativado** esteja ativada nas propriedades de todos os pontos de distribuição necessários. Quando essa opção é desativada para um ponto de distribuição, os dispositivos incluídos no escopo das atualizações de download do ponto de distribuição do repositório do Servidor de Administração.

5. **Como otimizar o processo de atualização usando os arquivos diff (opcional)**

   Você pode otimizar o tráfego entre o Servidor de Administração e os dispositivos gerenciados usando arquivos diff. Quando esse recurso for ativado, o Servidor de Administração ou um ponto de distribuição baixará arquivos diff em vez de arquivos inteiros de bancos de dados ou módulos de software da Kaspersky. Um arquivo diff descreve as diferenças entre duas versões de um arquivo de banco de dados ou módulo de software. Por isso, um arquivo diff ocupa menos espaço do que um arquivo inteiro. Isso resulta na redução no tráfego entre o Servidor de Administração ou os pontos de distribuição e os dispositivos gerenciados. Para usar esse recurso, ative a opção **Baixar arquivos diff** nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e/ou da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.

   Instruções: Uso de arquivos diff para atualizar bancos de dados e módulos do software da Kaspersky

6. **Configuração da instalação automática de atualizações para os aplicativos de segurança**

   Crie a tarefa *Atualizar* para os aplicativos gerenciados para fornecer atualizações oportunas para os módulos do software e bancos de dados Kaspersky, inclusive bancos de dados de antivírus. Para assegurar atualizações oportunas, recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório** ao configurar a programação de tarefa.

   Se uma atualização necessitar de análise e aceitação dos termos do Contrato de Licença do Usuário Final, você primeiro precisará aceitar os termos. Depois disso, a atualização poderá ser propagada para os dispositivos gerenciados.

7. **Aprovar e recusar atualizações de aplicativos Kaspersky gerenciados**

   Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Você pode alterar o status para *Aprovado* ou *Negado*. As atualizações aprovadas sempre são instaladas. Se uma atualização de um aplicativo da Kaspersky gerenciado exigir a revisão e aceitação dos termos do Contrato de Licença do Usuário Final, primeiro você precisará aceitar os termos. Depois disso, a atualização poderá ser propagada para os dispositivos gerenciados. As atualizações para as quais você define o status *Negado* não serão instaladas em dispositivos. Se uma atualização recusada para um aplicativo gerenciado tiver sido instalada anteriormente, o Kaspersky Security Center Linux tentará desinstalar a atualização de todos os dispositivos.

   A aprovação e a recusa de atualizações estão disponíveis apenas para o Agente de Rede e os aplicativos gerenciados da Kaspersky que estejam instalados em dispositivos clientes baseados em Windows e Linux. A atualização contínua do Servidor de Administração, do Kaspersky Security Center Web Console e dos plug-ins da web de gerenciamento não é compatível.

   Instruções: Aprovar e recusar atualizações de software

   Às vezes, após a atualização do Agente de Rede, você pode receber uma solicitação para reiniciar os dispositivos gerenciados. Se a notificação sobre a reinicialização necessária for exibida, clique no link **Visualizar dispositivos** na notificação, marque as caixas de seleção ao lado dos dispositivos a serem reiniciados e clique no botão **Reiniciar** para concluir a atualização do Agente de Rede.

Resultados

Após a conclusão do cenário, o Kaspersky Security Center Linux é configurado para atualizar os bancos de dados da Kaspersky após as atualizações serem baixadas para o repositório do Servidor de Administração. Você poderá prosseguir para monitorar o status da rede.

Sobre atualização de bancos de dados, módulos de software e aplicativos da Kaspersky

Para ter certeza de que a proteção dos seus Servidores de Administração e dispositivos gerenciados esteja atualizada, você deverá fornecer atualizações oportunas dos seguintes:

- Bancos de dados e módulos de software da Kaspersky

  Antes de baixar os bancos de dados e módulos de software da Kaspersky, o Kaspersky Security Center Linux verifica se os servidores da Kaspersky estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos. Isso é necessário para garantir que os bancos de dados antivírus sejam atualizados e que o nível de segurança seja mantido para os dispositivos gerenciados.

- Aplicativos Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center Linux

  O Kaspersky Security Center Linux permite atualizar automaticamente o Agente de Rede e os aplicativos da Kaspersky instalados em dispositivos clientes baseados no Windows e no Linux. A atualização contínua do Servidor de Administração, do Kaspersky Security Center Web Console e dos plug-ins da web de gerenciamento não é compatível. Para atualizar esses componentes, você deve baixar as versões mais recentes do site da Kaspersky e, em seguida, instalá-las manualmente.

Dependendo da configuração da rede, você pode usar os seguintes esquemas de download e distribuição das atualizações necessárias para os dispositivos gerenciados:

- Usando uma única tarefa: *Baixar atualizações no repositório do Servidor de Administração*
- Usando duas tarefas:
  - A tarefa *Baixar atualizações no repositório do Servidor de Administração*
  - A tarefa *Baixar atualizações para os repositórios de pontos de distribuição*
- Manualmente por meio de uma pasta compartilhada ou de um servidor FTP
- Diretamente dos servidores de atualização da Kaspersky para o Kaspersky Endpoint Security nos dispositivos gerenciados
- Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Usando a tarefa Baixar atualizações no repositório do Servidor de Administração

Nesse esquema, o Kaspersky Security Center Linux baixa as atualizações por meio da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Em redes pequenas que contêm menos de 300 dispositivos gerenciados em um segmento de rede único ou menos de 10 dispositivos gerenciados em cada segmento de rede, as atualizações são distribuídas aos dispositivos gerenciados diretamente do repositório do Servidor de Administração (veja a figura abaixo).



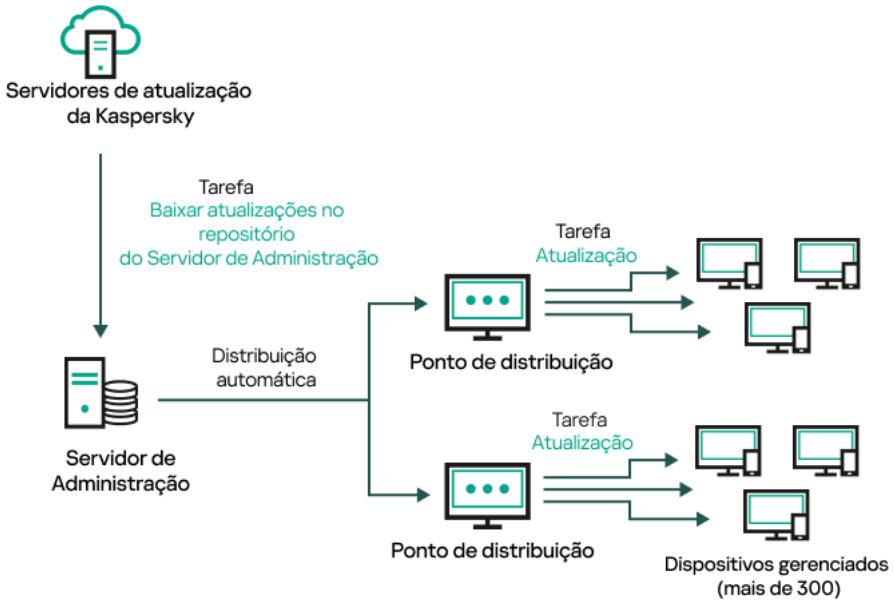
Atualizando usando a tarefa *Baixar atualizações no repositório do Servidor de Administração* sem pontos de distribuição

Como uma fonte de atualizações, é possível usar não somente os servidores de atualização Kaspersky, mas também uma pasta local ou de rede.

Por padrão, o Servidor de Administração comunica-se com os servidores de atualização Kaspersky e baixa as atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração para usar o protocolo HTTP em vez de HTTPS.

Caso a rede contenha 300 dispositivos gerenciados ou mais em um segmento de rede único ou caso a rede consista em vários segmentos de rede com mais de 9 dispositivos gerenciados em cada segmento de rede, recomendamos o uso de pontos de distribuição para propagar as atualizações aos dispositivos gerenciados (veja a figura abaixo). Os pontos de distribuição reduzem a carga no Servidor de Administração e otimizam o tráfego entre o Servidor de Administração e os dispositivos gerenciados. Você pode calcular o número e a configuração de pontos de distribuição necessários para a rede.

Nesse esquema, as atualizações são baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.



Atualizando usando a tarefa *Baixar atualizações no repositório do Servidor de Administração* com pontos de distribuição

Quando a tarefa *Baixar atualizações no repositório do Servidor de Administração* estiver concluída, as atualizações dos bancos de dados da Kaspersky e módulos de software do Kaspersky Endpoint Security serão baixados para o repositório do Servidor de Administração. Essas atualizações são instaladas por meio da tarefa de *Atualização* para o Kaspersky Endpoint Security.

A tarefa *Baixar atualizações para o repositório do Servidor de Administração* não está disponível nos Servidores de Administração virtuais. O repositório do Servidor de Administração virtual exibe as atualizações baixadas para o Servidor de Administração principal.

Você pode configurar as atualizações a serem verificadas quanto a operabilidade e erros em um conjunto de dispositivos de teste. Se a verificação for bem-sucedida, as atualizações serão distribuídas para outros dispositivos gerenciados.

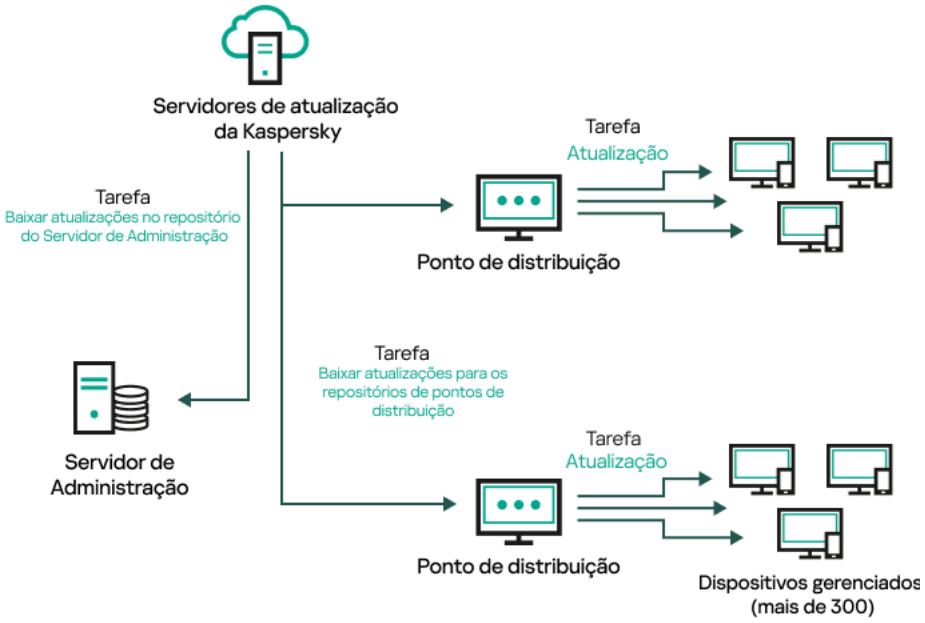
Cada aplicativo da Kaspersky solicita as atualizações necessárias do Servidor de Administração. O Servidor de Administração agrega essas solicitações e baixa somente as que são solicitadas por qualquer aplicativo. Isso garante que as mesmas atualizações não sejam baixadas várias vezes e impede que as atualizações desnecessárias sejam baixadas. Ao executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, o Servidor de Administração envia automaticamente as seguintes informações para os servidores de atualização da Kaspersky para assegurar o download das versões relevantes dos bancos de dados e dos módulos de software da Kaspersky:

- ID e versão do aplicativo
- ID de configuração do aplicativo
- ID da chave ativa
- ID de execução da tarefa *Baixar atualizações para o repositório do Servidor de Administração*

Nenhuma das informações transmitidas contém informações pessoais ou outros dados confidenciais. A AO Kaspersky Lab protege as informações de acordo com os requisitos estabelecidos por lei.

Usando duas tarefas: a tarefa Baixar atualizações no repositório do Servidor de Administração e a tarefa Baixar atualizações para os repositórios de pontos de distribuição

Você pode baixar atualizações para os repositórios de pontos de distribuição diretamente dos servidores de atualização Kaspersky em vez de do repositório do Servidor de Administração e distribuir as atualizações para os dispositivos gerenciados (veja a figura abaixo). Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.



Atualização usando a tarefa *Baixar atualizações no repositório do Servidor de Administração* e a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*

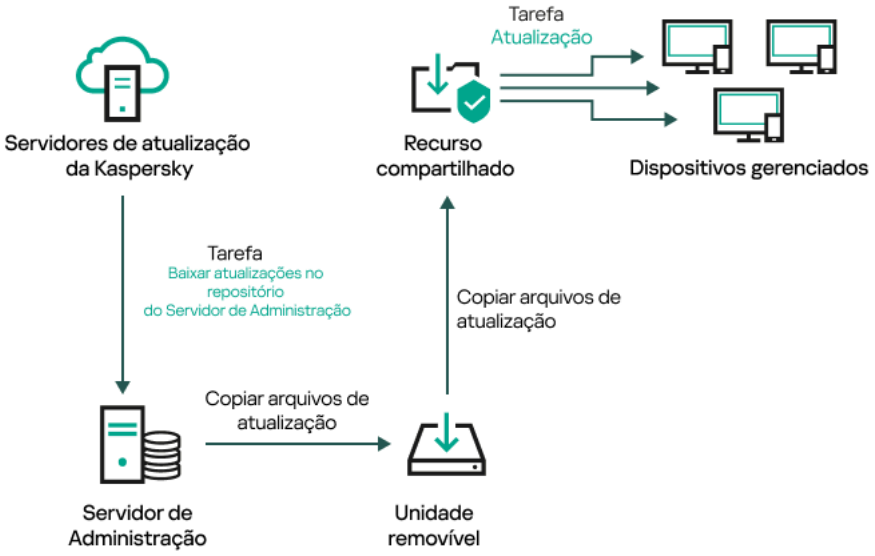
Por padrão, o Servidor de Administração e os pontos de distribuição comunicam-se com Servidores de atualização Kaspersky e baixam de atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração e/ou os pontos de distribuição para usar o protocolo HTTP em vez de HTTPS.

Para implementar esse esquema, crie a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* além da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Depois disso, os pontos de distribuição baixarão atualizações dos servidores de atualização Kaspersky e não do repositório do Servidor de Administração.

A tarefa *Baixar atualizações no repositório do Servidor de Administração* também é necessária para esse esquema, porque essa tarefa é usada para baixar módulos de software e bancos de dados da Kaspersky para o Kaspersky Security Center Linux.

Manualmente por meio de uma pasta compartilhada ou de um servidor FTP

Se os dispositivos cliente não tiverem uma conexão com o Servidor de Administração, você poderá usar uma pasta local ou um recurso compartilhado como uma origem para atualizar bancos de dados, módulos de software e aplicativos Kaspersky. Nesse esquema, você precisa copiar as atualizações necessárias do repositório do Servidor de Administração para uma unidade removível e depois copiar as atualizações para a pasta local ou o recurso compartilhado especificado como uma fonte de atualização nas configurações do Kaspersky Endpoint Security (veja a figura abaixo).



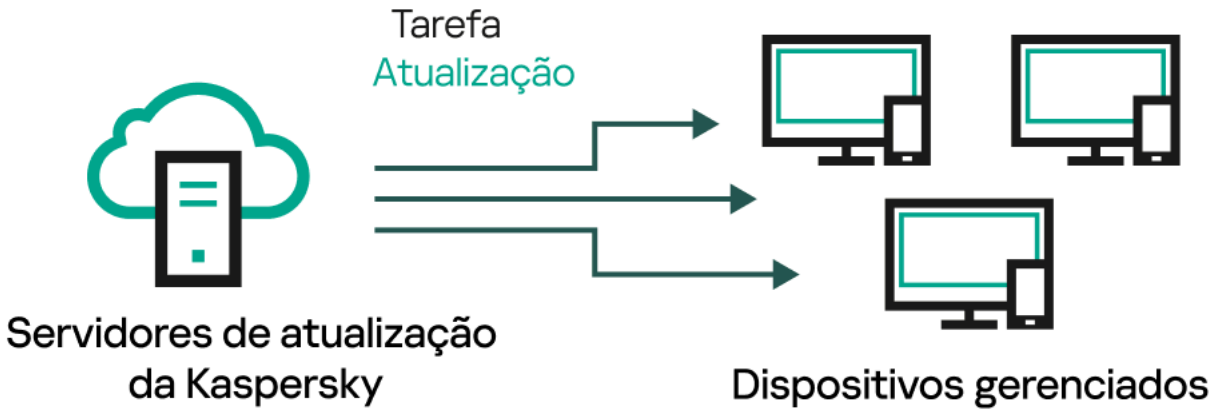
Atualização por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

Para obter mais informações sobre fontes de atualizações no Kaspersky Endpoint Security, consulte a seguinte ajuda:

- Ajuda do Kaspersky Endpoint Security for Linux
- Ajuda do Kaspersky Endpoint Security for Windows

Diretamente dos servidores de atualização da Kaspersky para o Kaspersky Endpoint Security nos dispositivos gerenciados

Nos dispositivos gerenciados, você pode configurar o Kaspersky Endpoint Security para receber atualizações diretamente dos servidores de atualização da Kaspersky (veja a figura abaixo).



Atualização de aplicativos de segurança diretamente dos servidores de atualização da Kaspersky

Nesse esquema, o aplicativo de segurança não usa os repositórios fornecidos pelo Kaspersky Security Center Linux. Para receber atualizações diretamente dos servidores de atualização da Kaspersky, especifique os servidores de atualização da Kaspersky como uma fonte de atualização no aplicativo de segurança. Para obter mais informações sobre essas configurações, consulte as seguintes ajudas:

- Ajuda do Kaspersky Endpoint Security for Linux
- Ajuda do Kaspersky Endpoint Security for Windows

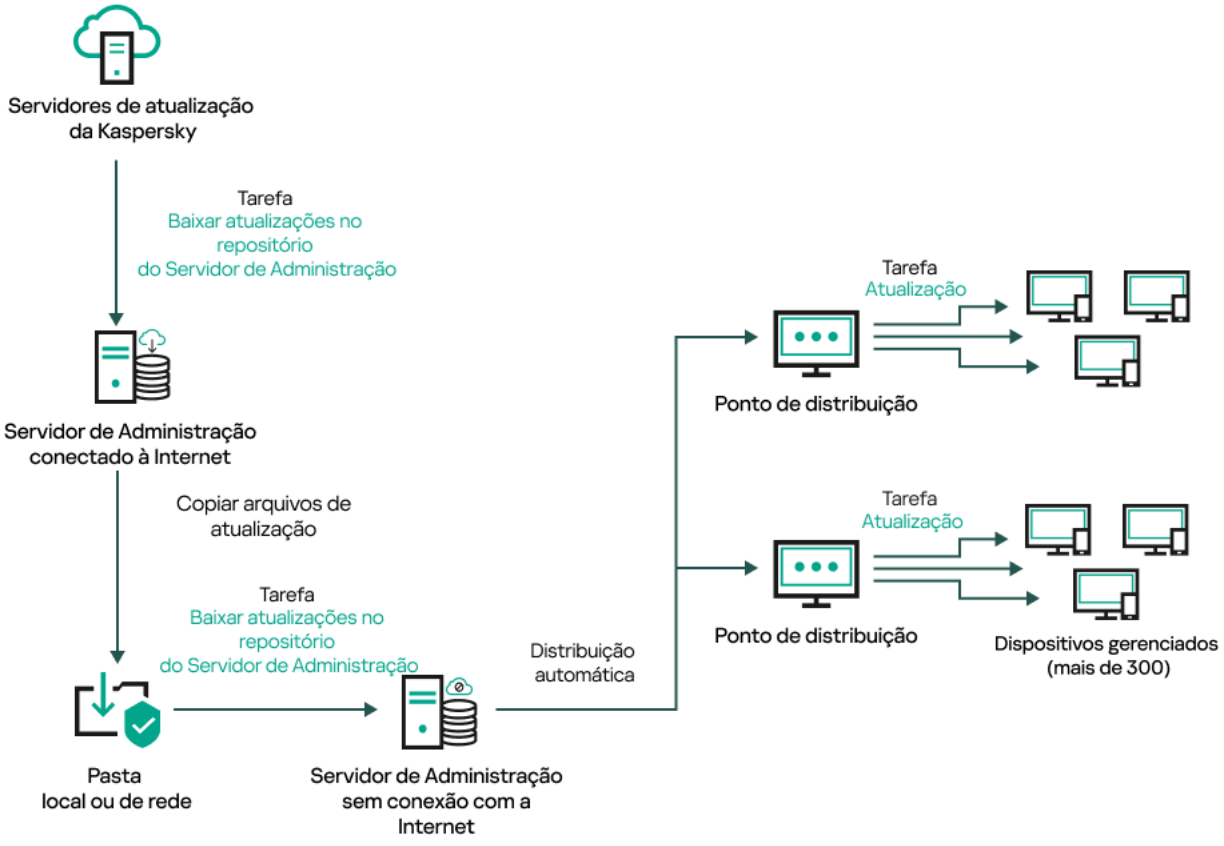
Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Se o Servidor de Administração não tiver conexão com a Internet, você poderá configurar a tarefa *Baixar atualizações no repositório do Servidor de Administração* para baixar atualizações de uma pasta local ou de rede. Nesse caso, você deve copiar os arquivos de atualização necessários para a pasta especificada de tempos em tempos. Por exemplo, você pode copiar os arquivos de atualização necessários de uma das seguintes fontes:

- Servidor de Administração que possui conexão com a Internet (veja a figura abaixo)

  Como um Servidor de Administração baixa apenas as atualizações solicitadas pelos aplicativos de segurança, os conjuntos de aplicativos de segurança gerenciados pelos Servidores de Administração (o que tem conexão com a Internet e o que não tem) devem corresponder.

  Se o Servidor de Administração que você usa para baixar atualizações tiver a versão 13.2 ou anterior, abra as propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e, em seguida, ative a opção **Baixar atualizações usando o esquema antigo**.



Atualização por meio de uma pasta de rede se o Servidor de Administração não tiver conexão com a Internet

- Utilitário de atualização da Kaspersky

  Como este utilitário usa o esquema antigo para baixar atualizações, abra as propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e, em seguida, ative a opção *Baixar atualizações usando o esquema antigo*. Se desejar, você também pode configurar a opção *Baixar o arquivo de solicitação de atualização automaticamente* para que o Utilitário de Atualização do Kaspersky só baixe as atualizações necessárias.

Criação da tarefa baixar atualizações no repositório do Servidor de Administração

A tarefa *Baixar atualizações no repositório do Servidor de Administração* permite baixar atualizações de bancos de dados e módulos de software do aplicativos de segurança do Kaspersky a partir dos servidores de atualização do Kaspersky para o repositório do Servidor de Administração.

A tarefa *Baixar atualizações no repositório do Servidor de Administração* é criada automaticamente quando o Servidor de Administração é iniciado pela primeira vez. Na lista de tarefas, só pode haver uma tarefa *Baixar atualizações no repositório do Servidor de Administração*. É possível criar esta tarefa novamente caso ela seja removida da lista de tarefas do Servidor de Administração.

Após a tarefa *Baixar atualizações no repositório do Servidor de Administração* ser concluída e as atualizações forem baixadas, elas poderão ser propagadas aos dispositivos gerenciados.

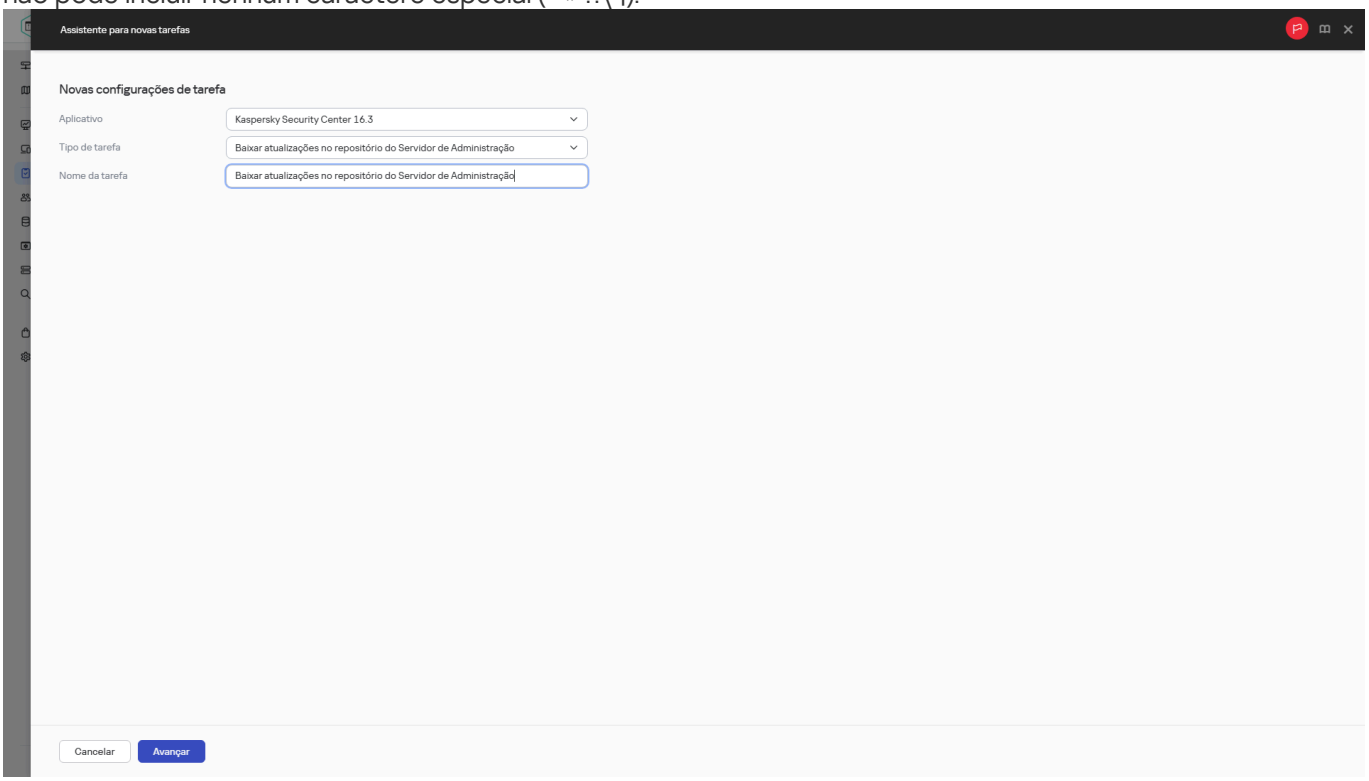
Antes de distribuir as atualizações para os dispositivos gerenciados, é possível executar a tarefa de *Verificação de atualizações*. Isso permite ter a certeza de que o Servidor de Administração instalará as atualizações baixadas corretamente e que um nível de segurança não diminuirá devido às atualizações. Para verificá-las antes de distribuir, configure a opção **Executar verificação de atualizações** nas configurações de tarefas *Baixar atualizações no repositório do Servidor de Administração*.

Para criar uma tarefa Baixar atualizações no repositório do Servidor de Administração:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

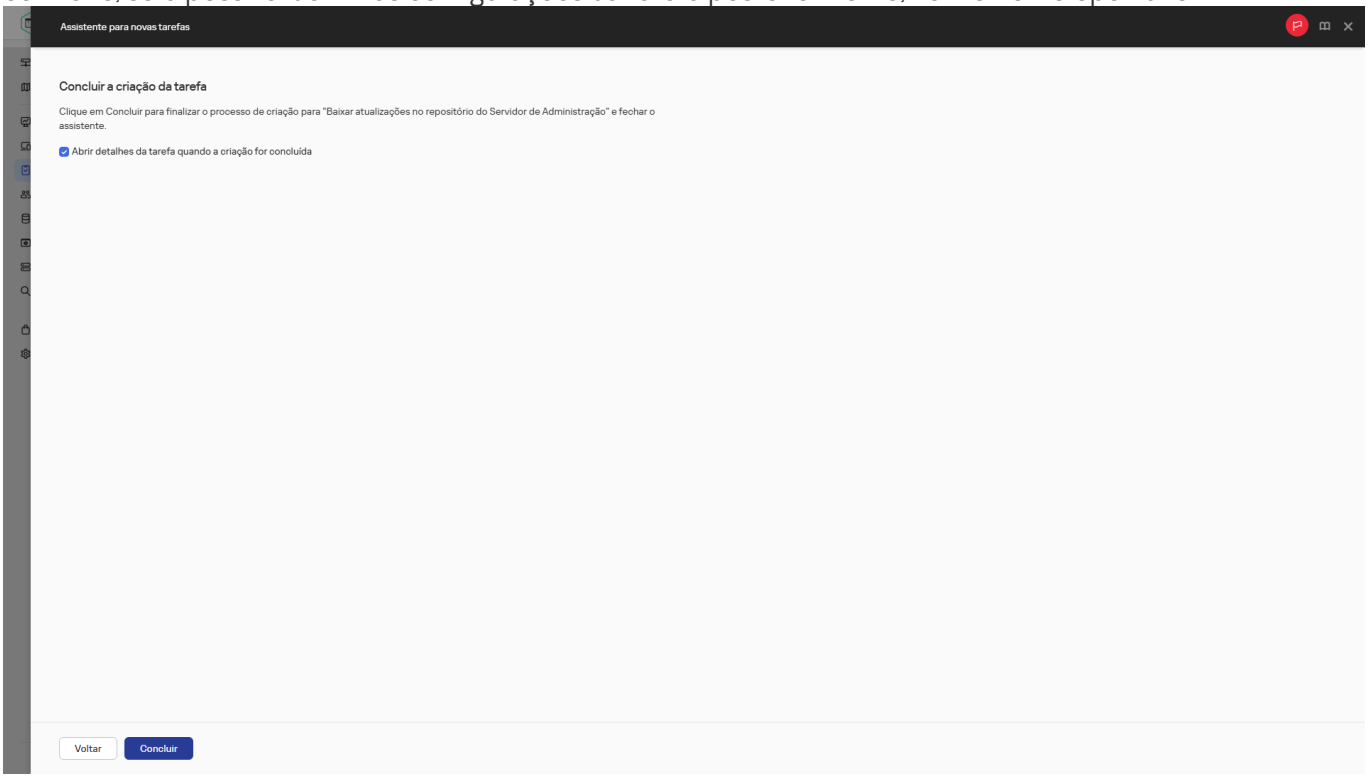
   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Baixar atualizações no repositório do Servidor de Administração**.

4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).



Criação da tarefa baixar atualizações no repositório do Servidor de Administração

5. Na página **Concluir a criação da tarefa**, é possível ativar a opção **Abrir detalhes da tarefa quando a criação for concluída** para abrir a janela de propriedades da tarefa e modificar as configurações padrão da tarefa. Caso contrário, será possível definir as configurações da tarefa posteriormente, no momento oportuno.



Finalização da criação da tarefa

6. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.

7. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

8. Na janela de propriedades da tarefa, na guia **Configurações do aplicativo**, especifique as seguintes configurações:

Fontes de atualizações

Como uma fonte de atualizações, você pode usar:

- Servidores de atualização Kaspersky (selecionados por padrão)
- Servidor de Administração principal

  Este recurso é aplicado a tarefas criadas para um Servidor de Administração virtual ou secundário.
- Pasta local ou de rede

  Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Uma pasta de rede pode ser um servidor FTP ou HTTP, ou um compartilhamento SMB.

  Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado. O caminho para a pasta depende do sistema operacional do dispositivo. Como a pasta local está localizada no Servidor de Administração baseado em Linux, você precisa especificar o caminho POSIX, por exemplo: /caminho/para/diretório.

  Ao selecionar uma pasta de rede SMB como fonte de atualização, monte a pasta no dispositivo em que o Servidor de Administração está instalado antes de selecioná-la. Em seguida, especifique o caminho para a pasta montada usando o respectivo caminho no sistema de arquivos local. O acesso à pasta é realizado usando o protocolo SMB.

  > Uma pasta local ou de rede ou um servidor FTP ou HTTP usado como fonte de atualização deve conter uma estrutura de pastas que corresponda à estrutura de pastas dos servidores de atualização Kaspersky. Você pode obter essa estrutura usando o Kaspersky Update Utility.

> Na tarefa *Baixar atualizações no repositório do Servidor de Administração* e na tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a autenticação do usuário não funcionará se for selecionada uma pasta local ou de rede protegida por senha como fonte de atualização. Para resolver esse problema, primeiro monte a pasta protegida por senha e, em seguida, especifique as credenciais necessárias, por exemplo, por meio do sistema operacional. Depois disso, será possível selecionar essa pasta como fonte de atualização em uma tarefa de download de atualizações. O Kaspersky Security Center Linux não solicitará a inserção das credenciais.

Pasta para armazenar atualizações

O caminho para a pasta especificada para armazenar as atualizações salvas. É possível copiar o caminho da pasta especificada para uma área de transferência. Não é possível alterar o caminho para uma pasta especificada para uma tarefa de grupo.

Forçar a atualização de Servidores de Administração secundários

Caso esta opção esteja ativada, o Servidor de Administração inicia as tarefas de atualização nos Servidores de Administração secundários assim que as novas atualizações são baixadas. As tarefas de atualização são iniciadas usando a fonte de atualização configurada nas propriedades da tarefa nos Servidores de Administração secundários.

Caso esta opção esteja desativada, as tarefas de atualização nos Servidores de Administração secundários serão iniciadas de acordo com seus agendamentos.

Por padrão, esta opção está desativada.

Copiar as atualizações baixadas em pastas adicionais

Após recepção das atualizações pelo Servidor de Administração, estas são copiadas para as pastas especificadas. Use esta opção se você deseja gerenciar manualmente a distribuição das atualizações na rede.

Por exemplo, você pode desejar usar esta opção na seguinte situação: a rede de sua organização consiste em várias sub-redes independentes e os dispositivos de cada uma das sub redes não têm acesso a outras sub-redes. Entretanto, os dispositivos em todas das sub-redes têm acesso a um compartilhamento de rede comum. Neste caso, você define o Servidor de Administração em uma das sub-redes para baixar atualizações dos Servidores de Atualização Kaspersky, ativar essa opção e especificar esse compartilhamento de rede. Nas atualizações baixadas para as tarefas de repositório de outros Servidores de Administração, especifique o mesmo compartilhamento de rede como a origem da atualização.

Se você selecionar copiar as atualizações baixadas para uma pasta local, deverá especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado. O caminho para a pasta depende do sistema operacional do dispositivo. Como a pasta local está localizada no Servidor de Administração baseado em Linux, você precisa especificar o caminho POSIX, por exemplo: /caminho/para/diretório.

Ao selecionar uma pasta de rede localizada no Servidor de Administração do Linux, você deve primeiro garantir o acesso à pasta de rede no dispositivo onde o Servidor de Administração está instalado, montando a pasta. O acesso à pasta é realizado usando o protocolo SMB.

Por padrão, esta opção está desativada.

Baixar arquivos diff

Esta opção ativa o recurso de download dos arquivos diff.

Por padrão, esta opção está desativada.

Baixar atualizações usando o esquema antigo

A partir da versão 14, o Kaspersky Security Center baixa as atualizações de bancos de dados e os módulos de software usando o novo esquema. Para que o aplicativo baixe atualizações usando o novo esquema, a fonte de atualização deve conter os arquivos de atualização com os metadados compatíveis com o novo esquema. Caso a fonte de atualização contenha os arquivos de atualização com os metadados compatíveis apenas com o esquema antigo, ative a opção **Baixar atualizações usando o esquema antigo**. Caso contrário, a tarefa de download de atualizações falhará.

Por exemplo, é preciso habilitar essa opção quando uma pasta local ou de rede for especificada como fonte de atualização, e os arquivos de atualização nesta pasta tiverem sido baixados por um dos seguintes aplicativos:

- Utilitário de atualização da Kaspersky

  Esse utilitário baixa as atualizações usando o esquema antigo.

- Kaspersky Security Center 13 Linux

  Por exemplo, o Servidor de Administração 1 não possui uma conexão com a Internet. Nesse caso, é possível baixar as atualizações usando o Servidor de Administração 2, desde que ele tenha conexão com a Internet e, em seguida, colocar as atualizações em uma pasta local ou de rede para usá-la como fonte de atualização para o Servidor de Administração 1. Caso o Servidor de Administração 2 tenha a versão 13, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa para o Servidor de Administração 1.

Por padrão, esta opção está desativada.

Executar verificação de atualizações

O Servidor de Administração baixa as atualizações da fonte, salva-as num repositório temporário e executa a tarefa definida no campo **Tarefa de verificação de atualizações**. Se a tarefa for concluída com êxito, as atualizações serão copiadas do repositório temporário para uma pasta compartilhada no Servidor de Administração e distribuídas a todos os dispositivos para os quais o Servidor de Administração atua como a fonte de atualizações (tarefas com o agendamento de **Quando novas atualizações são baixadas no repositório** forem iniciadas). A tarefa de download de atualizações para o repositório é concluída somente após o término da *Tarefa de verificação de atualizações*.

Por padrão, esta opção está desativada.

Baixe o arquivo de solicitação de atualização automaticamente

Se você quiser que o Utilitário de Atualização do Kaspersky baixe apenas as atualizações necessárias com a configuração adequada, ative esta opção e especifique o caminho onde o Kaspersky Security Center Linux criará o arquivo de solicitação de atualização com informações sobre as atualizações a serem baixadas. O arquivo de solicitação de atualização contém o carimbo de data e hora e o hash MD5 para controle de versão.

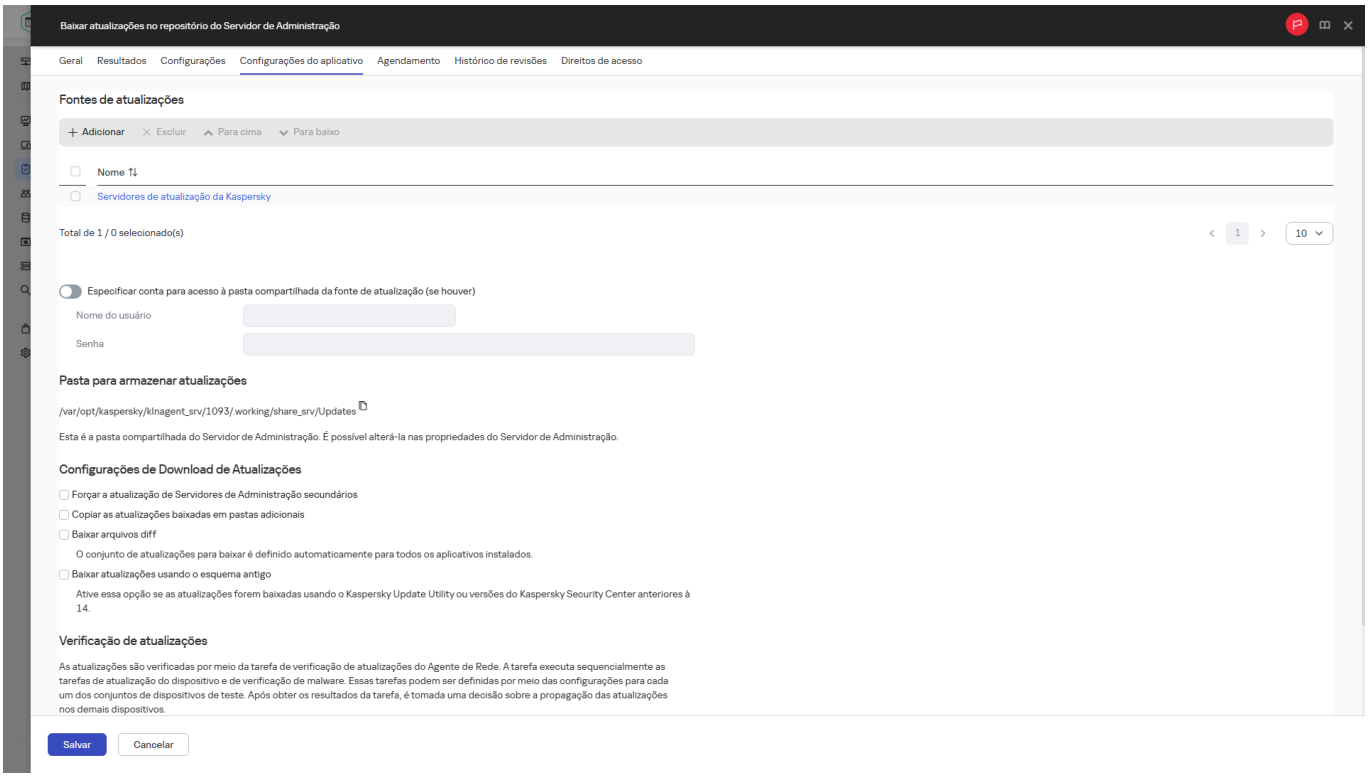
A opção **Baixar atualizações usando o esquema antigo** deve estar desativada.

Além disso, o download da atualização no Utilitário de Atualização da Kaspersky deve ser configurado.

Por padrão, o seguinte caminho é especificado: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml. Se necessário, é possível alterar o nome padrão (retranslation_request) e o caminho.

> O arquivo de solicitação pode ser colocado em uma pasta local ou compartilhada. Quando estiver usando uma pasta compartilhada, é necessário confirmar se o dispositivo pode acessá-la com o servidor de administração instalado. As formas de garantir o acesso e as ferramentas usadas dependem da sua infraestrutura.

Ao executar a tarefa *Baixar atualizações para o repositório do Servidor de Administração*, o Kaspersky Security Center Linux cria o arquivo de solicitação de atualização no formato .xml no caminho especificado. O Utilitário de Atualização do Kaspersky obtém automaticamente as informações do arquivo de solicitação e baixa apenas as atualizações necessárias. Se o Utilitário de Atualização do Kaspersky não conseguir obter as informações automaticamente (por exemplo, não conseguir acessar a pasta onde o Kaspersky Security Center Linux criou o arquivo de solicitação), você terá que transmitir o arquivo através de ferramentas de terceiros.



Especificação das propriedades da tarefa Baixar atualizações para o repositório do Servidor de Administração

9. Na janela de propriedades da tarefa, na guia **Agendamento**, crie uma programação para o início da tarefa. Caso seja necessário, defina as seguintes configurações:

- **Iniciar tarefa**:

  Manualmente (selecionado por padrão)

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

  A cada N minutos

  A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

  Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  A cada N horas

  A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

  Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  A cada N dias

  A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

Por dias da semana

A tarefa é executada regularmente, nos dias da semana e no horário especificados.

Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

Mensalmente

A tarefa é executada regularmente, no dia do mês e na hora especificados.

Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

Mensalmente em um dia da semana selecionado

A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

Por padrão, a hora de início é 18:00 e nenhum dia do mês é selecionado.

> Observe que você não seleciona uma data específica no mês, nem o número da semana (primeira, segunda semana do mês), mas o número de sequência do dia da semana dentro de um mês. Por exemplo, se definir o cursor na célula **Ter** da **Primeiro(a)** linha, a tarefa será executada toda primeira terça-feira de cada novo mês.

É possível selecionar vários dias da semana.

Na conclusão de outra tarefa

A tarefa atual inicia após outra tarefa ser concluída. Esta opção só funciona se ambas as tarefas estiverem atribuídas aos mesmos dispositivos. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus* com um tarefa de acionamento.

É necessário selecionar a tarefa de acionamento na tabela e o status com o qual a tarefa deve ser concluída (**Conclusão com êxito** ou **Falhou**).

Caso seja necessário, é possível pesquisar, classificar e filtrar as tarefas na tabela da seguinte maneira:

- Insira o nome da tarefa no campo de pesquisa para pesquisar a tarefa pelo nome.
- Clique no ícone de classificação para classificar as tarefas por nome.

  Por padrão, as tarefas são classificadas em ordem alfabética crescente.
- Clique no ícone de filtragem e, na janela exibida, filtre as tarefas por grupo e clique no botão **Aplicar**.

- Configurações adicionais da tarefa:

  Executar tarefas ignoradas

  Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

  Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está ativada.

Usar atraso aleatório automaticamente para início da tarefa

Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

Por padrão, esta opção está ativada.

Usar atraso aleatório automaticamente para início de tarefa em um intervalo de

Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

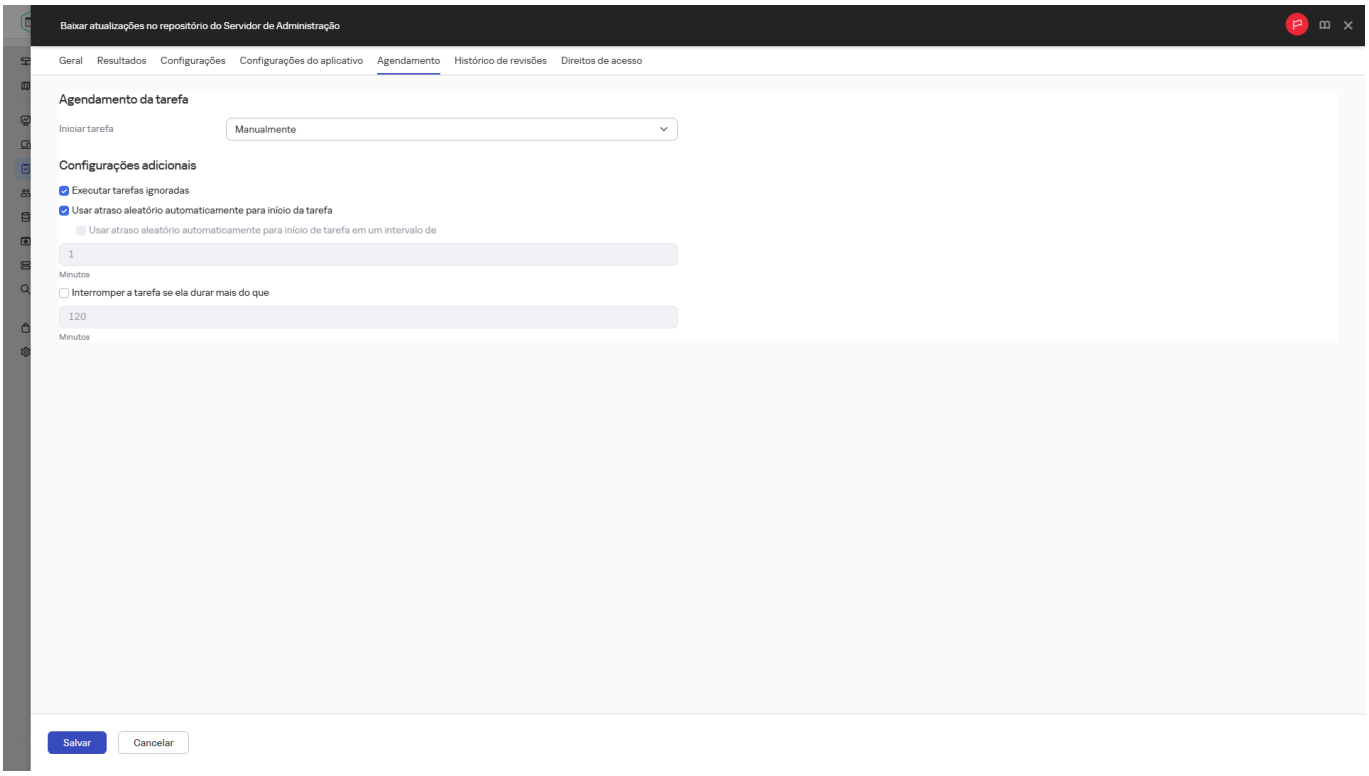
Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

Interromper a tarefa se ela durar mais do que

Após o final do período especificado, a tarefa é interrompida automaticamente, quer tenha sido concluída ou não.

Ative esta opção se você quiser interromper (ou parar) tarefas que levam muito tempo para serem executadas.

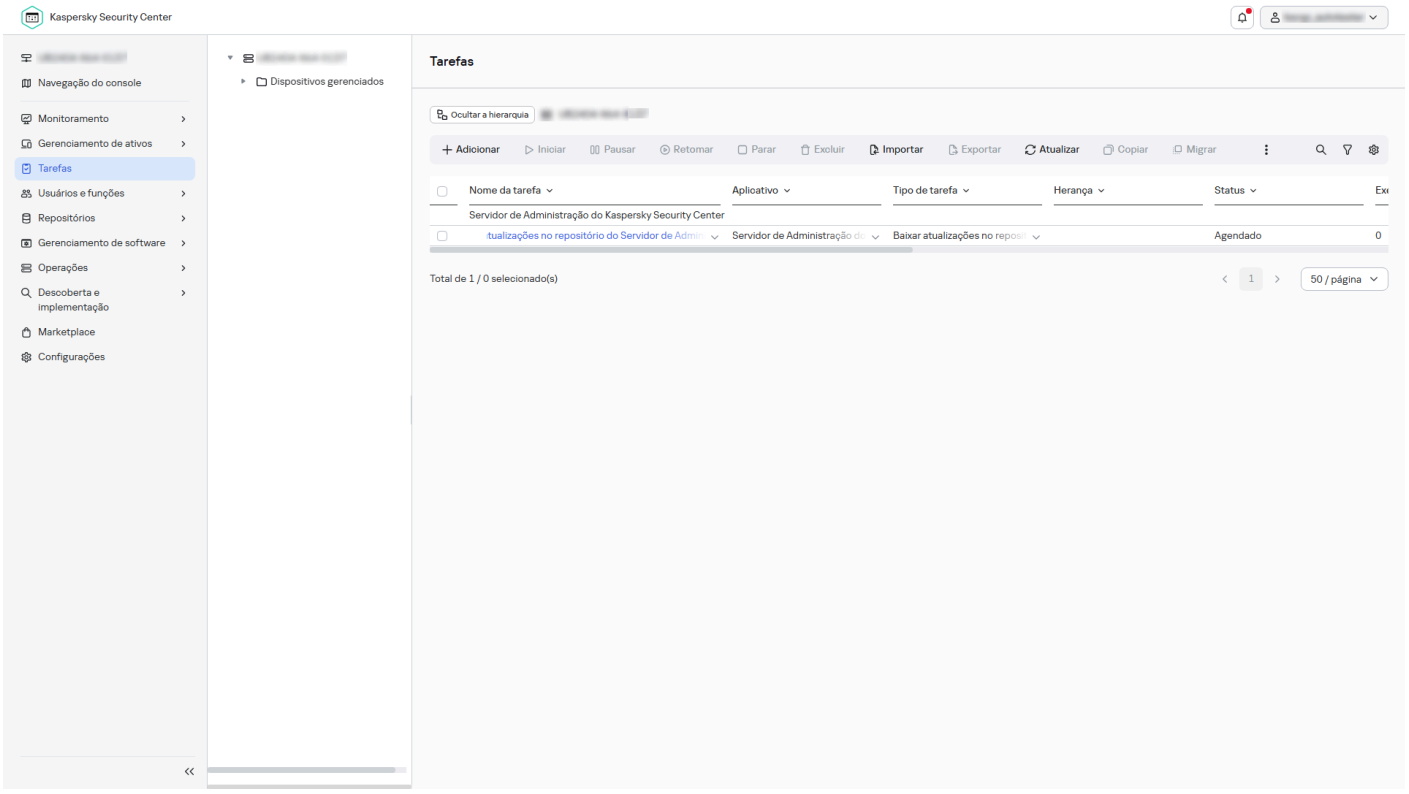
Por padrão, esta opção está desativada. O tempo predefinido de execução da tarefa é de 120 minutos.



Especificação da programação da tarefa Baixar atualizações para o repositório do Servidor de Administração

10. Clique no botão **Salvar**.

A tarefa é criada e configurada.



A lista de tarefas

Quando o Servidor de Administração executa a tarefa *Baixar atualizações no repositório do Servidor de Administração*, as atualizações de bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada do Servidor de Administração. Se você criar esta tarefa para um grupo de administração, ela somente será aplicada aos Agentes de Rede incluídos no grupo de administração especificado.

As atualizações são distribuídas aos dispositivos clientes e aos Servidores de Administração secundários da pasta compartilhada do Servidor de Administração.

Verificação das atualizações baixadas

Antes de instalar as atualizações nos dispositivos gerenciados, é possível verificar primeiro as atualizações sobre operabilidade e erros por meio da tarefa de *Verificação de atualizações*. A tarefa de *Verificação de atualizações* é executada automaticamente como parte da tarefa *Baixar atualizações no repositório do Servidor de Administração*. O Servidor de Administração baixa as atualizações da origem, salva-as no armazenamento temporário e executa a tarefa de *Verificação de atualizações*. Caso a tarefa seja concluída com êxito, as atualizações são copiadas do repositório temporário para a pasta compartilhada do Servidor de Administração. Elas são distribuídas à todos os dispositivos clientes para os quais o Servidor de Administração for a fonte de atualizações.

Caso os resultados da tarefa de *Verificação de atualizações* demonstrarem que as atualizações localizadas no repositório temporário estão incorretas ou se a tarefa de Verificação de atualizações concluir com erro, as atualizações não serão copiadas para a pasta compartilhada. O Servidor de Administração retém o conjunto anterior de atualizações. Além disso, as tarefas que têm o tipo de agendamento **Quando novas atualizações são baixadas no repositório** não são iniciadas. Essas operações são realizadas no próximo início da tarefa *Baixar atualizações no repositório do Servidor de Administração* se a verificação das novas atualizações for concluída com êxito.

Um conjunto de atualizações é considerado inválido se uma das seguintes condições for atendida em pelo menos um dispositivo de teste:

- Ocorreu um erro na tarefa de atualização.
- O status da proteção em tempo real do aplicativo de segurança foi modificado após a aplicação das atualizações.
- Um objeto infectado foi detectado durante a execução da tarefa de verificação sob demanda.
- Ocorreu um erro de tempo de execução de um aplicativo da Kaspersky.

Caso nenhuma das condições listadas sejam verdadeiras em nenhum dispositivo de teste, o conjunto de atualizações é considerado como válido, e a tarefa de *Verificação de atualizações* será considerada com êxito na conclusão.

Antes de começar a criar a tarefa de *Verificação de atualizações*, execute os pré-requisitos:

1. Criar um grupo de administração com vários dispositivos de teste. Esse grupo será necessário para verificar as atualizações.

   Recomenda-se usar os dispositivos com a proteção mais confiável e com a configuração de aplicativo mais popular na rede. Essa abordagem aumenta a qualidade e a probabilidade de detecção de vírus durante as verificações e minimiza o risco de falsos positivos. Caso sejam detectados vírus nos dispositivos de teste, a tarefa de *Verificação de atualizações* será considerada malsucedida.

2. Criar as tarefas de atualização e verificação de malware para um aplicativo compatível com o Kaspersky Security Center Linux, por exemplo, o Kaspersky Endpoint Security for Linux. Ao criar as tarefas de atualização e verificação de malwares, especifique o grupo de administração com os dispositivos de teste.

   A tarefa de *verificação de atualizações* executa sequencialmente as tarefas de atualização e verificação de malwares em dispositivos de teste para verificar se todas as atualizações são válidas. Além disso, ao criar a tarefa de *Verificação de atualizações*, será necessário especificar as tarefas de atualização e verificação de malwares.

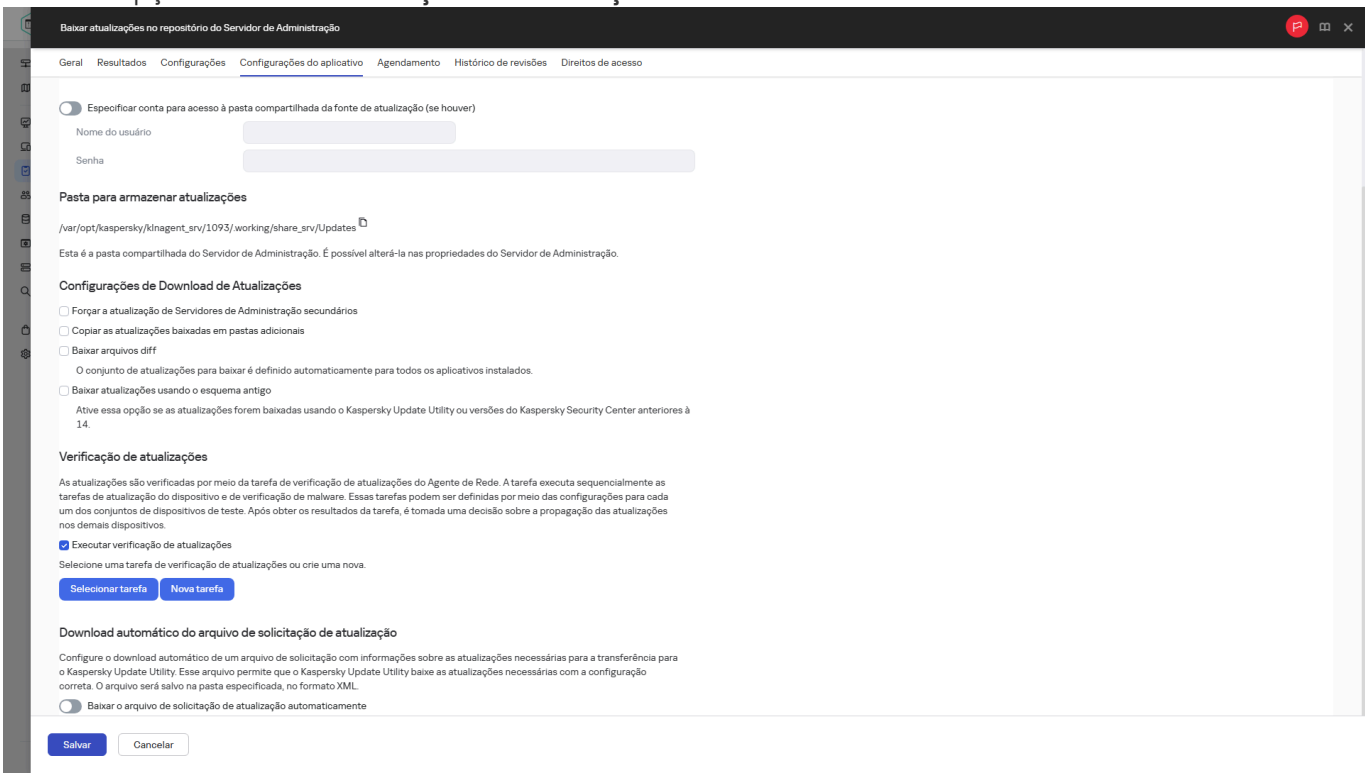
3. Crie a tarefa *Baixar atualizações no repositório do Servidor de Administração*.

Para que o Kaspersky Security Center Linux verifique as atualizações baixadas antes de distribuí-las para os dispositivos clientes:

1. No menu principal, vá para **Tarefas**.

2. Clique na tarefa **Baixar atualizações no repositório do Servidor de Administração**.

3. Na janela de propriedades do aplicativo que se abre, acesse a guia **Configurações do aplicativo** e, então, habilite a opção **Executar verificação de atualizações**.



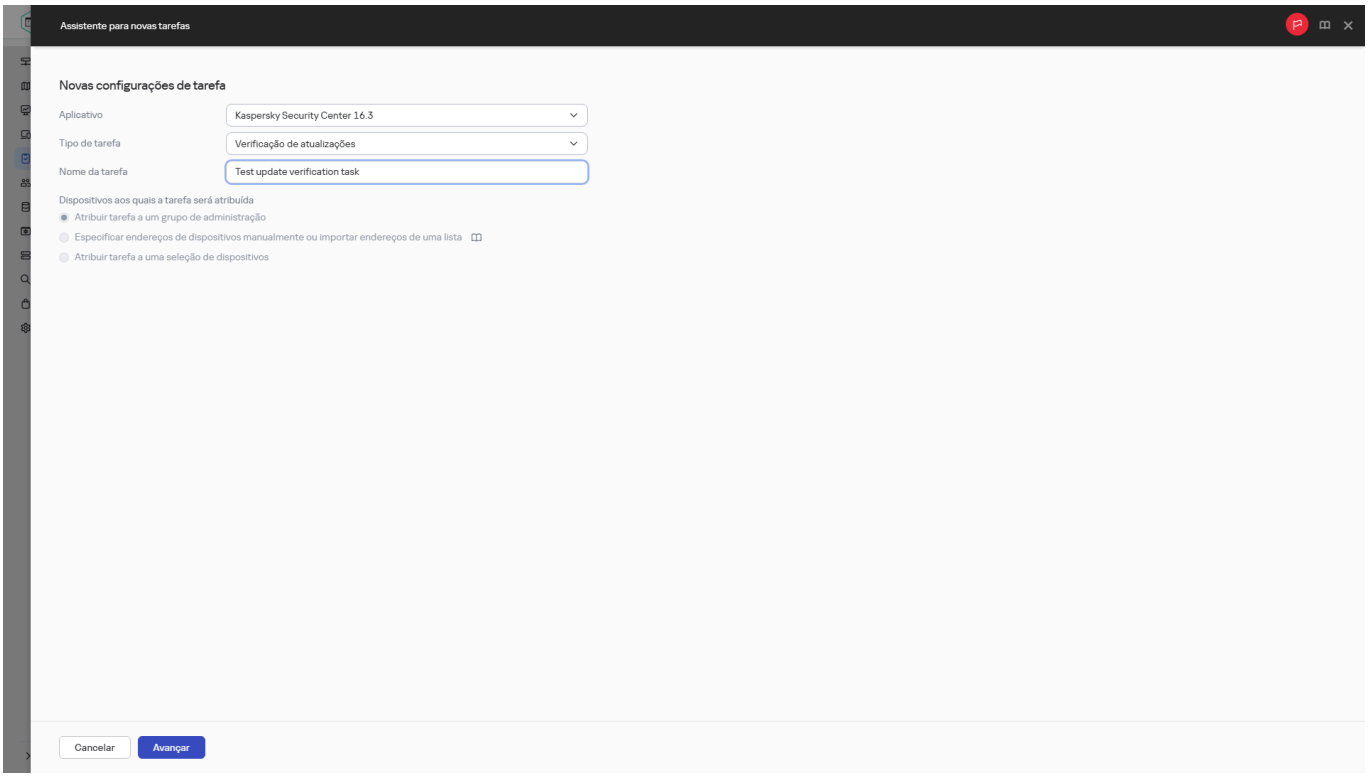
Propriedades da tarefa Baixar atualizações no repositório do Servidor de Administração

4. Caso a tarefa *Verificação de atualizações* exista, clique no botão **Selecionar tarefa**. Na janela aberta, selecione a tarefa de *Verificação de atualizações* no grupo de administração com dispositivos de teste.

5. Caso não tenha criado a tarefa de *Verificação de atualizações* anteriormente, faça o seguinte:

   a. Clique no botão **Nova tarefa**.

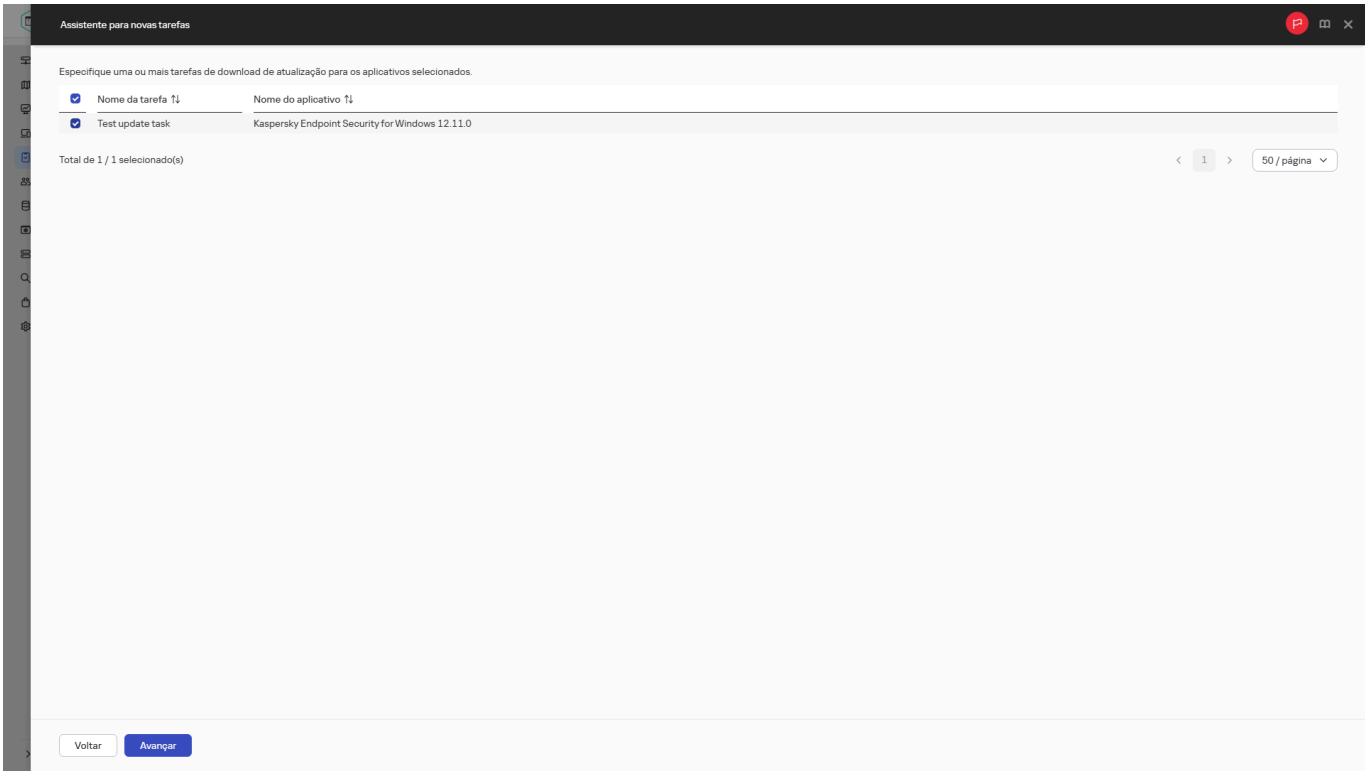
   b. No Assistente para novas tarefas aberto, especifique o nome da tarefa caso queira alterar o nome da predefinição.



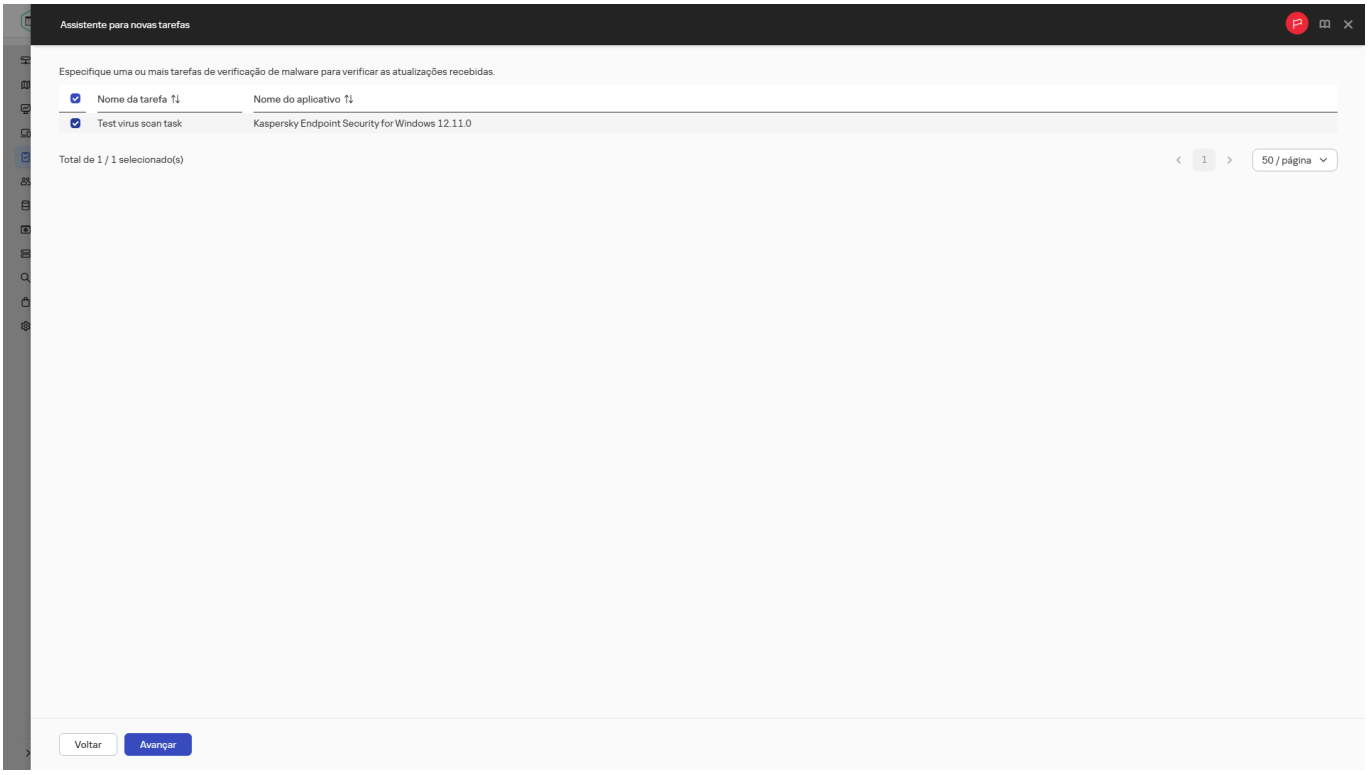
Criação de uma tarefa Verificação de atualização

   a. Selecione o grupo de administração com os dispositivos de teste criado anteriormente.

   b. Selecione a tarefa de atualização de um aplicativo necessário compatível com o Kaspersky Security Center Linux.



a. Selecione a tarefa de verificação de malware de um aplicativo necessário compatível com o Kaspersky Security Center Linux.



Seleção da tarefa de verificação de malware

Depois disso, as seguintes opções aparecem. Recomendamos deixá-las ativadas:

Reiniciar o dispositivo após a atualização do banco de dados

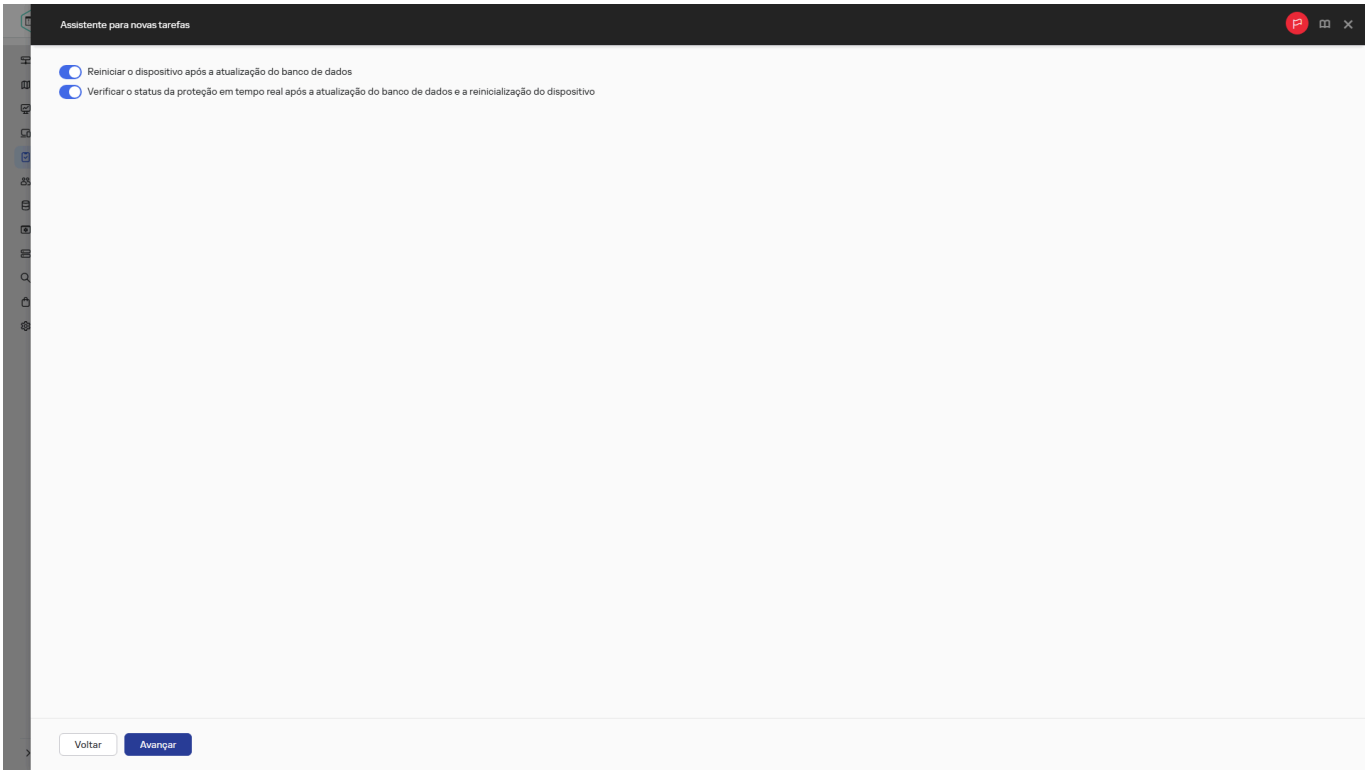
Depois que os bancos de dados antivírus forem atualizados em um dispositivo, recomendamos reinicializar o dispositivo.

Por padrão, esta opção está ativada.

Verificar o status da proteção em tempo real após a atualização do banco de dados e a reinicialização do dispositivo

Caso esta opção esteja habilitada, a tarefa de *Verificação de atualizações* verifica se as atualizações baixadas para o repositório do Servidor de Administração são válidas e se o nível de proteção diminuiu após a atualização do banco de dados antivírus e a reinicialização do dispositivo.

Por padrão, esta opção está ativada.



Especificação das configurações da tarefa

a. Especifique uma conta a partir da qual a tarefa de *Verificação de atualizações* será executada. É possível usar a conta e manter a opção **Conta padrão** ativada. Como alternativa, é possível especificar que a tarefa seja executada em outra conta com os direitos de acesso necessários. Para isso, selecione a opção **Especificar conta** e, em seguida, insira as credenciais dessa conta.

6. Clique em **Salvar** para fechar a janela de propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*.

A verificação de atualizações automática é ativada. Agora, é possível executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, e ela começará a partir da verificação de atualização.

Criar a tarefa para baixar as atualizações aos repositórios de pontos de distribuição

É possível criar a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* para um grupo de administração. Esta tarefa será executada para pontos de distribuição incluídos no grupo de administração especificado.

Você pode usar esta tarefa, por exemplo, se o tráfego entre o Servidor de Administração e pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.

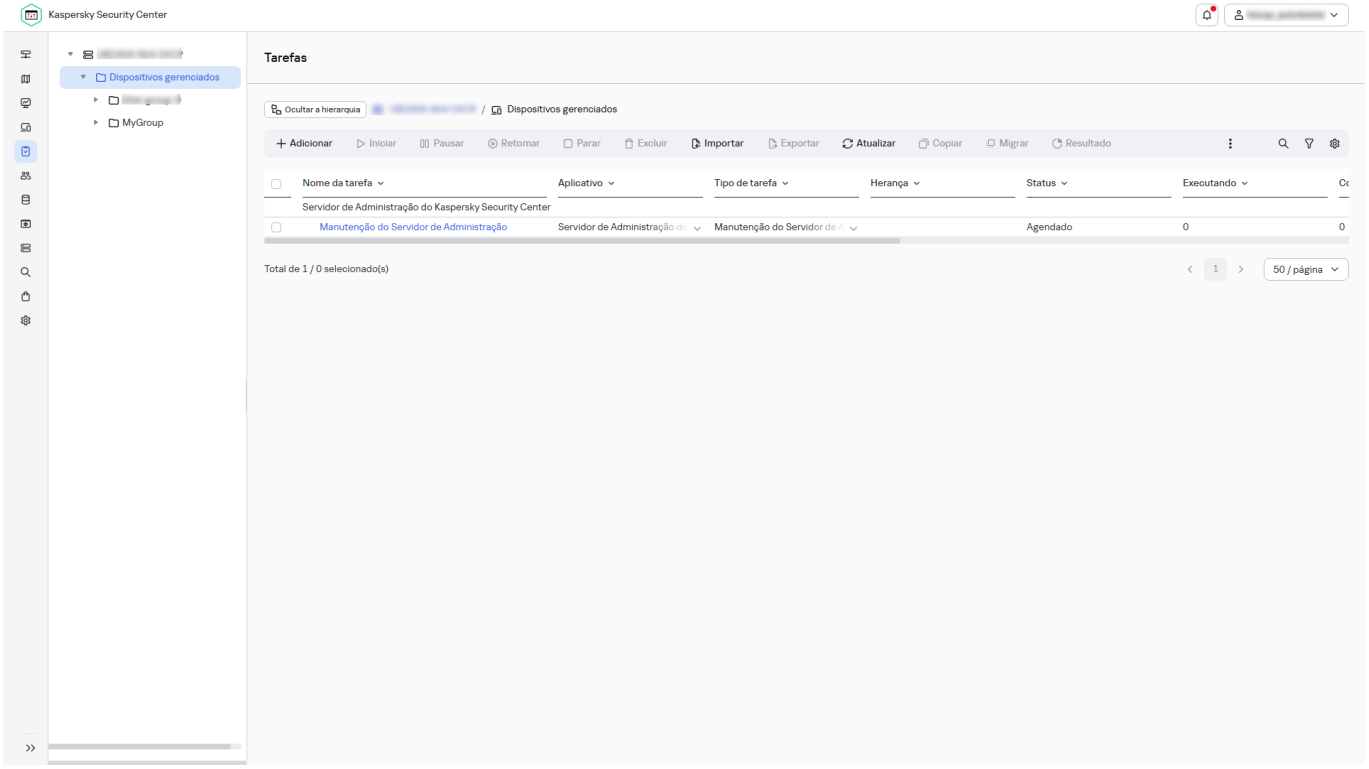
Esta tarefa é necessária para baixar atualizações de servidores de atualização da Kaspersky para os repositórios de pontos de distribuição. A lista de atualizações inclui:

- Atualizações para bancos de dados e módulos do software de aplicativos de segurança Kaspersky
- Atualizações para componentes do Kaspersky Security Center
- Atualizações para aplicativos de segurança Kaspersky

Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

*Para criar a tarefa **Baixar atualizações para os repositórios de pontos de distribuição**, para um grupo de administração selecionado:*

1. No menu principal, vá para **Tarefas**.



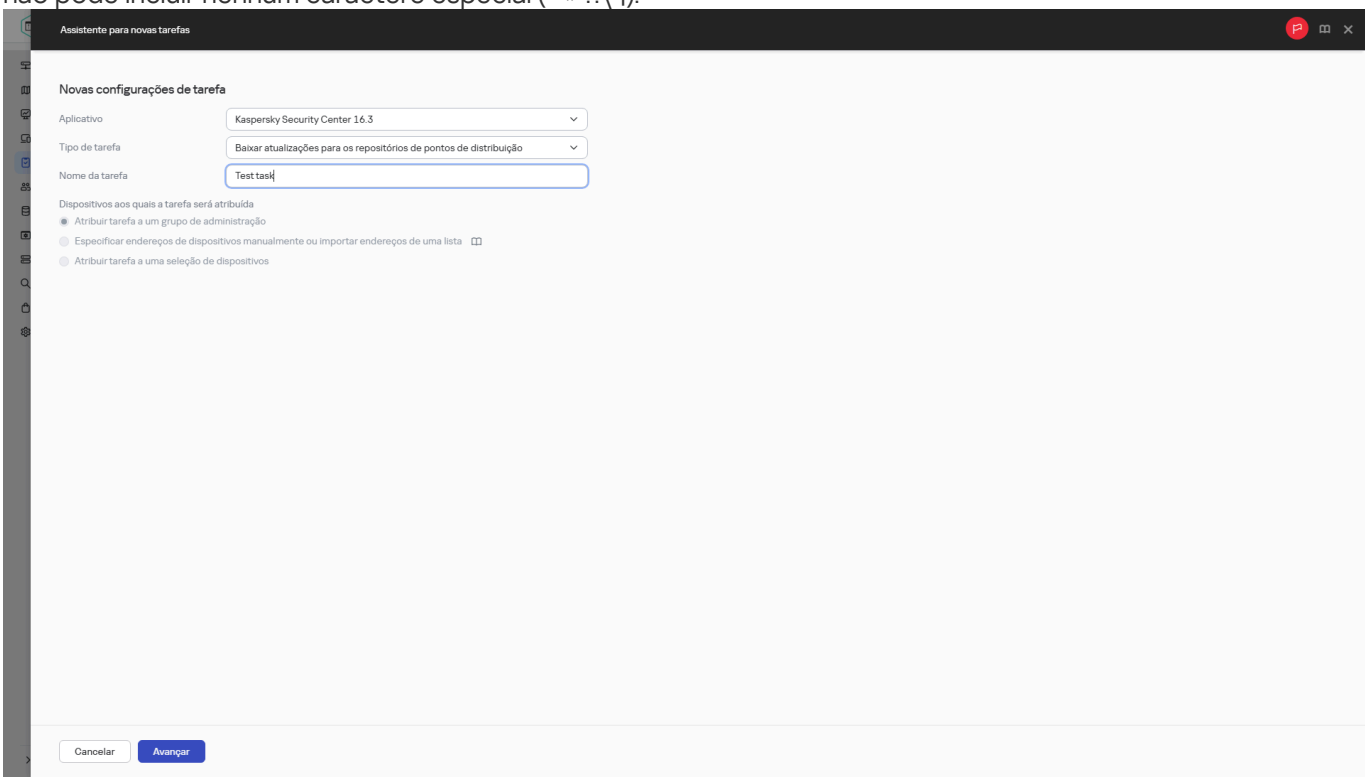
A seção Tarefas

2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

3. Para o aplicativo Kaspersky Security Center, no campo **Tipo de tarefa**, selecione **Baixar atualizações para os repositórios de pontos de distribuição**.

4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).



Criação da tarefa Baixar atualizações para os repositórios de pontos de distribuição

5. Selecione um botão de opção para especificar o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.

6. Na etapa **Concluir a criação da tarefa**, caso queira modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode alterar as configurações padrão depois, a qualquer momento.

7. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.

8. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

9. Na guia **Configurações do aplicativo** da janela de propriedades da tarefa, especifique as seguintes configurações:

   Fontes de atualizações

   Os seguintes recursos podem ser utilizados como uma origem das atualizações para o ponto de distribuição:

   - Servidores de atualização da Kaspersky

     Servidores HTTP na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

     Esta opção está marcada por padrão.

   - Pasta local ou de rede

     Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Somente um compartilhamento SMB montado pode ser usado como uma pasta de rede. Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado.

Na tarefa *Baixar atualizações no repositório do Servidor de Administração* e na tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a autenticação do usuário não funcionará se for selecionada uma pasta local ou de rede protegida por senha como fonte de atualização. Para resolver esse problema, primeiro monte a pasta protegida por senha e, em seguida, especifique as credenciais necessárias, por exemplo, por meio do sistema operacional. Depois disso, será possível selecionar essa pasta como fonte de atualização em uma tarefa de download de atualizações. O Kaspersky Security Center Linux não solicitará a inserção das credenciais.

Pasta para armazenar atualizações

O caminho para a pasta especificada para armazenar atualizações salvas. É possível copiar o caminho da pasta especificada para uma área de transferência. Não é possível alterar o caminho para uma pasta especificada para uma tarefa de grupo.

Baixar arquivos diff

Esta opção ativa o recurso de download dos arquivos diff.

Por padrão, esta opção está desativada.

Baixar atualizações usando o esquema antigo

A partir da versão 14, o Kaspersky Security Center baixa as atualizações de bancos de dados e os módulos de software usando o novo esquema. Para que o aplicativo baixe atualizações usando o novo esquema, a fonte de atualização deve conter os arquivos de atualização com os metadados compatíveis com o novo esquema. Caso a fonte de atualização contenha os arquivos de atualização com os metadados compatíveis apenas com o esquema antigo, ative a opção **Baixar atualizações usando o esquema antigo**. Caso contrário, a tarefa de download de atualizações falhará.

Por exemplo, é preciso habilitar essa opção quando uma pasta local ou de rede for especificada como fonte de atualização, e os arquivos de atualização nesta pasta tiverem sido baixados por um dos seguintes aplicativos:

- Utilitário de atualização da Kaspersky

  Esse utilitário baixa as atualizações usando o esquema antigo.

- Kaspersky Security Center 13 Linux

  Por exemplo, um ponto de distribuição está configurado para receber as atualizações de uma pasta local ou de rede. Nesse caso, é possível baixar as atualizações usando um Servidor de Administração que tenha uma conexão com a Internet e, em seguida, colocar as atualizações na pasta local no ponto de distribuição. Caso o Servidor de Administração tenha a versão 13, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa *Baixe atualizações para os repositórios de pontos de distribuição*.

Por padrão, esta opção está desativada.

10. Crie um agendamento para o início da tarefa. Caso seja necessário, defina as seguintes configurações:

- **Iniciar tarefa**:

  Manualmente (selecionado por padrão)

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

  A cada N minutos

  A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

  Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

A cada N horas

A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

A cada N dias

A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

Por dias da semana

A tarefa é executada regularmente, nos dias da semana e no horário especificados.

Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

Mensalmente

A tarefa é executada regularmente, no dia do mês e na hora especificados.

Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

Mensalmente em um dia da semana selecionado

A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

Por padrão, a hora de início é 18:00 e nenhum dia do mês é selecionado.

> Observe que você não seleciona uma data específica no mês, nem o número da semana (primeira, segunda semana do mês), mas o número de sequência do dia da semana dentro de um mês. Por exemplo, se definir o cursor na célula **Ter** da **Primeiro(a)** linha, a tarefa será executada toda primeira terça-feira de cada novo mês.

É possível selecionar vários dias da semana.

No surto de vírus

A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

- Antivírus para estações de trabalho e servidores de arquivo
- Antivírus para defesa de perímetro
- Antivírus para sistemas de correio

Por padrão, todos os tipos de aplicativos estão selecionados.

Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

Na conclusão de outra tarefa

A tarefa atual inicia após outra tarefa ser concluída. Esta opção só funciona se ambas as tarefas estiverem atribuídas aos mesmos dispositivos. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus* com um tarefa de acionamento.

É necessário selecionar a tarefa de acionamento na tabela e o status com o qual a tarefa deve ser concluída (**Conclusão com êxito** ou **Falhou**).

Caso seja necessário, é possível pesquisar, classificar e filtrar as tarefas na tabela da seguinte maneira:

- Insira o nome da tarefa no campo de pesquisa para pesquisar a tarefa pelo nome.
- Clique no ícone de classificação para classificar as tarefas por nome.

  Por padrão, as tarefas são classificadas em ordem alfabética crescente.
- Clique no ícone de filtragem e, na janela exibida, filtre as tarefas por grupo e clique no botão **Aplicar**.

- **Executar tarefas ignoradas**

  Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

  Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

  Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

  Por padrão, esta opção está ativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

  Por padrão, esta opção está ativada.

- **Usar atraso aleatório automaticamente para início de tarefa em um intervalo de**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

11. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Quando a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for executada, as atualizações para bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada. As atualizações baixadas somente serão usadas por pontos de distribuição que estão incluídos no grupo de administração especificado e que não têm nenhuma tarefa de download de atualização explicitamente definida para eles.

Adicionando fontes de atualizações para a tarefa Baixar atualizações no repositório do Servidor de Administração

Ao criar ou usar a tarefa para baixar atualizações para o repositório do Servidor de Administração, é possível escolher as seguintes fontes de atualizações:

- Servidores de atualização da Kaspersky
- Servidor de Administração principal

  Este recurso é aplicado a tarefas criadas para um Servidor de Administração virtual ou secundário.
- Pasta local ou de rede

  Na tarefa *Baixar atualizações no repositório do Servidor de Administração* e na tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a autenticação do usuário não funcionará se for selecionada uma pasta local ou de rede protegida por senha como fonte de atualização. Para resolver esse problema, primeiro monte a pasta protegida por senha e, em seguida, especifique as credenciais necessárias, por exemplo, por meio do sistema operacional. Depois disso, será possível selecionar essa pasta como fonte de atualização em uma tarefa de download de atualizações. O Kaspersky Security Center Linux não solicitará a inserção das credenciais.

Por padrão, são usados os servidores de atualização da Kaspersky, mas também é possível baixar atualizações de uma pasta local ou de rede. Você pode querer usar a pasta se sua rede não tiver acesso à Internet. Nesse caso, é possível baixar manualmente as atualizações dos servidores de atualização da Kaspersky e colocar os arquivos baixados na pasta necessária. É possível especificar apenas um caminho para uma pasta local ou de rede.

Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado. O caminho para a pasta depende do sistema operacional do dispositivo. Como a pasta local está localizada no Servidor de Administração baseado em Linux, você precisa especificar o caminho POSIX, por exemplo: /caminho/para/diretório.

Somente um compartilhamento SMB montado pode ser usado como uma pasta de rede. Caso um compartilhamento SMB precise de autenticação, ele deverá ser montado no sistema com as credenciais necessárias com antecedência. Recomendamos não usar o protocolo SMB1, pois não é seguro.

Para adicionar as fontes de atualização:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Baixar atualizações no repositório do Servidor de Administração**.

3. Vá para a guia **Configurações do aplicativo**.
4. Na tabela **Fontes de atualizações**, clique no botão **Adicionar**.
5. Na janela exibida, adicione as fontes necessárias e clique no botão **Salvar**.

   Ao selecionar a caixa de seleção **Pasta local ou de rede**, especifique um caminho para a pasta.
6. Clique no botão **Salvar** na janela da tarefa.

Agora as atualizações são baixadas das fontes especificadas para o repositório do Servidor de Administração.

Se você adicionar os servidores de atualização da Kaspersky e a pasta local ou de rede, poderá definir prioridades para as atualizações. Para fazer isso, na tabela **Fontes de atualizações**, marque a caixa de seleção ao lado da atualização para a qual você deseja alterar a prioridade e clique no botão **Para cima** ou **Para baixo**.

Aprovar e recusar atualizações de software

As configurações de uma tarefa de instalação de atualização podem necessitar da aprovação de atualizações que devem ser instaladas. Você pode aprovar atualizações que devem ser instaladas e recusar as atualizações que não devem ser instaladas.

Por exemplo, pode ser necessário verificar primeiro a instalação das atualizações em um ambiente de teste, assegurar-se de que elas não interferem na operação dos dispositivos e, só então, permitir a instalação dessas atualizações nos dispositivos cliente.

A aprovação e recusa de atualizações estão disponíveis apenas para o Agente de Rede e aplicativos gerenciados instalados em dispositivos clientes baseados em Windows. A atualização contínua do Servidor de Administração, do Kaspersky Security Center Web Console e dos plug-ins da web de gerenciamento não é compatível. Para atualizar esses componentes, você deve baixar as versões mais recentes do site da Kaspersky e, em seguida, instalá-las manualmente.

Para aprovar ou recusar uma ou várias atualizações:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos da Kaspersky → Atualizações contínuas**.

   Aparece uma lista das atualizações disponíveis.

   As atualizações de aplicativos gerenciados podem exigir a instalação de uma versão mínima específica do Kaspersky Security Center. Se esta versão for posterior à versão atual, essas atualizações serão exibidas, mas não poderão ser aprovadas. Além disso, nenhum pacote de instalação pode ser criado a partir dessas atualizações até que você atualize o Kaspersky Security Center. Você receberá uma solicitação para atualizar sua instância do Kaspersky Security Center para a versão mínima necessária.
2. Se necessário, aceite o EULA clicando no botão **Exibir e aceitar os Contratos de Licença**.
3. Selecione as atualizações que deseja aprovar ou recusar.

4. Clique em **Aprovar** para aprovar as atualizações selecionadas ou **Recusar** para recusar as atualizações selecionadas.

   O valor padrão é *Indefinido*.

As atualizações às quais você atribui o status *Aprovado* são colocadas em uma fila para instalação.

As atualizações às quais você atribui o status *Negado* são desinstaladas (se possível) de todos os dispositivos nos quais elas foram anteriormente instaladas. Além disso, elas não serão instaladas em outros dispositivos no futuro.

Algumas atualizações para aplicativos da Kaspersky não podem ser desinstaladas. Se você definir o status *Recusado* para elas, o Kaspersky Security Center Linux não desinstalará essas atualizações dos dispositivos nos quais foram instaladas anteriormente. No entanto, essas atualizações nunca serão instaladas em outros dispositivos no futuro.

Se você definir o status *Negado* para atualizações de software de terceiros, estas atualizações não serão instaladas em dispositivos para os quais elas foram planejadas, mas que ainda não foram instaladas. As atualizações permanecerão nos dispositivos nos quais elas já foram instaladas. Se você tiver as atualizações, poderá exclui-las de forma manual localmente.

Instalação automática de atualizações para o Kaspersky Endpoint Security for Windows

Você pode configurar as atualizações automáticas dos bancos de dados e módulos de software do Kaspersky Endpoint Security for Windows nos dispositivos clientes.

Para configurar o download e a instalação automática das atualizações do Kaspersky Endpoint Security for Windows nos dispositivos:

1. No menu principal, vá para **Tarefas**.

2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

3. Para o aplicativo da Kaspersky Endpoint Security for Windows, selecione **Atualização** como o subtipo de tarefa.

4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

5. Selecione o escopo da tarefa.

6. Especifique o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.

7. Na etapa **Concluir a criação da tarefa**, caso queira modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode alterar as configurações padrão depois, a qualquer momento.

8. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.

9. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

10. Na guia **Configurações do aplicativo** da janela de propriedades de tarefa, defina as configurações da tarefa de atualização no modo local ou de dispositivos móveis:

    - **Modo local**: a conexão é estabelecida entre o dispositivo e o Servidor de Administração.
    - **Modo móvel**: nenhuma conexão é estabelecida entre o Kaspersky Security Center Linux e o dispositivo (por exemplo, quando o dispositivo não está conectado à Internet).

11. Ative as fontes de atualização que deseja usar para atualizar bancos de dados e módulos de aplicativo do Kaspersky Endpoint Security for Windows. Se necessário, altere as posições das fontes na lista usando os botões **Para cima** e **Para baixo**. Se várias fontes de atualizações forem ativadas, o Kaspersky Endpoint Security for Windows tentará se conectar a elas uma após a outra, começando pelo topo da lista, e executará a tarefa de atualização recuperando o pacote de atualização da primeira fonte disponível.

12. Ative a opção **Instalar apenas atualizações aprovadas** para baixar e instalar atualizações dos módulos de software junto com bancos de dados do aplicativo.

    Se a opção estiver ativada, o Kaspersky Endpoint Security for Windows notifica o usuário sobre as atualizações dos módulos de software disponíveis e inclui atualizações nos módulos de software no pacote de atualização ao executar a tarefa de atualização. O Kaspersky Endpoint Security for Windows instala somente as atualizações para as quais você definiu o status *Aprovado*; elas serão instaladas localmente por meio da interface do aplicativo ou do Kaspersky Security Center Linux.

    Você também pode ativar a opção **Instalar atualizações críticas do módulo de aplicativo automaticamente**. Se quaisquer atualizações do módulo de software estiverem disponíveis, o Kaspersky Endpoint Security for Windows as instala com o status *Crítico*; as atualizações remanescentes serão instaladas após a sua aprovação.

    Se a atualização do módulo de software requerer a revisão e aceitação dos termos do Contrato de Licença e da Política de Privacidade, o aplicativo instala as atualizações após os termos do Contrato de Licença e da Política de Privacidade terem sido aceitos pelo usuário.

13. Marque a caixa de seleção **Copiar atualizações para uma pasta** para que o aplicativo salve as atualizações baixadas em uma pasta e especifique o caminho da pasta.

14. Agende a tarefa. Para assegurar atualizações oportunas, recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório**.

15. Clique no botão **Salvar**.

Ao executar a tarefa de **Atualização**, o aplicativo envia solicitações aos servidores de atualização Kaspersky.

Algumas atualizações necessitam da instalação das versões mais recentes dos plug-ins de gerenciamento.

Sobre usar os arquivos diff para atualizar bancos de dados e módulos do software Kaspersky

Quando o Kaspersky Security Center Linux baixa atualizações de servidores de Atualização a partir da Kaspersky, ele otimiza o tráfego usando arquivos diff. Você também pode ativar o uso de arquivos diff pelos dispositivos (Servidores de Administração, pontos de distribuição e dispositivos clientes) que recebem atualizações de outros dispositivos na rede.

Sobre o recurso Baixar arquivos diff

Um arquivo diff descreve as diferenças entre duas versões de um arquivo de banco de dados ou módulo de software. O uso de arquivos diff poupa tráfego na rede da empresa porque os arquivos diff ocupam menos espaço do que arquivos completos de bancos de dados e módulos de software. Se o recurso *Baixar arquivos diff* estiver ativado no Servidor de Administração ou em um ponto de distribuição, os arquivos diff serão salvos no Servidor de Administração ou ponto de distribuição. Como resultado, os dispositivos que recebem atualizações desse Servidor de Administração ou ponto de distribuição podem usar os arquivos diff salvos para atualizar bancos de dados e módulos de software.

Para otimizar o uso de arquivos diff, recomendamos que você sincronize os agendamentos das atualizações dos dispositivos com os do Servidor de Administração ou do ponto de distribuição a partir do qual os dispositivos são atualizados. Entretanto, pode ocorrer economia de tráfego mesmo se os dispositivos forem atualizados com muito menos frequência do que o Servidor de Administração ou o ponto de distribuição a partir do qual os dispositivos são atualizados.

Os pontos de distribuição não usam multicasting de IP para distribuição automática de arquivos diff.

Ativação do recurso Baixar arquivos diff

Fases

1. **Como ativar o recurso no Servidor de Administração**

   Ative o recurso nas configuração de uma tarefa *Baixar atualizações para o repositório do Servidor de Administração*.

2. **Como ativar o recurso para um ponto de distribuição**

   Ative o recurso em um ponto de distribuição que recebe atualizações por meio de uma tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.

   Em seguida, ative o recurso nas configurações de política do Agente de Rede para um ponto de distribuição que recebe atualizações do Servidor de Administração.

   Em seguida, ative o recurso em um ponto de distribuição que recebe atualizações do Servidor de Administração.

O recurso é ativado nas configurações de política do Agente de Rede e – se os pontos de distribuição forem atribuídos manualmente e você quiser ignorar as configurações da política – na seção **Pontos de distribuição** das propriedades do Servidor de Administração.

Para verificar se o recurso Baixar arquivos diff está ativado com êxito, você pode medir o tráfego interno antes e depois de executar o cenário.

Baixar atualizações por pontos de distribuição

O Kaspersky Security Center Linux permite que os pontos de distribuição recebem atualizações do Servidor de Administração, dos servidores da Kaspersky ou de uma pasta local ou de rede.

Para configurar o download da atualização para um ponto de distribuição:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Clique no nome do ponto de distribuição por meio do qual as atualizações serão entregues aos dispositivos clientes no grupo.

4. Na janela de propriedades do ponto de distribuição, selecione a seção **Fonte de atualizações**.

5. Selecione uma origem de atualização para o ponto de distribuição:

   Fonte de atualizações

   Selecione uma origem de atualização para o ponto de distribuição:

   - Para permitir que o ponto de distribuição receba atualizações do Servidor de Administração, selecione **Obter do Servidor de Administração**.

   - Para permitir que o ponto de distribuição receba atualizações usando uma tarefa, selecione **Usar tarefa de download de atualizações** e, em seguida, especifique a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*:

     - Se essa tarefa já existir no dispositivo, selecione a tarefa na lista.

     - Se ainda não existir tal tarefa no dispositivo, clique no link **Criar tarefa** para criar uma tarefa. O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

   Baixar arquivos diff

   Esta opção ativa o recurso de download dos arquivos diff.

   Por padrão, esta opção está ativada.

O ponto de distribuição receberá as atualizações da origem especificada.

Atualização de bancos de dados e módulos de software da Kaspersky em dispositivos offline

A atualização dos bancos de dados e dos módulos de software da Kaspersky em dispositivos gerenciados é uma tarefa importante para manter a proteção dos dispositivos contra vírus e outras ameaças. Os administradores normalmente configuram atualizações regulares por meio do uso do repositório do Servidor de Administração.

Quando for preciso atualizar bancos de dados e módulos do software em um dispositivo (ou um grupo de dispositivos) que não está conectado ao Servidor de Administração (principal ou secundário), a um ponto de distribuição ou à Internet, você terá de usar fontes alternativas de atualizações, como um servidor FTP ou uma pasta local. Nesse caso, você precisa entregar os arquivos das atualizações necessárias usando um dispositivo de armazenamento em massa, como um pen drive ou um disco rígido externo.

Você pode copiar as atualizações necessárias de:

- O Servidor de Administração.

  Para ter certeza de que o repositório do Servidor de Administração contém as atualizações necessárias para o aplicativo de segurança instalado em um dispositivo offline, pelo menos um dos dispositivos online gerenciados deve ter o mesmo aplicativo de segurança instalado. Esse aplicativo deve ser configurado para receber as atualizações do repositório do Servidor de administração através da tarefa *Baixar atualizações no repositório do Servidor de Administração*.

- Qualquer dispositivo que tem o mesmo aplicativo de segurança instalado e configurado para receber as atualizações do repositório do Servidor de Administração, um repositório de ponto de distribuição ou diretamente dos servidores de atualização Kaspersky.

Abaixo há um exemplo de configuração de atualizações de bancos de dados e módulos de software copiando-os do repositório do Servidor de Administração.

Para atualizar os bancos de dados e módulos de software da Kaspersky em dispositivos offline:

1. Conecte a unidade removível ao dispositivo onde o Servidor de Administração está instalado.

2. Copie os arquivos de atualizações para a unidade removível.

   Por padrão, as atualizações estarão em: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   Como alternativa, é possível configurar o Kaspersky Security Center Linux para copiar regularmente as atualizações para a pasta selecionada. Para isso, use a opção **Copiar as atualizações baixadas em pastas adicionais** nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Se você especificar uma pasta localizada em um pendrive ou um disco rígido externo como uma pasta de destino dessa opção, esse dispositivo de armazenamento em massa sempre conterá a versão mais recente das atualizações.

3. Em dispositivos off-line, configure o aplicativo Kaspersky Endpoint Security para receber as atualizações de uma pasta local ou um recurso compartilhado, como um Servidor FTP ou uma pasta compartilhada.

   Instruções de como proceder:

   - Ajuda do Kaspersky Endpoint Security for Linux
   - Ajuda do Kaspersky Endpoint Security for Windows

4. Copie os arquivos de atualizações da unidade removível para a pasta local ou o recurso compartilhado que deseja usar como uma fonte de atualização.

5. No dispositivo off-line que requer a instalação da atualização, inicie a tarefa *Atualização* do Kaspersky Endpoint Security for Linux ou Kaspersky Endpoint Security for Windows, dependendo do sistema operacional do dispositivo off-line.

Depois que a tarefa de atualização for concluída, os bancos de dados e os módulos de software da Kaspersky serão atualizados no dispositivo.

Monitoramento, relatórios e auditoria

Esta seção descreve os recursos de monitoramento e emissão de relatórios no Kaspersky Security Center Linux. Esses recursos fornecem a você uma visão geral da infraestrutura, dos status de proteção e das estatísticas.

Após a implementação do Kaspersky Security Center Linux ou durante a operação, você pode configurar os recursos de monitoramento e emissão de relatórios de forma a melhor atender às suas necessidades.

Cenário: Monitoramento e relatórios

Esta seção fornece um cenário para a configuração do recurso de monitoramento e de relatórios no Kaspersky Security Center Linux.

Pré-requisitos

Após ter implementado o Kaspersky Security Center Linux na rede de uma organização, você poderá iniciar o monitoramento e gerar relatórios sobre o funcionamento.

O monitoramento e relatórios em na rede de uma organização prossegue em estágios:

1. **Configurar a alternância dos status do dispositivo**

   Conheça as configurações para os status do dispositivo dependendo de condições específicas. Modificando essas configurações, você pode alterar o número de eventos com os níveis de importância *Crítico* ou *Advertência*. Ao configurar a alternância dos status do dispositivo, esteja seguro do seguinte:

   - As novas configurações não entram em conflito com as políticas de segurança de informações da sua organização.
   - Você pode reagir a eventos de segurança importantes na rede da sua organização de maneira oportuna.

2. **Configurar as notificações de eventos em dispositivos clientes**

   Instruções de como proceder:

   Configure a notificação (por e-mail, SMS ou executando um arquivo executável) de eventos em dispositivos clientes

3. **Execução das ações recomendadas para as notificações Crítico e Advertência**

   Instruções de como proceder:

   Execute as ações recomendadas para a rede da sua organização

4. **Análise do status de segurança da rede da sua organização**

Instruções de como proceder:

- Revise o widget Status da proteção
- Gere e revise o Relatório do status da proteção
- Gere e revise o Relatório de erros

5. **Localize dispositivos clientes que não estão protegidos**

   Instruções de como proceder:

   - Revise o widget Novos dispositivos
   - Gere e revise o Relatório de implementação de proteção

6. **Verificação da proteção de dispositivos clientes**

   Instruções de como proceder:

   - Gere e revise os relatórios das categorias Status da proteção e Estatísticas de ameaças
   - Inicie e analise a seleção de eventos de Crítico

7. **Avaliação e limitação da carga de eventos no banco de dados**

   As informações sobre eventos que ocorrem durante a operação de aplicativos gerenciados são transferidas a partir de um dispositivo cliente e registradas no banco de dados do Servidor de Administração. Para reduzir a carga do Servidor de Administração, avalie e limite o número máximo de eventos que podem ser armazenados no banco de dados.

   Instruções de como proceder:

   - Limitação do número máximo de eventos

8. **Análise de informações de licença**

   Instruções de como proceder:

   - Adicione o widget de Uso de chaves de licença ao painel e o analise
   - Gere e revise o Relatório de uso das chaves de licença

Resultados

Após a conclusão do cenário, você é informado sobre a proteção da rede da sua organização e, portanto, poderá planejar ações para proteção adicional.

Sobre os tipos do monitoramento e relatórios

As informações sobre eventos de segurança na rede de uma organização são armazenadas no banco de dados do Servidor de Administração. Com base nos eventos, o Kaspersky Security Center Web Console fornece os seguintes tipos de monitoramento e relatórios na rede da sua organização:

- Painel
- Relatórios
- Seleções de eventos
- Notificações

Painel

O painel permite monitorar tendências de segurança na rede da sua organização fornecendo uma exibição gráfica das informações.

Relatórios

O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las.

Seleções de eventos

As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. Esses conjuntos de eventos são agrupados de acordo com as seguintes categorias:

- Por nível de importância – **Eventos críticos**, **Falhas funcionais**, **Advertências** e **Eventos de informações**
- Por tempo – **Eventos recentes**
- Por tipo – **Pedidos de usuário** e **Eventos de auditoria**

Você pode criar e visualizar seleções de eventos definidas pelos usuários baseado nas configurações disponíveis para configuração na interface do Kaspersky Security Center Web Console.

As Notificações alertam sobre os eventos e ajudam a agilizar as respostas a estes eventos executando ações recomendadas ou ações que você considera apropriadas.

Acionamento de regras no modo de Treinamento inteligente

Esta seção fornece informações sobre as detecções realizadas pelas regras do Controle Adaptativo de Anomalias no Kaspersky Endpoint Security for Windows em dispositivos cliente.

As regras detectam e podem bloquear comportamento anômalo nos dispositivos cliente. Se as regras funcionarem no modo de Treinamento Inteligente, elas detectarão o comportamento anômalo e enviarão relatórios sobre cada ocorrência ao Servidor de Administração. Você pode conferir os relatórios sobre comportamento anômalo detectado em **Repositórios → Acionadores de regra no estado de Treinamento inteligente**. Você pode confirmar que as detecções estão corretas ou adicioná-las como exclusões para que esse tipo do comportamento não seja mais considerado como anômalo.

As informações sobre detecções são armazenadas no log de eventos no Servidor de Administração (junto com outros eventos) e no relatório do Controle Adaptativo de Anomalias.

Para mais informações sobre o Controle Adaptativo de Anomalia, as regras, seus modos e status, consulte a Ajuda do Kaspersky Endpoint Security for Windows Help.

Exibir e confirmar detecções executadas usando regras do Controle Adaptativo de Anomalias

Para exibir a lista de detecções executadas usando regras do Controle Adaptativo de Anomalias:

1. No menu principal, vá para **Repositórios → Acionadores de regra no estado de Treinamento inteligente**.

   A lista exibe as seguintes informações sobre as detecções executadas usando regras do Controle Adaptativo de Anomalias:

   - **Grupo de administração**

     O nome do grupo de administração ao qual o dispositivo pertence.

   - **Servidor de Administração virtual**

     Servidor de Administração virtual que gerencia o dispositivo.

   - **Nome do dispositivo**

     O nome do dispositivo cliente onde a regra foi aplicada.

- **Nome**

  O nome da regra aplicada.

- **Status**

  Excluir – Se o Administrador processou e adicionou este item como uma exclusão às regras. Este status permanecerá até a próxima sincronização do dispositivo cliente com o Servidor de Administração; após a sincronização, o item desaparecerá da lista.

  Confirmar – Se o Administrador processou e confirmou este item. Este status permanecerá até a próxima sincronização do dispositivo cliente com o Servidor de Administração; após a sincronização, o item desaparecerá da lista.

  Vazio – Se o Administrador não processou este item.

- **Contagem de detecções**

  O número de detecções incluídas em uma regra heurística, em um processo e em um dispositivo cliente. Este número é contabilizado pelo Kaspersky Endpoint Security.

- **Nome do usuário**

  O nome do usuário de dispositivo cliente que executou o processo que gerou a detecção.

- **Caminho do processo de origem**

  Caminho até o processo de origem, isto é, até o processo que executa a ação (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do processo de origem**

  Hash SHA256 do arquivo do processo de origem (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Caminho do objeto de origem**

  Caminho até o objeto que iniciou o processo (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do objeto de origem**

  Hash SHA256 do arquivo de origem (para mais informações, consulte a ajuda do Kaspersky Endpoint Security).

- **Caminho do processo de destino**

  Caminho até o processo de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do processo de destino**

  Hash SHA256 do processo de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Caminho do objeto de destino**

  Caminho até o objeto de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do objeto de destino**

  Hash SHA256 do processo de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Processado**

  Data em que a anomalia foi detectada.

Para visualizar as propriedades de uma detecção:

1. No menu principal, vá para **Repositórios** → **Acionadores de regra no estado de Treinamento inteligente**.
2. Execute uma das seguintes ações:

   - Na coluna **Nome**, clique no link com o nome da detecção que deseja visualizar.
   - Na lista de detecções, marque a caixa de seleção ao lado da detecção que deseja visualizar e clique no botão **Propriedades**.

   A janela de propriedades da detecção selecionada é aberta e exibe as informações sobre ela.

Você pode confirmar qualquer detecção na lista de detecções das regras do Controle Adaptativo de Anomalias ou na janela de propriedades de uma detecção selecionada.

Para confirmar uma detecção:

- Selecione uma ou várias detecções na lista de detecções e clique no botão **Confirmar**.
- Abra a janela de propriedades de uma detecção selecionada e clique no botão **Confirmar**.

O status da detecção será alterado para **Confirmando**. A detecção desaparecerá da lista de detecções após a próxima sincronização do dispositivo cliente com o Servidor de Administração.

Sua confirmação contribuirá para as estatísticas em que as regras se baseiam. Para mais informações, confira a página Ajuda para Kaspersky Endpoint Security for Windows.

Adicionar exclusões a partir das regras do Controle Adaptativo de Anomalias

O assistente de exclusões Adicionar ao Controle Adaptativo de Anomalias permite adicionar exclusões das regras do Controle Adaptativo de Anomalias para o Kaspersky Endpoint Security.

Para adicionar exclusões às regras de Controle Adaptativo de Anomalias com o Assistente:

1. Inicie o Assistente de alguma das seguintes formas:

   - No menu principal, vá para **Repositórios** → **Acionadores de regra no estado de Treinamento inteligente**, selecione uma ou várias detecções e depois clique no botão **Excluir**.

     Você pode adicionar até 1.000 exclusões por vez.

Antes de adicionar uma detecção às exclusões, verifique as propriedades de detecção clicando no nome da mesma ou no botão **Propriedades**. Na janela de propriedades de detecção que será aberta, também é possível clicar no botão **Excluir**.

- No menu principal, vá para **Monitoramento → Seleções de eventos**, clique no link que contém a seleção de eventos necessária, marque a caixa de seleção ao lado da detecção que você quer excluir e clique no botão **Excluir do Controle Adaptativo de Anomalia**.

O assistente Adicionar exclusões ao Controle Adaptativo de Anomalias é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Selecione as políticas e os perfis aos quais você quer adicionar exclusões.

   As políticas herdadas não podem ser atualizadas. Se você não tiver os direitos de modificar uma política, ela não será atualizada.

3. Clique em **Concluído** para fechar o assistente.

O status da detecção será alterado para **Excluindo**. A detecção desaparecerá da lista de detecções após a próxima sincronização do dispositivo cliente com o Servidor de Administração. A exclusão das regras de Controle Adaptativo de Anomalias é configurada e aplicada.

Painel e widgets

Esta seção contém informações sobre o painel e os widgets que o painel fornece. A seção inclui instruções sobre como gerenciar e definir as configurações dos widgets.

Usar o painel

O painel permite monitorar tendências de segurança na rede da sua organização fornecendo uma exibição gráfica das informações.

O painel está disponível no Kaspersky Security Center Web Console, na seção **Monitoramento**, clicando em **Painel**.

O painel fornece widgets que podem ser personalizados. Você pode selecionar um grande número de widgets diferentes, apresentadas como gráficos de pizza ou gráficos de rosca, tabelas, gráficos, gráficos de barras e listas. As informações exibidas nos widgets são atualizadas automaticamente; o período de atualização é de um a dois minutos. O intervalo entre atualizações varia para widgets diferentes. Você pode atualizar dados sobre um widget manualmente a qualquer momento por meio do menu de configurações.

Por padrão, os widgets contém informações sobre todos os eventos armazenados no banco de dados do Servidor de Administração.

O Kaspersky Security Center Web Console tem um conjunto padrão de widgets para as seguintes categorias:

- **Status da proteção**
- **Implementação**
- **Atualizando**

- **Estatísticas de ameaças**
- **Outro**

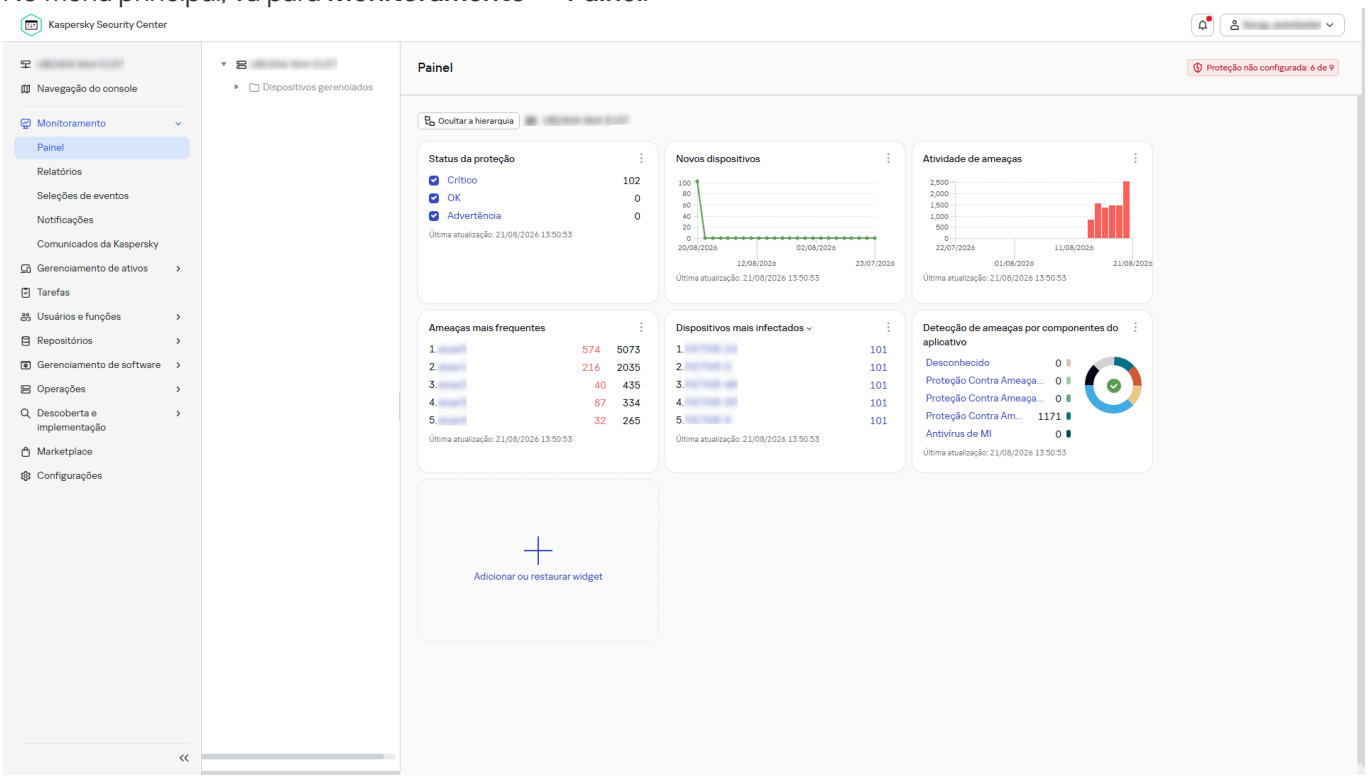
Alguns widgets têm informações de texto com links. Você pode exibir informações detalhadas clicando no link.

Ao configurar o painel, você pode adicionar os widgets de que precisa, ocultar widgets de que não precisa, modificar o tamanho ou a aparência de widgets, mover widgets e modificar suas configurações.

Adição de widgets ao painel

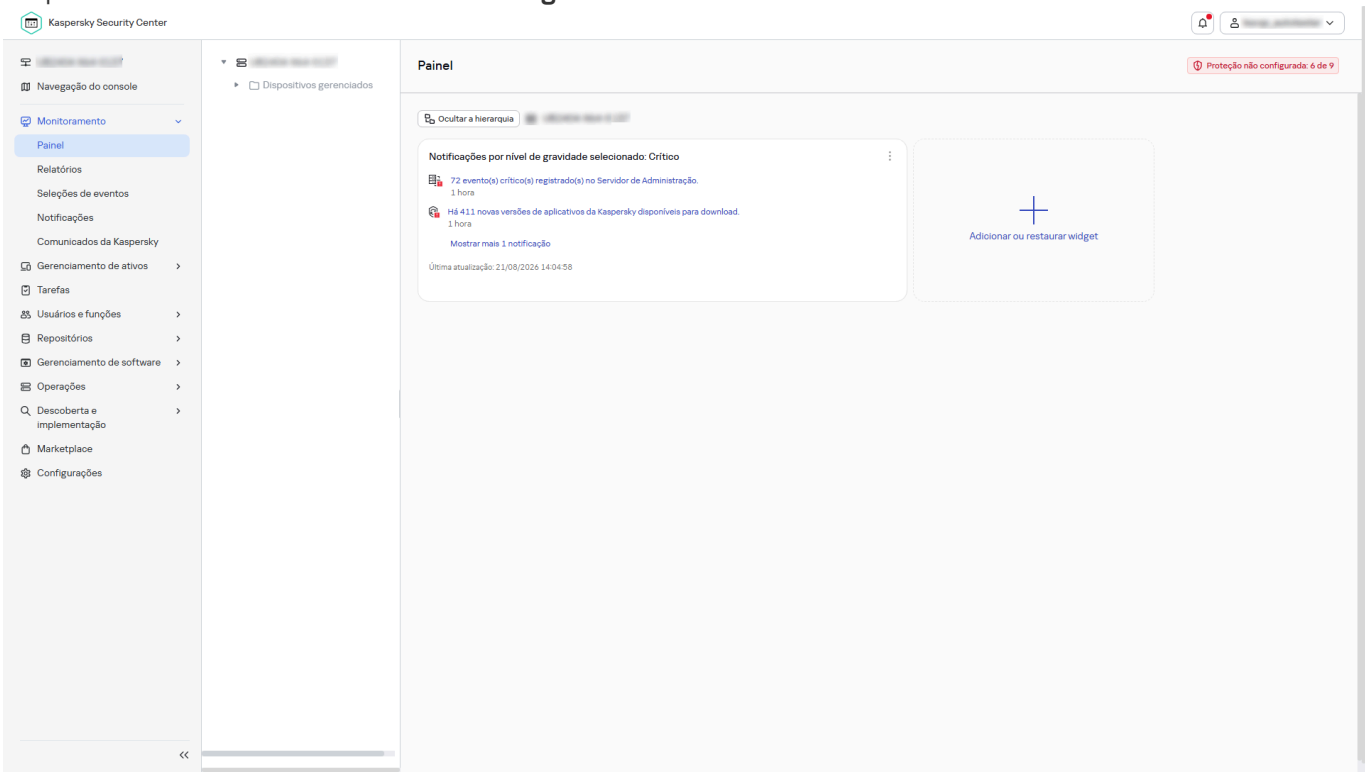
Para adicionar widgets ao painel:

1. No menu principal, vá para **Monitoramento → Painel**.



O painel com widgets

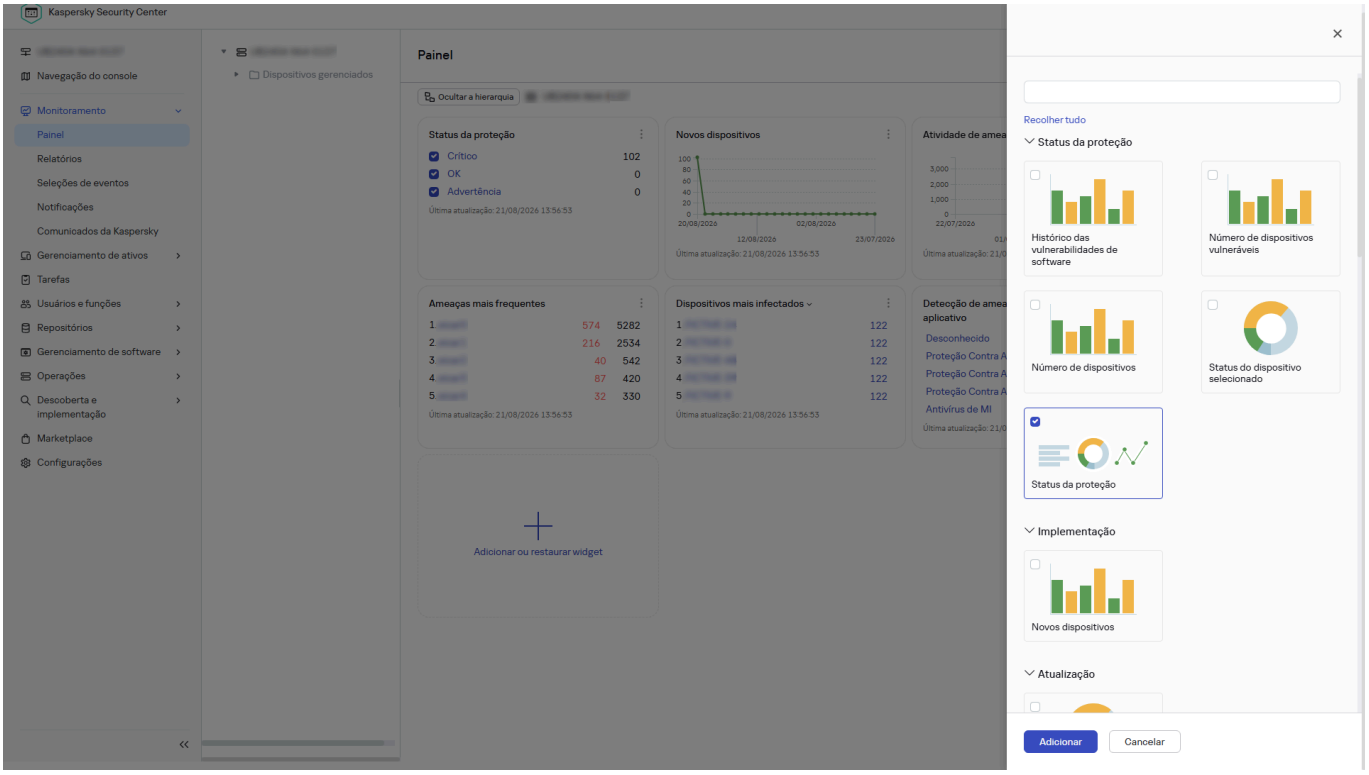
2. Clique no botão **Adicionar ou restaurar widget**.



Adição de um widget

3. Na lista de widgets disponíveis, selecione os widgets que deseja adicionar ao painel.

   Os widgets são agrupados por categoria. Para visualizar a lista de widgets incluídos em uma categoria, clique no ícone de insígnia (>) ao lado do nome da categoria.



Seleção do tipo de widget

4. Clique em **Adicionar**.

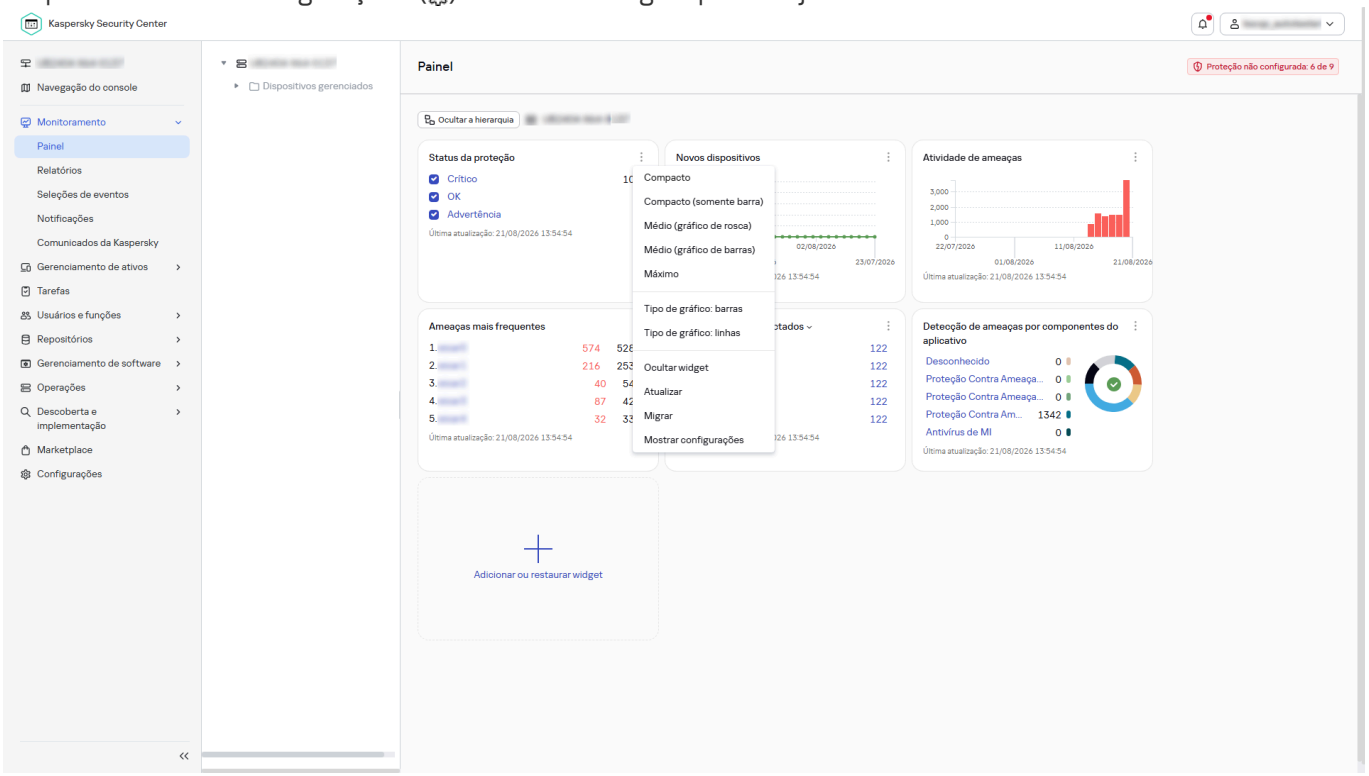
Os widgets selecionados são adicionados no final do painel.

Você pode editar agora a representação e os parâmetros dos widgets adicionados.

Ocultação de um widget do painel

Para ocultar um widget exibido do painel:

1. No menu principal, vá para **Monitoramento** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja ocultar.



O menu de widgets

3. Selecione **Ocultar widget**.
4. Na janela **Advertência** que se abre, clique em **OK**.

O widget selecionado fica oculto. Depois, você pode adicionar esse widget ao painel novamente.

Movimentação de um widget no painel

Para mover um widget no painel:

1. No menu principal, vá para **Monitoramento** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja mover.

3. Selecione **Migrar**.

4. Clique no lugar para o qual deseja mover o widget. Você pode selecionar apenas outro widget.

Os lugares dos widgets selecionados são trocados.

Alteração do tamanho ou da aparência do widget

Para widgets que exibem um gráfico, você pode alterar sua representação: um gráfico de barras ou um gráfico de linhas. Para alguns widgets, você pode alterar seu tamanho: compacto, médio ou máximo.

Para alterar a representação do widget:

1. No menu principal, vá para **Monitoramento** → **Painel**.

2. Clique no ícone de configurações (⚙) ao lado do widget que deseja editar.

3. Execute uma das seguintes ações:

   - Para exibir o widget como um gráfico de barras, selecione **Tipo de gráfico: barras**.
   - Para exibir o widget como um gráfico de linhas, selecione **Tipo de gráfico: linhas**.
   - Para alterar a área ocupada pelo widget, selecione um dos valores:
     - **Compacto**
     - **Compacto (somente barra)**
     - **Médio (gráfico de rosca)**
     - **Médio (gráfico de barras)**
     - **Máximo**

A representação do widget selecionado é alterada.

Alteração das configurações do widget

Para alterar as configurações de um widget:

1. No menu principal, vá para **Monitoramento** → **Painel**.

2. Clique no ícone de configurações (⚙) ao lado do widget que deseja editar.

3. Selecione **Mostrar configurações**.

4. Na janela de configurações de widget exibida, modifique as configurações de widget conforme necessário.

5. Clique em **Salvar** para salvar as alterações.

As configurações do widget selecionado são alteradas.

O conjunto de configurações depende do widget específico. Abaixo estão algumas configurações comuns:

- **Escopo do widget** (o conjunto de objetos para os quais o widget exibe informações): por exemplo, um grupo de administração ou uma seleção de dispositivos.
- **Selecionar tarefa** define a tarefa para a qual o widget exibe informações.
- **Intervalo de tempo** (o intervalo de tempo durante o qual as informações são exibidas no widget): entre as duas datas especificadas; desde a data especificada até o dia atual; ou do dia atual menos o número especificado de dias até o dia atual.
- As regras **Definir como Crítico se as seguintes configurações forem especificadas** e **Definir como Advertência se as seguintes configurações forem especificadas** determinam como as cores são atribuídas no gráfico de status.

Depois de alterar as configurações do widget, você pode atualizar os dados manualmente.

Para atualizar dados e um widget:

1. No menu principal, vá para **Monitoramento → Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja mover.
3. Selecione **Atualizar**.

Os dados no widget são atualizados.

Sobre o modo somente painel

É possível configurar o modo somente painel para funcionários que não gerenciam a rede, mas que desejam visualizar as estatísticas de proteção da rede no Kaspersky Security Center Linux (por exemplo, um gerente superior). Quando um usuário tem esse modo ativado, apenas um painel com um conjunto predefinido de widgets é exibido para o usuário. Assim, ele pode monitorar as estatísticas especificadas nos widgets, por exemplo, o status de proteção de todos os dispositivos gerenciados, o número de ameaças detectadas recentemente ou a lista das ameaças mais frequentes na rede.

Quando um usuário trabalha no modo somente painel, as seguintes restrições são aplicadas:

- O menu principal não é exibido para o usuário, portanto, ele não pode alterar as configurações de proteção de rede.
- O usuário não pode realizar nenhuma ação com widgets, por exemplo, adicioná-los ou ocultá-los. Portanto, não é necessário colocar todos os widgets requeridos para o usuário no painel e configurá-los, por exemplo, para definir a regra de contagem de objetos ou especificar o intervalo de tempo.

Não é possível atribuir o modo somente painel a si mesmo. Caso queira trabalhar nesse modo, entre em contato com um administrador do sistema, o Provedor de Serviços Gerenciados (MSP) ou um usuário com o direito **Modificar ACLs de objetos** na área funcional **Recursos gerais: Permissões do usuário**.

Configurando o modo somente painel

Antes de iniciar a configuração do Modo somente painel, verifique se os seguintes pré-requisitos foram atendidos:

- O usuário tem o direito de **Modificar ACLs de objetos** na área funcional **Recursos gerais: permissões do usuário**. Caso não tenha esse direito, a guia para configurar o modo estará ausente.
- O usuário tem o direito de **Leitura** na área funcional **Recursos gerais: funcionalidade básica**.

Caso uma hierarquia de Servidores de Administração esteja organizada em sua rede, para configurar o modo somente Painel, acesse o servidor onde a conta de usuário está disponível na guia **Usuários** da seção **Usuários e funções → Usuários e grupos**. Pode ser um servidor principal ou um servidor secundário físico. Não é possível ajustar o modo em um servidor virtual.

Para configurar o modo somente painel:

1. No menu principal, vá para **Usuários e funções → Usuários e grupos** e, em seguida, selecione a guia **Usuários**.
2. Clique no nome da conta de usuário para a qual deseja ajustar o painel com widgets.
3. Na janela aberta de configurações do usuário, selecione a guia **Painel**.

   Na guia aberta, o mesmo painel é exibido para você e para o usuário.
4. Caso o **modo Exibir o console no modo somente painel** estiver habilitado, alterne o botão de alternância para desativá-la.

   Quando essa opção está habilitada, também não será possível alterar o painel. Depois de desativar a opção, será possível gerenciar widgets.
5. Configure a aparência do painel. O conjunto de widgets preparados na guia **Painel** está disponível para o usuário com a conta personalizável. Ele ou ela não pode alterar nenhuma configuração ou tamanho dos widgets, adicionar ou remover quaisquer widgets do painel. Portanto, ajuste-os para o usuário, para que ele possa visualizar as estatísticas de proteção da rede. Para isso, na guia **Painel**, é possível executar as mesmas ações com widgets que na seção **Monitoramento → Painel**:
   - Adicionar novos widgets ao painel.
   - Ocultar widgets que o usuário não precisa.
   - Mover widgets em uma ordem específica.
   - Alterar o tamanho ou a aparência de widgets.
   - Alterar as configurações do widget.
6. Alterne o botão de alternância para habilitar a opção **Exibir o console no modo somente painel**.

   Depois disso, apenas o painel ficará disponível para o usuário. Ele ou ela pode monitorar as estatísticas, mas não pode alterar as configurações de proteção de rede e a aparência do painel. Como o mesmo painel é exibido para você e para o usuário, você também não pode alterar o painel.

   Caso mantenha a opção desativada, o menu principal será exibido ao usuário, para que ele possa realizar várias ações no Kaspersky Security Center Linux, inclusive alterar as configurações de segurança e os widgets.

7. Clique no botão **Salvar** quando terminar de configurar o modo somente painel. Somente depois disso o dashboard preparado será exibido ao usuário.

8. Caso o usuário queira visualizar as estatísticas de aplicativos Kaspersky compatíveis e precisar de direitos de acesso para isso, configure os direitos para o usuário. Depois disso, os dados dos aplicativos Kaspersky são exibidos para o usuário nos widgets desses aplicativos.

Agora, o usuário pode fazer login no Kaspersky Security Center Linux com a conta personalizada e monitorar as estatísticas de proteção de rede no modo somente painel.

Relatórios de administração e proteção

Esta seção descreve como usar relatórios, gerenciar modelos de relatórios personalizados, usar modelos de relatórios para gerar novos relatórios e criar tarefas de entrega de relatórios.

Usar os relatórios

O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las.

Os relatórios estão disponíveis no Kaspersky Security Center Web Console, na seção **Monitoramento**, clicando em **Relatórios**.

Por padrão, os relatórios contém informações dos últimos 30 dias.

O Kaspersky Security Center Linux tem um conjunto padrão de relatórios para as seguintes categorias:

- **Status da proteção**
- **Implementação**
- **Atualizando**
- **Estatísticas de ameaças**
- **Outro**

Você pode criar modelos de relatório personalizados, editar modelos de relatório e excluí-los.

Você pode criar relatórios que são baseados em modelos existentes, exportar relatórios para arquivos e criar tarefas para entrega de relatório.

Criação de um modelo de relatório

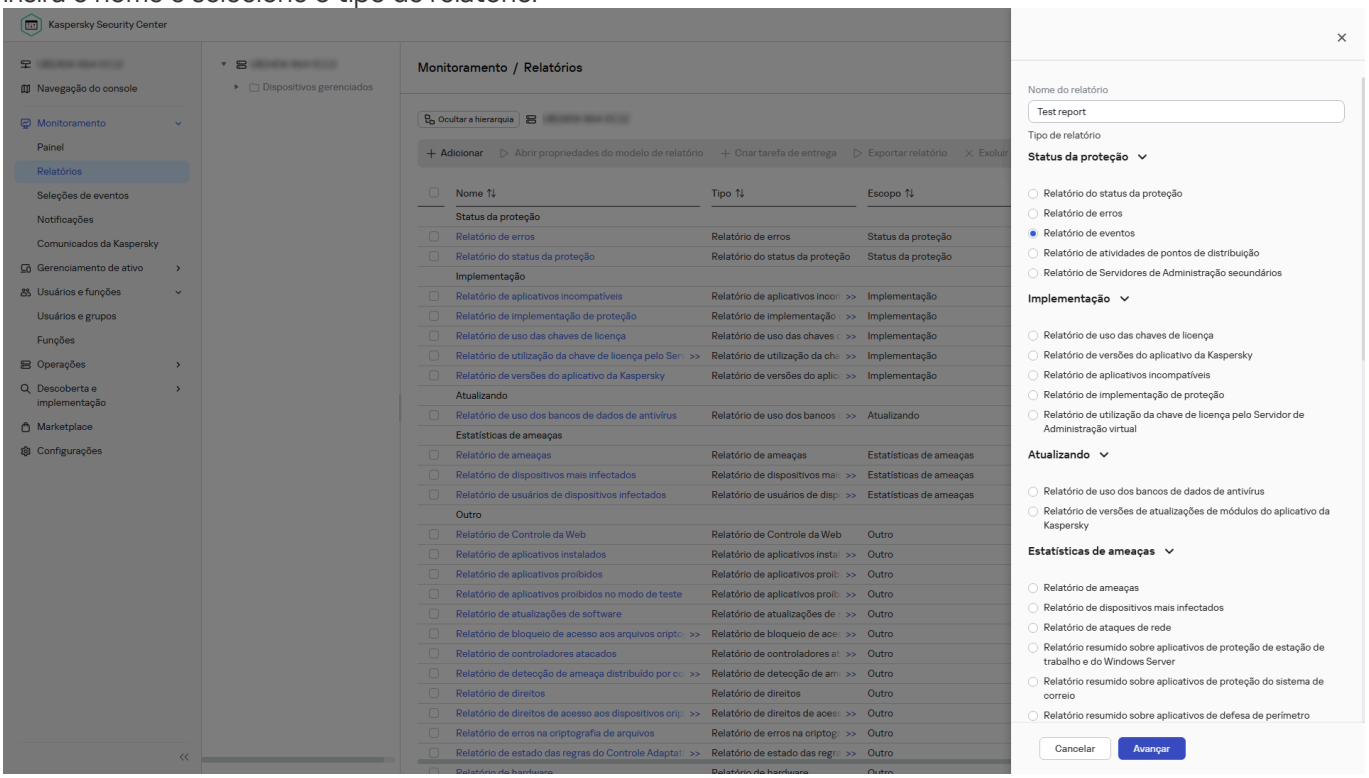
Para criar um modelo de relatório:

1. No menu principal, vá para **Monitoramento** → **Relatórios**.

2. Clique em **Adicionar**.

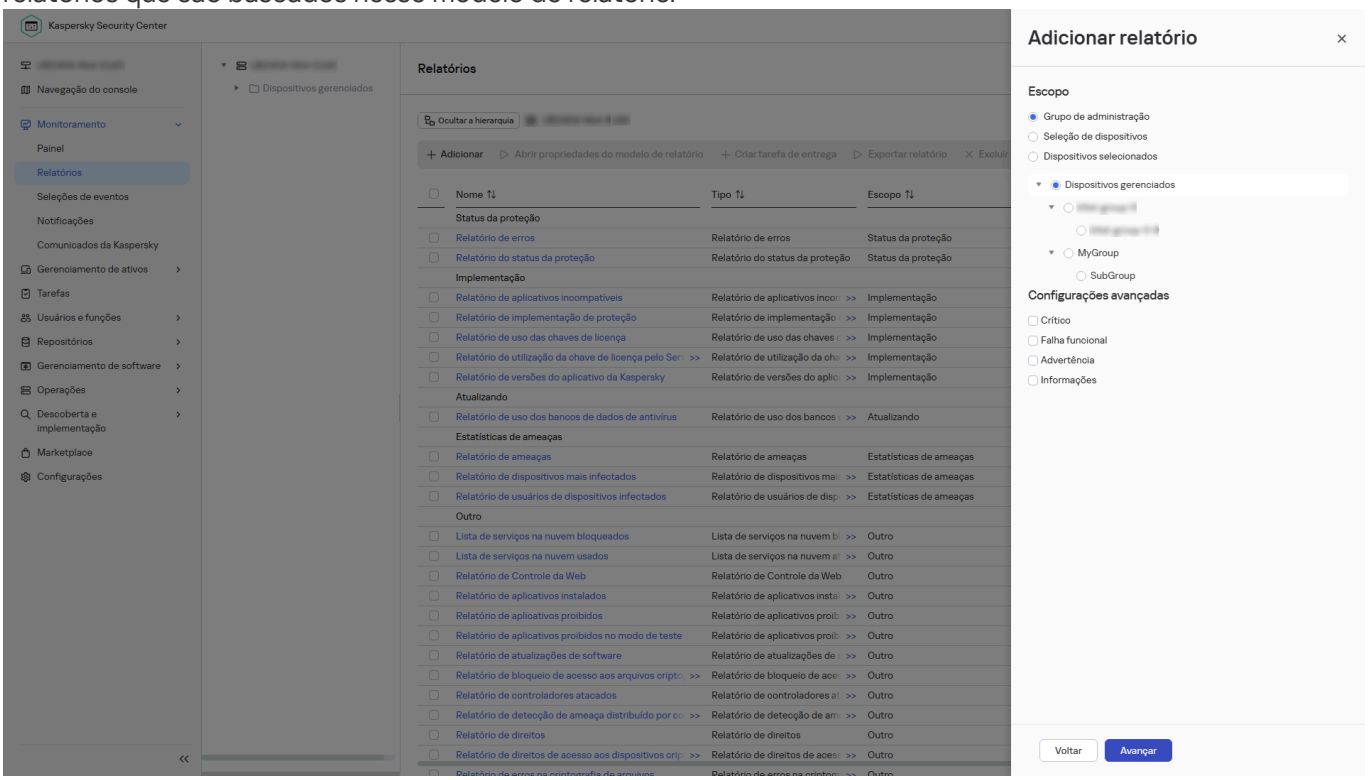
   O assistente de novo modelo de relatório é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

3. Insira o nome e selecione o tipo de relatório.



Especificação do nome do relatório e seleção do tipo de relatório

4. Na etapa **Escopo** do assistente, selecione o conjunto de dispositivos clientes (grupo de administração, seleção de dispositivos, dispositivos selecionados ou todos os dispositivos em rede) cujos dados serão exibidos em relatórios que são baseados nesse modelo de relatório.

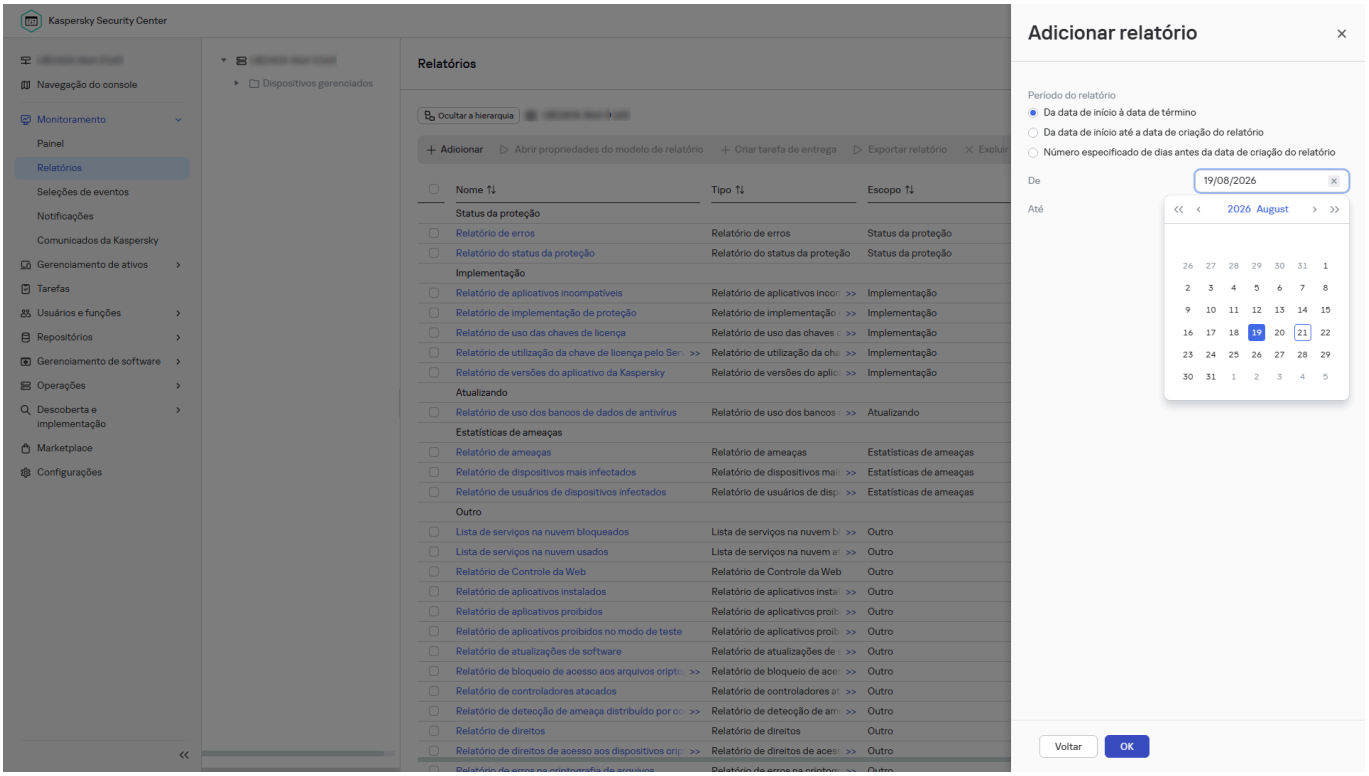


Especificação do escopo do relatório

5. Na etapa **Período do relatório** do assistente, especifique o período de relatório. Valores disponíveis:

   - Entre as duas datas especificadas
   - A partir da data especificada até à data de criação do relatório
   - Desde a data de criação do relatório menos o número especificado de dias, até a data de criação do relatório

Essa página pode não aparecer para alguns relatórios.



Especificação do período do relatório

6. Clique em **OK** para fechar o assistente.

7. Execute uma das seguintes ações:

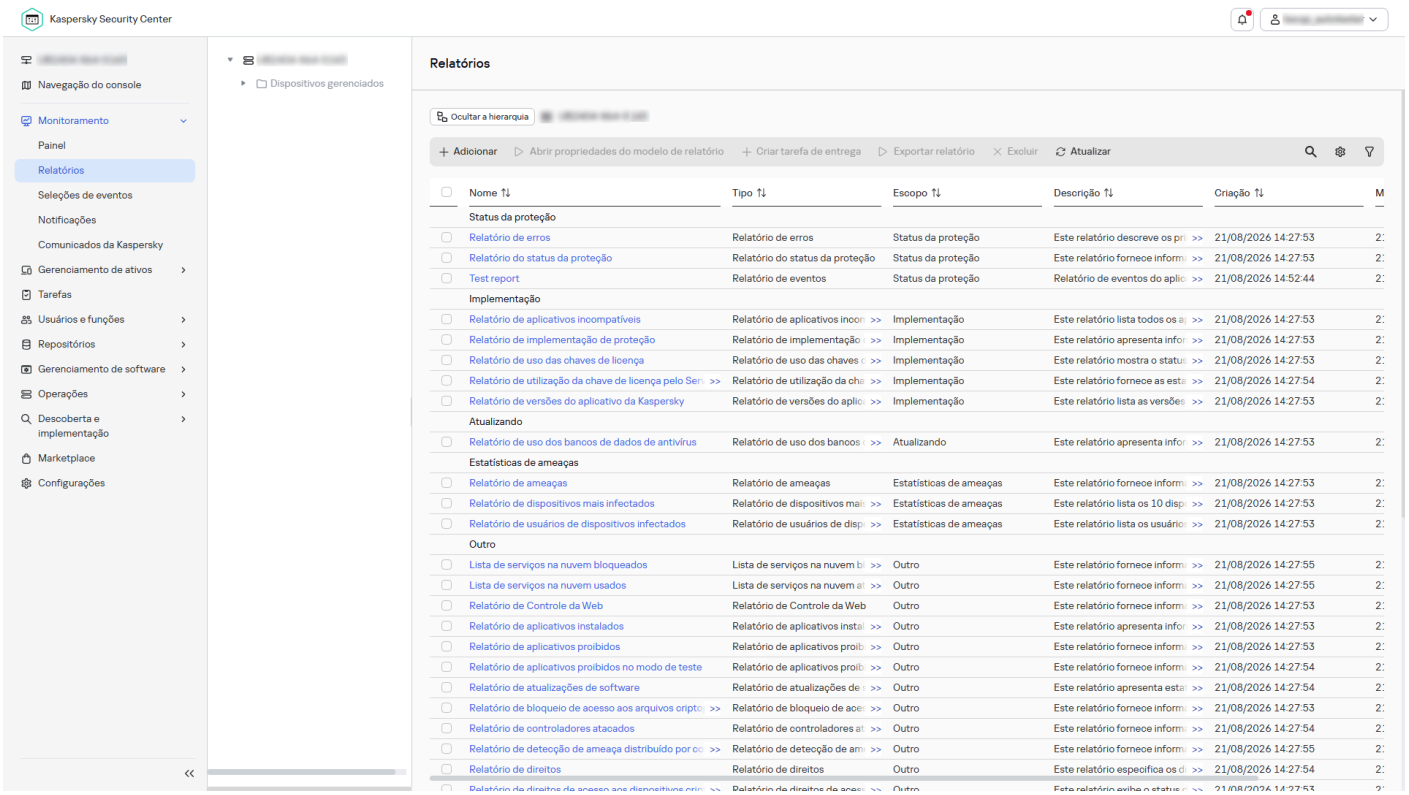
   - Clique no botão **Salvar e executar** para salvar o novo modelo de relatório e executar um relatório baseado nele.

     O modelo de relatório é salvo. O relatório é gerado.

   - Clique no botão **Salvar** para salvar o novo modelo de relatório.

     O modelo de relatório é salvo.

Você pode usar o novo modelo para gerar e visualizar relatórios.



A lista de relatórios

Visualização e edição das propriedades do modelo de relatório

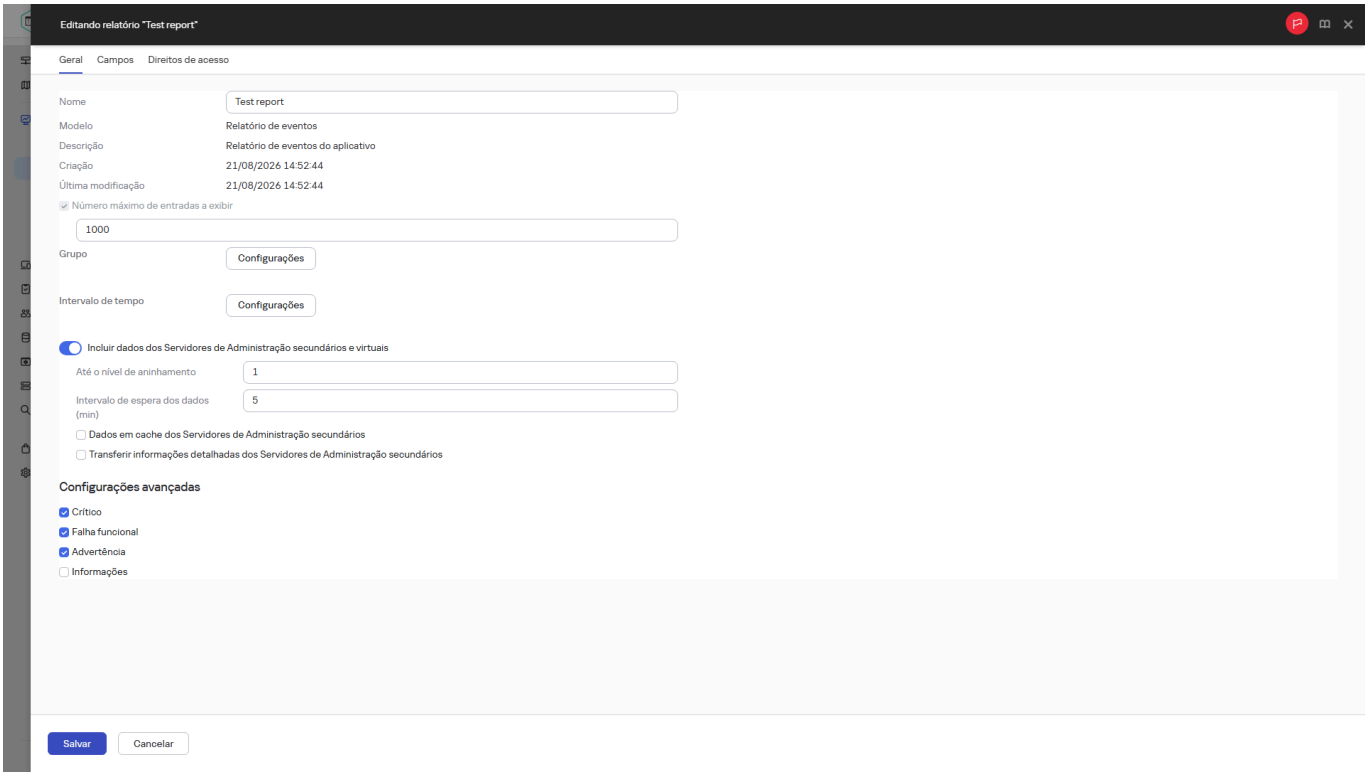
Você pode visualizar e editar propriedades básicas de um modelo de relatório como, por exemplo, o nome do modelo de relatório ou os campos exibidos no relatório.

Para visualizar e editar propriedades de um modelo de relatório:

1. No menu principal, vá para **Monitoramento** → **Relatórios**.
2. Marque a caixa de seleção ao lado do modelo de relatório cujas propriedades deseja visualizar e editar.

   Como uma alternativa, você pode primeiro gerar o relatório e depois clicar no botão **Editar**.
3. Clique no botão **Abrir propriedades do modelo de relatório**.

A janela **Edição de relatório <Nome do relatório>** é exibida com a guia **Geral** selecionada.



As propriedades do modelo de relatório

4. Edite as propriedades do modelo de relatório:

   - Guia **Geral**:

     - Nome do modelo de relatório

     - **Número máximo de entradas a exibir**

       Se esta opção estiver ativada, o número de entradas exibidas na tabela com dados de relatório detalhados não será maior que o valor especificado. Observe que esta opção não afeta o número máximo de eventos que é possível incluir no relatório ao exportar o relatório para um arquivo.

       As entradas de relatório são primeiro classificadas segundo as regras especificadas na seção **Campos → Campos de detalhes** das propriedades do modelo de relatório e, em seguida, apenas a primeira das entradas resultantes é mantida. O cabeçalho da tabela com dados de relatório detalhados mostra o número de entradas exibidas e o número total de entradas disponíveis que combinam com outras configurações do modelo de relatório.

       Se esta opção estiver desativada, a tabela com dados de relatório detalhados exibe todas as entradas disponíveis. Não recomendamos que você desative essa opção. Limitar o número de entradas de relatório exibidas reduz a carga do sistema de gerenciamento de banco de dados (DBMS) e reduz o tempo necessário para gerar e exportar o relatório. Alguns dos relatórios contêm entradas excessivas. Se este for o caso, você pode ter dificuldade para ler e analisar todas elas. Além disso, o dispositivo pode ficar sem memória ao gerar esse relatório. Isso pode impedir que você visualize o relatório.

       Por padrão, esta opção está ativada. O valor predefinido é de 1.000.

     - **Grupo**

       Clique no botão **Configurações** para alterar o conjunto de dispositivos clientes para os quais o relatório é criado. Para alguns tipos dos relatórios, o botão pode estar indisponível. As configurações reais dependem das configurações especificadas durante a criação do modelo de relatório.

     - **Intervalo de tempo**

Clique no botão **Configurações** para modificar o período de relatório. Para alguns tipos dos relatórios, o botão pode estar indisponível. Valores disponíveis:

- Entre as duas datas especificadas
- A partir da data especificada até à data de criação do relatório
- Desde a data de criação do relatório menos o número especificado de dias, até a data de criação do relatório

- **Incluir dados dos Servidores de Administração secundários e virtuais**

  Se esta opção estiver ativada, o relatório inclui as informações dos Servidores de Administração secundário e virtual subordinados ao Servidor de Administração para o qual o modelo de relatório é criado.

  Desative esta opção se você quiser visualizar dados somente do Servidor de Administração atual.

  Por padrão, esta opção está ativada.

- **Até o nível de aninhamento**

  O relatório inclui dados de servidores de administração secundários e virtuais localizados sob o Servidor de administração atual a um nível de agrupamento menor ou igual ao valor especificado.

  O valor padrão é 1. Convém alterar esse valor caso necessite recuperar as informações dos Servidores de administração secundários localizados em níveis mais baixos na árvore.

- **Intervalo de espera dos dados (min)**

  Antes de gerar o relatório, o Servidor de administração para o qual o modelo de relatório é criado aguarda pelos dados de Servidores de administração secundários durante o número de minutos especificado. Se nenhum dado for recebido de um Servidor de administração secundário ao fim desse período, o relatório é executado mesmo assim. Em vez de dados reais, o relatório exibe os dados retirados do cache (se a opção **Dados em cache dos Servidores de Administração secundários** estiver ativada) ou, caso contrário, **N/A** (não acessível).

  O valor padrão é de 5 minutos.

- **Dados em cache dos Servidores de Administração secundários**

  Os Servidores de Administração secundários regularmente transferem dados para o Servidor de Administração para o qual o modelo de relatório é criado. Nesse local, os dados transferidos são armazenados em cache.

  Se o Servidor de administração atual não puder receber dados de um Servidor de administração secundário enquanto o relatório estiver sendo gerado, o relatório exibirá dados retirados do cache. A data em que os dados foram transferidos para o cache também é exibida.

  Ativar essa opção permite a visualização das informações dos Servidores de administração secundários, mesmo se os dados atualizados não puderem ser recuperados. Entretanto, os dados exibidos podem ser obsoletos.

  Por padrão, esta opção está desativada.

- **Frequência de atualização de cache (h)**

  Os Servidores de Administração secundários regularmente transferem dados para o Servidor de Administração para o qual o modelo de relatório é criado. É possível especificar o período em horas. Se o valor for 0, os dados serão transferidos somente quando o relatório for gerado.

  O valor padrão é 0.

- **Transferir informações detalhadas dos Servidores de Administração secundários**

  No relatório gerado, a tabela contendo dados de relatório detalhados inclui dados dos Servidores de Administração secundários do Servidor de Administração para o qual o modelo de relatório é criado.

  Ativar esta opção reduz a velocidade de geração de relatórios e aumenta o tráfego entre Servidores de Administração. Entretanto, você pode visualizar todos os dados em um relatório.

  Em vez de ativar a opção, convém analisar dados de relatório detalhados para detectar um Servidor de administração secundário defeituoso e, em seguida, gerar o mesmo relatório apenas para o Servidor de administração defeituoso.

  Por padrão, esta opção está desativada.

- Guia **Campos**

  Selecione os campos que deseja exibir no relatório. Use os botões **Para cima** e **Para baixo** para alterar a ordem de exibição dos campos. Use o botão **Adicionar** ou **Editar** para especificar se as informações no relatório devem ser classificadas e filtradas segundo cada um dos campos.

  Na seção **Filtros dos campos Detalhes**, você também pode clicar em **Converter filtros** para começar a usar o formato de filtragem estendido. Este formato permite combinar as condições de filtragem especificadas em vários campos, usando a operação lógica OR. Depois de clicar no botão, o painel **Converter filtros** abre à direita. Clique no botão **Converter filtros** para confirmar a conversão. Agora, você pode definir um filtro convertido com as condições da seção **Campos de detalhes**, que são aplicadas usando a operação lógica OR.

  > A conversão de um relatório para o formato compatível com as condições de filtragem complexas tornará o relatório incompatível com as versões anteriores do Kaspersky Security Center (11 e anteriores). Além disso, o relatório convertido não conterá nenhum dado dos Servidores de Administração secundários executando tais versões incompatíveis.

5. Clique em **Salvar** para salvar as alterações.

6. Feche a janela **Editar relatório <Nome do relatório>**.

O modelo de relatório atualizado aparece na lista de modelos de relatório.

Exportar um relatório para um arquivo

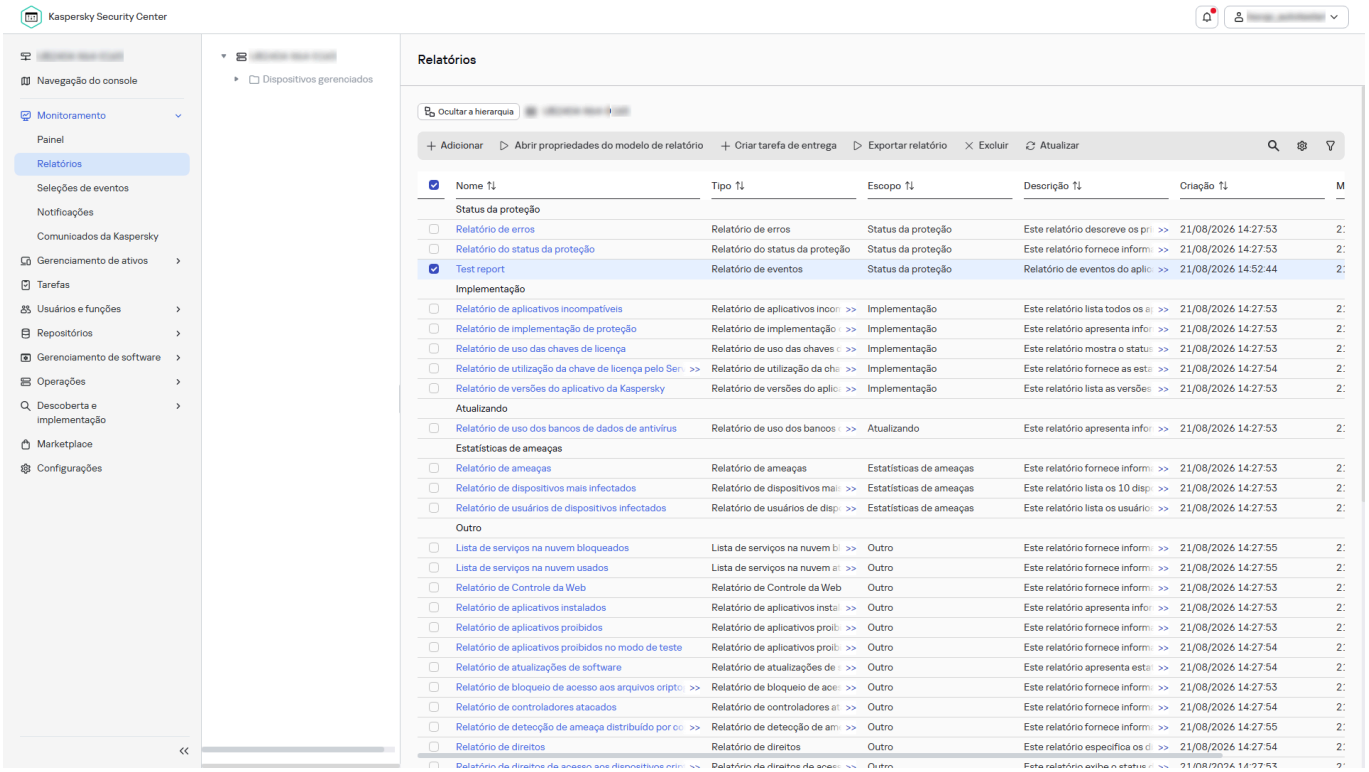
É possível salvar um ou vários relatórios em XML, HTML ou PDF. O Kaspersky Security Center Linux permite exportar até 10 relatórios para arquivos do formato especificado ao mesmo tempo.

Para exportar um relatório para um arquivo:

1. No menu principal, vá para **Monitoramento → Relatórios**.

2. Escolha os relatórios que deseja exportar.

Caso queira escolher mais de 10 relatórios, o botão **Exportar relatório** será desativado.



A lista de relatórios

3. Clique no botão **Exportar relatório**.

4. Na janela aberta, especifique os seguintes parâmetros de exportação:

   - **Nome do arquivo**.

     Ao selecionar um relatório para exportar, especifique o nome do arquivo do relatório.

     Ao selecionar mais de um relatório, os nomes dos arquivos de relatório coincidirão com o nome dos modelos de relatório selecionados.

   - **Número máximo de entradas**.

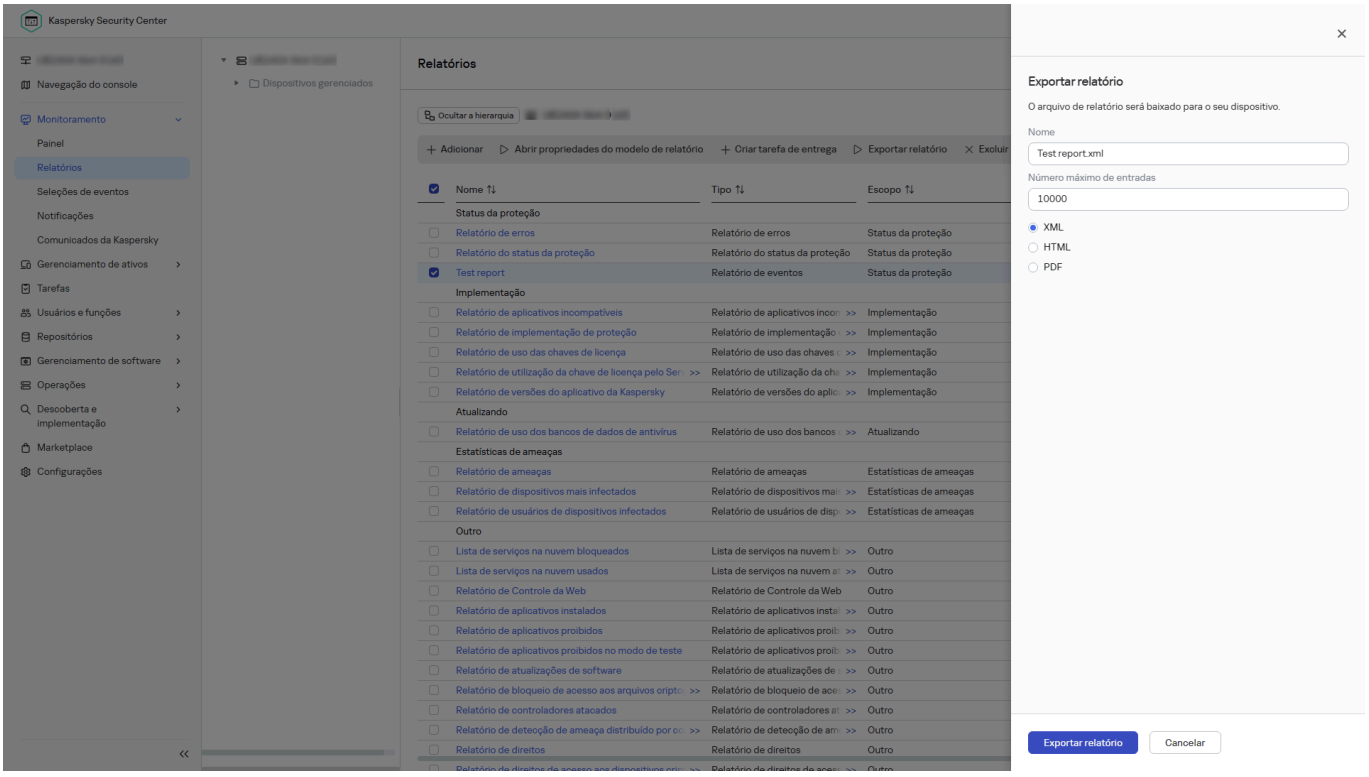
     Especifique o número máximo de entradas incluídas no arquivo de relatório. O valor padrão é 10.000.

     É possível exportar um relatório com um número ilimitado de entradas. Observe que, se o seu relatório contiver um grande número de entradas, o tempo necessário para gerar e exportar o relatório aumentará.

   - **Formato do arquivo**.

     Selecione o tipo de arquivo do relatório: XML, HTML ou PDF. Ao exportar vários relatórios, todos os relatórios selecionados serão salvos no formato especificado como arquivos separados.

A ferramenta wkhtmltopdf é necessária para converter um relatório em PDF. Ao selecionar a opção PDF, o Servidor de Administração verifica se a ferramenta wkhtmltopdf está instalada no dispositivo. Se a ferramenta não estiver instalada, o aplicativo exibirá uma mensagem sobre a necessidade de instalar a ferramenta no dispositivo do Servidor de Administração. Instale a ferramenta manualmente e prossiga para a próxima etapa.



Especificação das configurações de exportação do relatório

5. Clique no botão **Exportar relatório**.

O relatório é salvo em um arquivo no formato especificado.

Como gerar e visualizar um relatório

Para criar e visualizar um relatório:

1. No menu principal, vá para **Monitoramento** → **Relatórios**.
2. Clique no nome do modelo de relatório que deseja usar para criar um relatório.

   Um relatório usando o modelo selecionado é gerado e exibido.

Os dados do relatório são exibidos de acordo com a localização definida para o Servidor de Administração.

Nos relatórios gerados, algumas fontes podem ser exibidas incorretamente nos diagramas. Para resolver esse problema, instale a biblioteca fontconfig. Além disso, verifique se as fontes correspondentes à localidade do seu sistema operacional estão instaladas nele.

O relatório exibe os seguintes dados:

- Na guia **Resumo**:
  - O nome e tipo de relatórios, uma breve descrição e o período de relatórios, assim como as informações sobre o grupo de dispositivos para os quais o relatório é gerado.
  - Gráfico que mostra os dados do relatório mais representativos.
  - Tabela consolidada com os indicadores do relatório calculados.
- Na guia **Detalhes**, uma tabela com dados detalhados do relatório é exibida.

Criação de uma tarefa de entrega de relatório

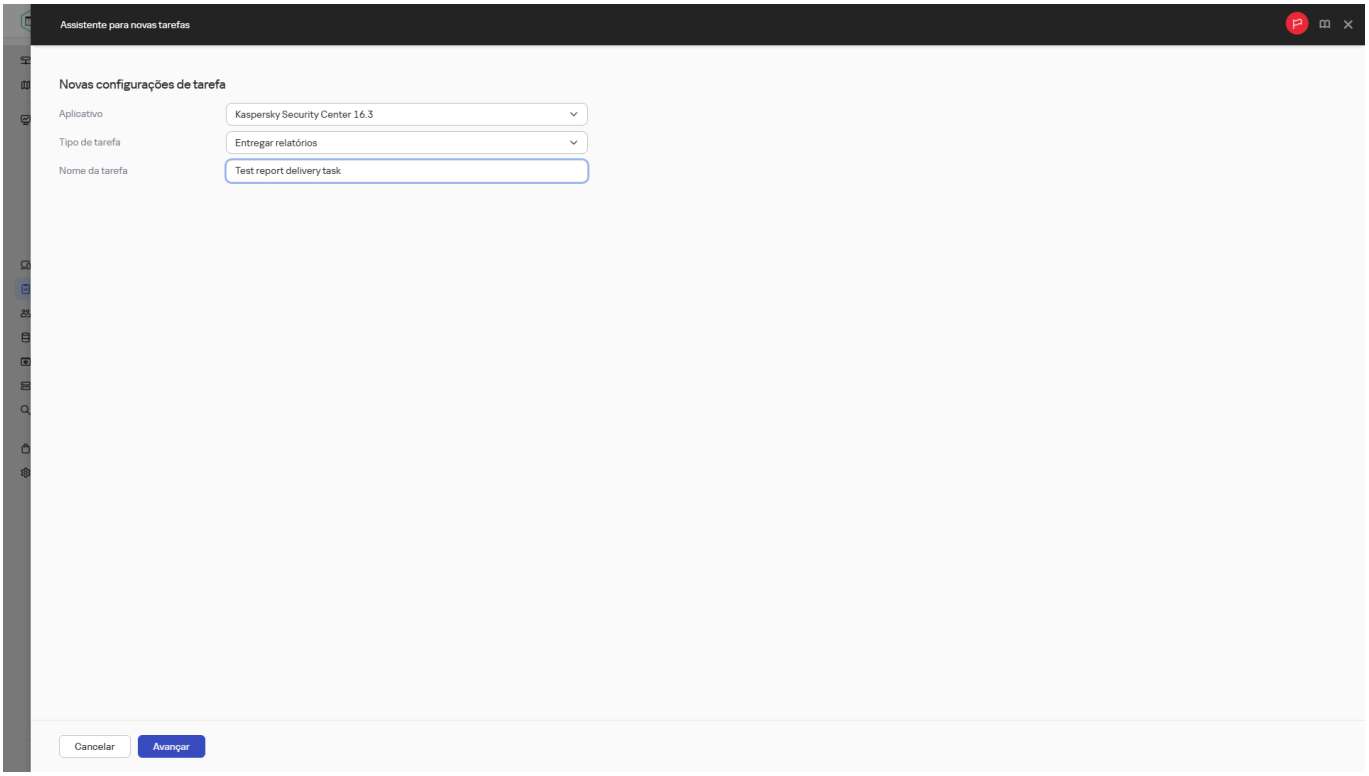
Você pode criar uma tarefa que entregará os relatórios selecionados.

Para criar uma tarefa de entrega de um relatório:

1. No menu principal, vá para **Monitoramento** → **Relatórios**.
2. Marque as caixas de seleção próximas aos modelos de relatório para os quais você deseja criar uma tarefa de entrega de relatório.
3. Clique no botão **Criar tarefa de entrega**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
4. Na etapa **Novas configurações de tarefa** do assistente, insira o nome da tarefa.

   O nome padrão é **Entregar relatórios.** Se já existir uma tarefa com este nome, um número de sequência (<N>) é adicionado ao nome da tarefa.



Criação de uma tarefa de entrega de relatório

5. Na etapa **Configuração do relatório** do assistente, especifique as seguintes configurações:

   a. Modelos de relatório a serem entregues pela tarefa.

   b. O formato do relatório: HTML, XLS ou PDF.

      A ferramenta wkhtmltopdf é necessária para converter um relatório em PDF. Ao selecionar a opção PDF, o Servidor de Administração verifica se a ferramenta wkhtmltopdf está instalada no dispositivo. Se a ferramenta não estiver instalada, o aplicativo exibirá uma mensagem sobre a necessidade de instalar a ferramenta no dispositivo do Servidor de Administração. Instale a ferramenta manualmente e prossiga para a próxima etapa.

   c. Se os relatórios precisarem ser enviados por e-mail, em conjunto com as configurações de notificação por e-mail.

      Você pode especificar até 20 endereços de e-mail. Para separar endereços de e-mail, pressione **Enter**. Você também pode colar uma lista de endereços de e-mail separados por vírgulas e pressionar **Enter**.

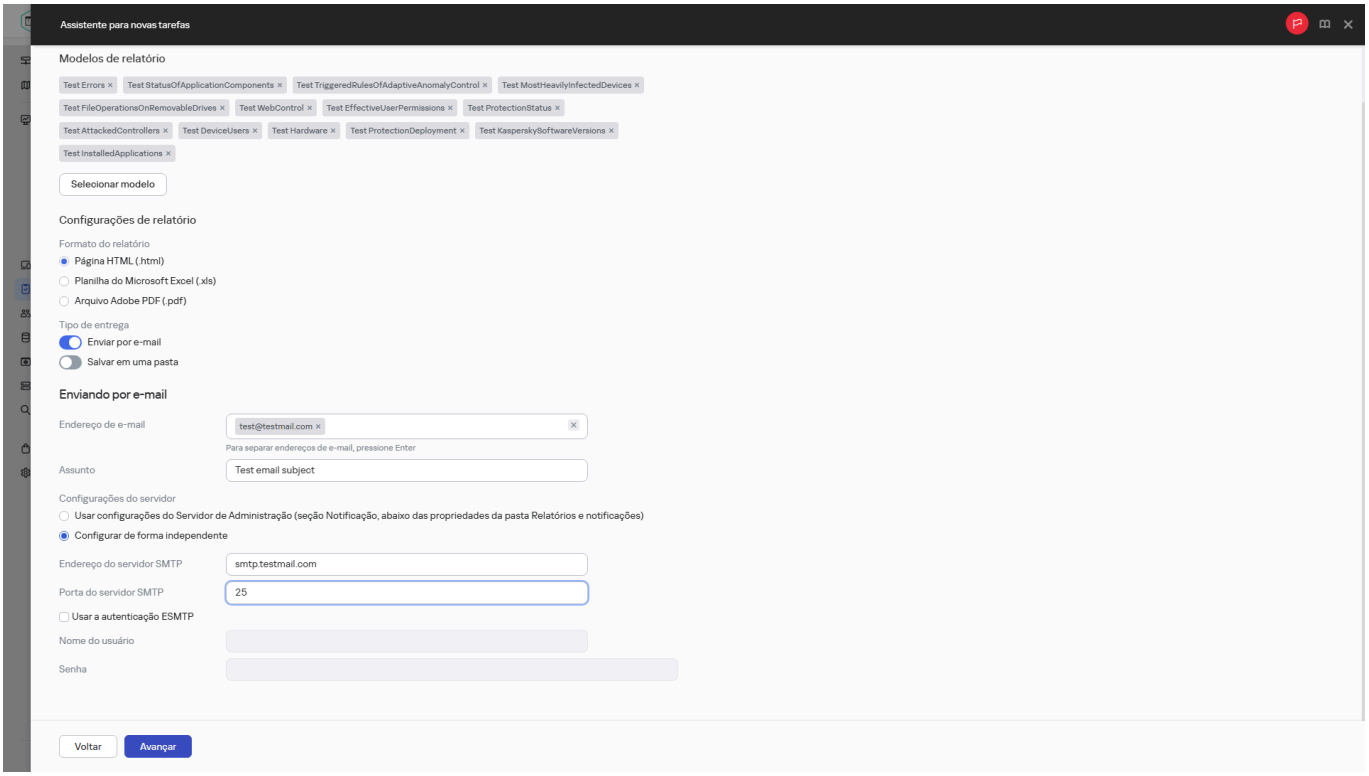
   d. Se os relatórios devem ser salvos em uma pasta, juntamente com as configurações correspondentes.

      Depois de habilitar a opção **Salvar em uma pasta**, você deve especificar um caminho POSIX para a pasta. Se quiser salvar os relatórios em uma pasta compartilhada, você também precisa marcar a caixa de seleção **Especificar uma conta para acessar a pasta compartilhada** e, em seguida, especificar a conta de usuário e a senha para acessar essa pasta.

      > Caso opte por salvar os relatórios em uma pasta compartilhada, será necessário garantir o acesso a essa pasta pelo dispositivo com o Servidor de Administração instalado. As formas de garantir o acesso e as ferramentas usadas dependem da sua infraestrutura.

      Ao salvar os relatórios em uma pasta local, geralmente não é necessário fornecer credenciais, pois a conta que executa o Servidor de Administração tem acesso a essa pasta. Se necessário, você pode especificar as credenciais do usuário na etapa **Selecionar uma conta para executar a tarefa** do assistente.

Independentemente da pasta escolhida, você pode marcar a caixa de seleção **Substituir relatórios antigos do mesmo tipo** para que o novo arquivo de relatório substitua o arquivo salvo na pasta de relatórios durante a inicialização da tarefa anterior.



Especificação das configurações da tarefa

6. Na etapa **Configurar agendamento da tarefa** do assistente, selecione o agendamento de início da tarefa.

   As seguintes opções de agendamento de tarefas estão disponíveis:

   - **Manualmente**

     A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

     Por padrão, esta opção está selecionada.

   - **A cada N minutos**

     A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

     Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

   - **A cada N horas**

     A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

     Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

   - **A cada N dias**

     A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

     Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

- **A cada N semanas**

  A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

  Por padrão, a tarefa é executada toda sexta-feira no horário atual do sistema.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Em dias especificados**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, a hora de início é 18:00 e nenhum dia do mês é selecionado.

  > Observe que você não seleciona uma data específica no mês, nem o número da semana (primeira, segunda semana do mês), mas o número de sequência do dia da semana dentro de um mês. Por exemplo, se definir o cursor na célula **Ter** da **Primeiro(a)** linha, a tarefa será executada toda primeira terça-feira de cada novo mês.

  É possível selecionar vários dias da semana.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

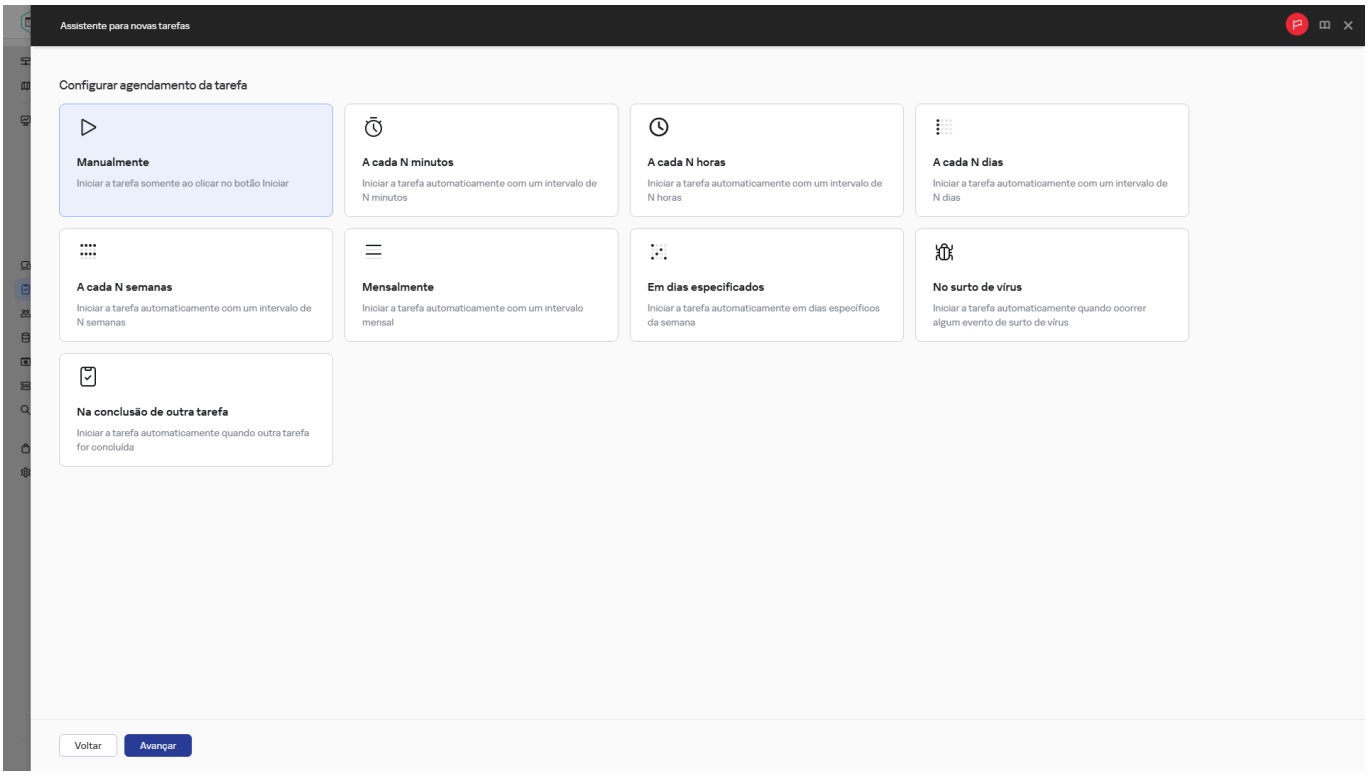
  A tarefa atual inicia após outra tarefa ser concluída. Esta opção só funciona se ambas as tarefas estiverem atribuídas aos mesmos dispositivos. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus* com um tarefa de acionamento.

  É necessário selecionar a tarefa de acionamento na tabela e o status com o qual a tarefa deve ser concluída (**Conclusão com êxito** ou **Falhou**).

Caso seja necessário, é possível pesquisar, classificar e filtrar as tarefas na tabela da seguinte maneira:

- Insira o nome da tarefa no campo de pesquisa para pesquisar a tarefa pelo nome.
- Clique no ícone de classificação para classificar as tarefas por nome.

  Por padrão, as tarefas são classificadas em ordem alfabética crescente.
- Clique no ícone de filtragem e, na janela exibida, filtre as tarefas por grupo e clique no botão **Aplicar**.



Seleção da programação de início da tarefa

7. Nesta etapa do assistente, defina outras configurações de agendamento de tarefas:

- Na seção **Agendamento da tarefa**, verifique ou reconfigure o agendamento selecionado anteriormente e defina o intervalo de tempo, os dias do mês ou da semana, defina a condição de surto de vírus ou a conclusão de outra tarefa como um acionador para iniciar a tarefa. Uma hora de início também pode ser especificada nesta seção se uma programação aplicável for selecionada.
- Na seção **Configurações adicionais**, especifique as seguintes configurações:
  - **Executar tarefas ignoradas**

    Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

    Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

    Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

    Por padrão, esta opção está ativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

  Por padrão, esta opção está ativada.

- **Usar atraso aleatório automaticamente para início de tarefa em um intervalo de**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

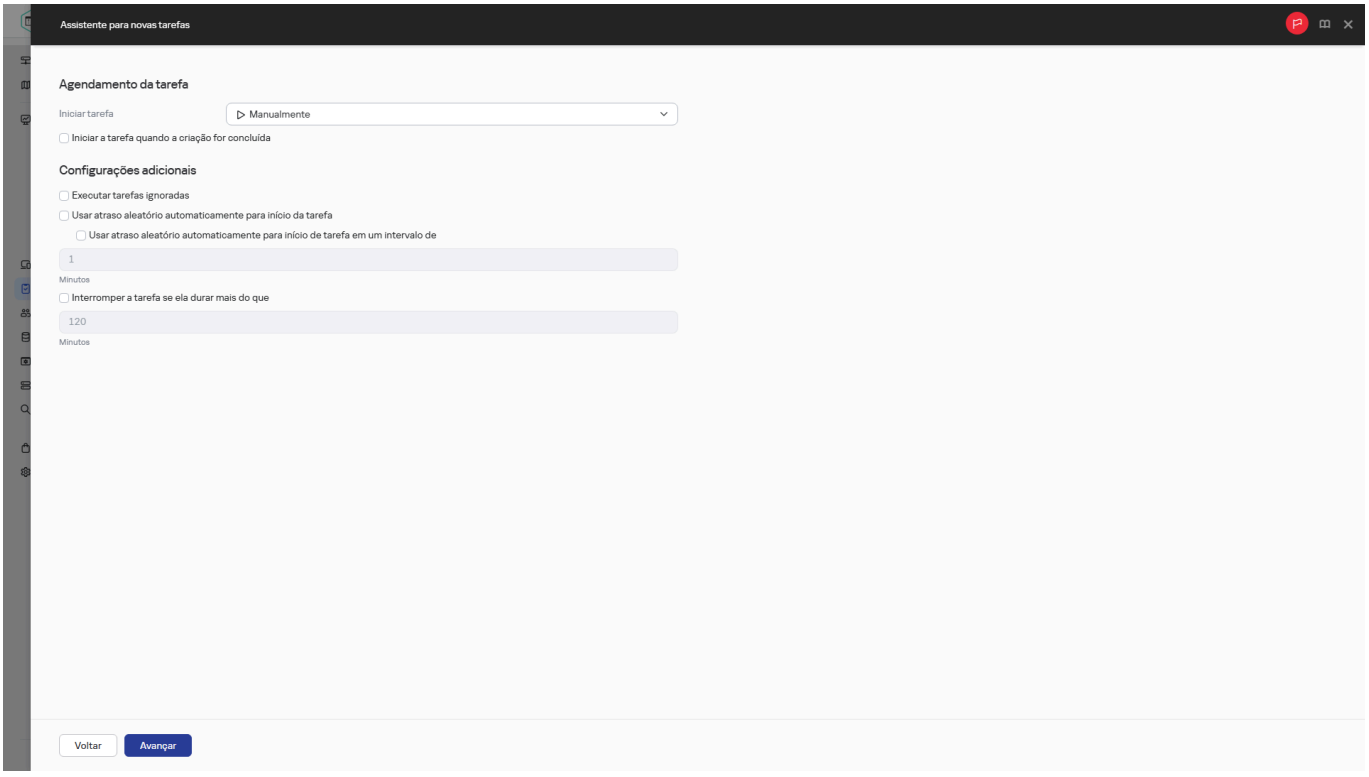
  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

- **Interromper a tarefa se ela durar mais do que**

  Após o final do período especificado, a tarefa é interrompida automaticamente, quer tenha sido concluída ou não.

  Ative esta opção se você quiser interromper (ou parar) tarefas que levam muito tempo para serem executadas.

  Por padrão, esta opção está desativada. O tempo predefinido de execução da tarefa é de 120 minutos.

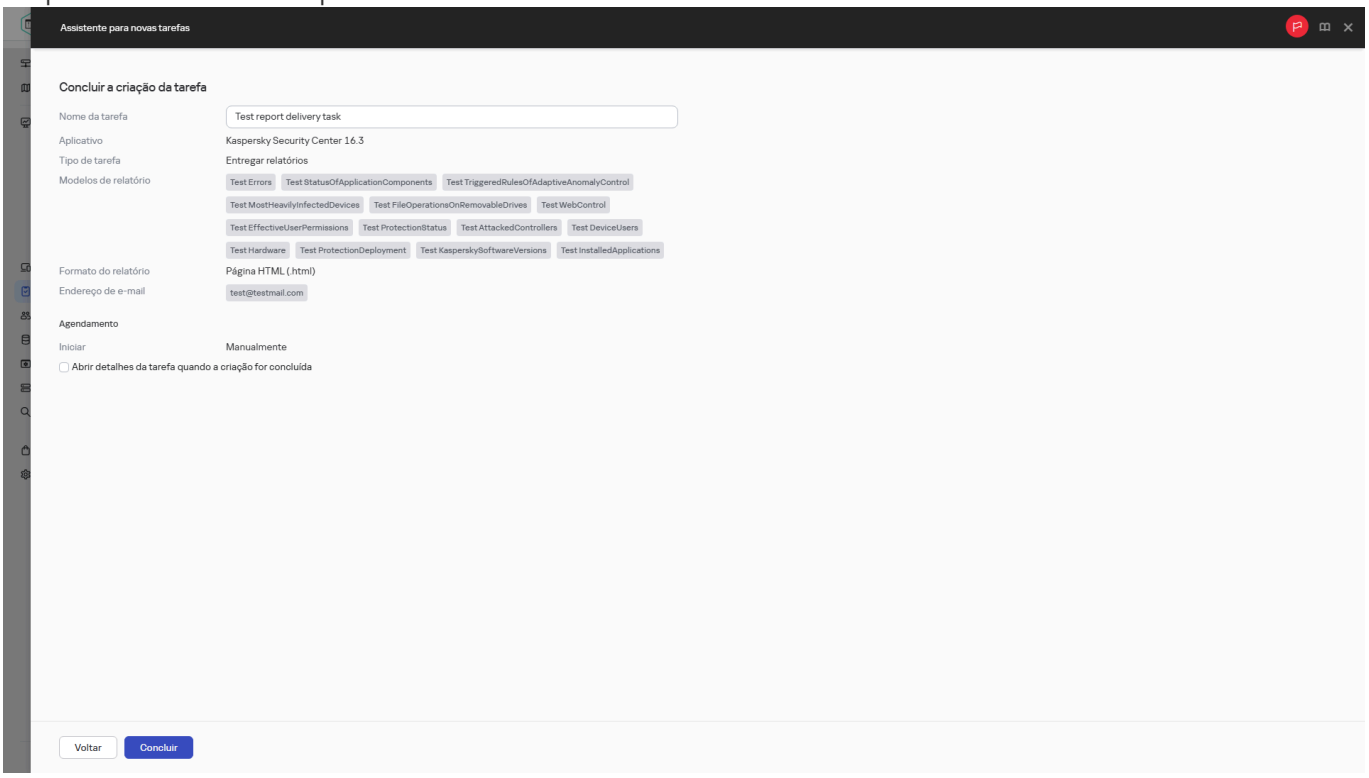


Especificação das configurações de programação de tarefas

8. Na etapa **Selecionar uma conta para executar a tarefa** do assistente, especifique as credenciais da conta de usuário usada para executar a tarefa.

9. Se você deseja modificar outras configurações da tarefa após a criação da tarefa, na etapa **Concluir a criação da tarefa** do assistente, habilite a opção **Abrir detalhes da tarefa quando a criação for concluída**. Por padrão, esta opção está ativada.

10. Clique no botão **Concluir** para criar a tarefa e fechar o assistente.



Finalização da criação da tarefa

A tarefa de entrega de relatório é criada. Se a opção **Abrir detalhes da tarefa quando a criação for concluída** estiver ativada, a janela de configurações da tarefa será aberta.

Excluir os modelos de relatório

Para excluir um ou vários modelos de relatório:

1. No menu principal, vá para **Monitoramento** → **Relatórios**.

2. Marque as caixas de seleção ao lado dos modelos de relatório que deseja excluir.

3. Em seguida, clique no botão **Excluir**.

4. Na janela que se abre, clique em **OK** para confirmar a sua seleção.

Os modelos de relatório selecionados são excluídos. Se esses modelos de relatório tiverem sido incluídos nas tarefas de entrega de relatório, eles também serão removidos das tarefas.

Centro de fortalecimento da segurança

O Centro de fortalecimento da segurança exibe informações atualizadas sobre a proteção do Servidor de Administração e dos pontos de distribuição. Essas informações são apresentadas como indicadores do nível de proteção. Esses indicadores permitem acompanhar a implementação do Guia de proteção e resolver prontamente os problemas de segurança em sua infraestrutura à medida que surgirem.

O indicador pode estar em um dos seguintes status:

- Proteção configurada.
- Proteção parcialmente configurada.
- Proteção não configurada.

Como exibir informações detalhadas sobre o nível de proteção

O status geral do indicador é formado pelo estado dos parâmetros de proteção.

*Para abrir o **Central de fortalecimento da segurança**:*

1. No menu principal, acesse a seção **Monitoramento** → **Painel**.
2. Clique no status da proteção no canto superior direito.

   Na janela **Central de fortalecimento da segurança** que é exibida, os parâmetros são agrupados por objetos protegidos: Servidor de Administração e pontos de distribuição.

Cada parâmetro de proteção é exibido em um dos estados, dependendo dos direitos de acesso:

- ✅ se não houver problemas a resolver ou se você não tiver os direitos de acesso necessários.
- ⚠ ou ❌ se houver problemas a serem resolvidos.

Os seguintes parâmetros são exibidos somente para o Servidor de Administração:

- Backup configurado
- Manutenção do Servidor de Administração configurada
- Criptografia TLS ativada

Os seguintes parâmetros são exibidos para o Servidor de Administração e os pontos de distribuição:

- Aplicativo de segurança instalado
- Política de aplicativo de segurança aplicada
- Atualizações do banco de dados de antivírus configuradas

- Todos os dispositivos são gerenciados

  Essa configuração também é exibida para dispositivos que não são pontos de distribuição nem dispositivos do Servidor de Administração.

Considerações especiais para o Servidor de Administração:

- Todos os parâmetros de proteção são calculados somente para o servidor de administração físico e não são aplicados a servidores virtuais.

  Se você tiver uma estrutura hierárquica de vários Servidores de Administração, o indicador de nível de proteção será calculado para cada servidor físico separadamente.

- Os parâmetros de **Aplicativo de segurança instalado**, **Política de aplicativo de segurança aplicada** e **Atualizações do banco de dados de antivírus configuradas** são calculados para um dispositivo com o Servidor de Administração instalado.

- Ao implementar um cluster de failover do Kaspersky Security Center Linux, os parâmetros de **Aplicativo de segurança instalado**, **Política de aplicativo de segurança aplicada, Atualizações do banco de dados de antivírus configuradas** e **Todos os dispositivos são gerenciados** são avaliados para cada nó. O nó é considerado no cálculo do status do indicador somente depois de se tornar ativo.

Como o status do indicador é calculado

A tabela abaixo descreve como o status do indicador é avaliado.

Status do indicador	Condição
Proteção configurada.	Todos os parâmetros de proteção estão em estado .
Proteção parcialmente configurada.	O parâmetro **Atualizações do banco de dados de antivírus configuradas** está no estado , enquanto todos os outros parâmetros estão no estado .
Proteção não configurada.	Se pelo menos um dos seguintes parâmetros de proteção estiver em estado .

Aplicativo de segurança instalado

Os aplicativos de segurança permitem proteger seus dispositivos contra vários tipos de ameaças, incluindo ataques de rede, phishing e golpes.

O parâmetro é exibido no estado ✅ se uma das condições for atendida:

- Você não tem direitos de acesso aos dispositivos.
- Você tem a permissão de **Ler** na área funcional **Recursos gerais** → **Funcionalidade básica**, enquanto o Agente de Rede e um aplicativo de segurança estiverem instalados nos dispositivos.

  A condição deve ser atendida em todos os dispositivos disponíveis para você com base nos seus direitos de acesso, exceto os dispositivos com um aplicativo instalado que não exija proteção antivírus (por exemplo, um sistema operacional seguro), os dispositivos sem o Agente de Rede instalado cujas informações sobre o dispositivo tenham aparecido no Servidor de Administração há menos de 24 horas e os dispositivos offline que se conectaram ao Servidor de Administração pela última vez há 7 dias ou mais.

O parâmetro é exibido no estado ❌ se pelo menos uma das condições abaixo for atendida.

Você deve clicar no botão **Exibir dispositivos** e executar as ações descritas na tabela para os dispositivos exibidos.

Condição	Solução
O Agente de Rede não está instalado no dispositivo	Instale o Agente de Rede. Para o dispositivo do Servidor de Administração, a forma mais simples de instalação do Agente de Rede é usar um pacote de instalação autônomo.
O dispositivo está incluído no grupo **Dispositivos não atribuídos**	Mova o dispositivo para o grupo Dispositivos gerenciados ou seu subgrupo
Nenhum aplicativo de segurança foi encontrado ou a proteção em tempo real não está em execução para o aplicativo de segurança instalado	Instale um aplicativo de segurança. O aplicativo transmitirá dados sobre o estado de proteção ao Servidor de Administração. Você pode visualizar o status de proteção de um dispositivo nas configurações do dispositivo: seção **Geral** → **Status do dispositivo**. No dispositivo do Servidor de Administração, você deve instalar o Kaspersky Endpoint Security for Linux.

Política aplicada

Uma política é um conjunto de configurações do aplicativo de segurança que são aplicadas a um grupo de administração e seus subgrupos.

O parâmetro é exibido no estado ✅ se uma das condições for atendida:

- Você não tem direitos de acesso aos dispositivos.
- Você tem a permissão de **Ler** na área funcional **Recursos gerais → Funcionalidade básica**, enquanto um aplicativo de segurança estiver instalado nos seus dispositivos e uma política ativa desse aplicativo de segurança for aplicada aos dispositivos.

> A condição deve ser atendida em todos os dispositivos disponíveis para você com base nos seus direitos de acesso, exceto os dispositivos com um aplicativo instalado que não exija proteção antivírus (por exemplo, um sistema operacional seguro), os dispositivos sem o Agente de Rede instalado cujas informações sobre o dispositivo tenham aparecido no Servidor de Administração há menos de 24 horas e os dispositivos offline que se conectaram ao Servidor de Administração pela última vez há 7 dias ou mais.

O parâmetro é exibido no estado ❌ se pelo menos uma das condições abaixo for atendida.

Você deve clicar no botão **Exibir dispositivos** e executar as ações descritas na tabela para os dispositivos exibidos.

Condição	Solução
Um aplicativo de segurança não está instalado no dispositivo.	Verifique se o dispositivo está ausente na seleção do parâmetro proteção do **Aplicativo de segurança instalado**.
Uma política não é aplicada ao dispositivo.	Verifique se a política está criada para o grupo de administração ao qual o dispositivo pertence. Caso contrário, crie e ative a política. Em caso afirmativo, certifique-se de que: • A política criada está ativa. Caso contrário, ative a política. • O status de distribuição da política é **Aplicado com sucesso**. Se o status for **Aplicado com erro**, o problema deve ser corrigido no aplicativo de segurança.

Atualização de banco de dados do antivírus configurada

Como os bancos de dados de antivírus protegem seus dispositivos contra ameaças, você precisa atualizá-los regularmente e no devido tempo.

O parâmetro é exibido no estado ✅ se uma das condições for atendida:

- Você não tem direitos de acesso aos dispositivos.
- Você tem a permissão de Ler na área funcional Recursos gerais → Funcionalidade básica, e os bancos de dados do antivírus são atualizados nos dispositivos.

> A condição deve ser atendida em todos os dispositivos disponíveis para você com base nos seus direitos de acesso, exceto os dispositivos com um aplicativo instalado que não exija proteção antivírus (por exemplo, um sistema operacional seguro), os dispositivos sem o Agente de Rede instalado cujas informações sobre o dispositivo tenham aparecido no Servidor de Administração há menos de 24 horas e os dispositivos offline que se conectaram ao Servidor de Administração pela última vez há 7 dias ou mais.

O parâmetro é exibido em estado ⚠ se os bancos de dados de antivírus tiverem sido atualizados pela última vez em um dispositivo há mais de três dias.

O parâmetro é exibido em estado ✖ se os bancos de dados de antivírus tiverem sido atualizados pela última vez em um dispositivo há mais de sete dias.

Para resolver o problema:

1. Clique no botão Exibir dispositivos ao lado do parâmetro.
2. Para os dispositivos exibidos, execute as seguintes ações:
   a. Verifique se essa conexão entre o Agente de Rede e o Servidor de Administração está estabelecida.

      Caso contrário, consulte os seguintes artigos:

      Solução de problemas ao atualizar os bancos de dados de antivírus do Kaspersky Endpoint Security for Linux

      Problemas ao atualizar os bancos de dados de antivírus pelo repositório do Kaspersky Security Center

   b. Certifique-se de que o aplicativo da Kaspersky cujos bancos de dados de antivírus você está verificando não esteja interrompido.

      Se o aplicativo estiver interrompido, inicie-o.

   c. No dispositivo, visualize os erros que ocorreram após a atualização.

Backup configurado

Para recomendações sobre o backup de dados do Servidor de Administração, consulte Cópia de backup e restauração de dados do Servidor de Administração.

O parâmetro é exibido no estado ✔ se uma das condições for atendida:

- Você não tem direitos de acesso para trabalhar com a tarefa de backup de dados do Servidor de Administração.
- Você tem permissões de **Ler, Gravar** e **Executar** na área funcional **Recursos gerais → Operações no Servidor de administração** e o backup é configurado e executado regularmente.

O parâmetro é exibido no estado ✖ se pelo menos uma das condições abaixo for atendida.

Condição	Solução
A tarefa de backup de dados do Servidor de Administração não foi criada.	Crie a tarefa.
As configurações de agendamento necessárias não estão definidas para a tarefa de backup de dados do Servidor de Administração.	Na tarefa de manutenção do Servidor de Administração, especifique as configurações para **Iniciar tarefa**, que não sejam **No surto de vírus** e **Manualmente**.

Manutenção do Servidor de Administração configurada

A manutenção do Servidor de Administração permite liberar espaço na pasta do Servidor de Administração, bem como minimizar o tamanho do banco de dados. Isso ajuda a acelerar o processamento da solicitação e aumenta a estabilidade geral do sistema.

O parâmetro é exibido no estado ✅ se uma das condições for atendida:

- Você não tem direitos de acesso para trabalhar com a tarefa de manutenção do Servidor de Administração.
- Você tem permissões de **Ler, Gravar** e **Executar** na área funcional **Recursos gerais → Operações no Servidor de administração**, enquanto a manutenção do Servidor de Administração é configurada e executada regularmente.

  > Os direitos devem ser definidos no nível do Servidor de Administração.

O parâmetro é exibido no estado ❌ se pelo menos uma das condições abaixo for atendida.

Condição	Solução
A tarefa de manutenção do Servidor de Administração não foi criada.	Crie a tarefa.
As configurações de agendamento necessárias não estão definidas para a tarefa de manutenção do Servidor de Administração.	Na tarefa de manutenção do Servidor de Administração, especifique as configurações para **Iniciar tarefa**, que não sejam **No surto de vírus** e **Manualmente**.

Criptografia TLS ativada

Você deve garantir que apenas as versões 1.2 e 1.3 do protocolo TLS sejam permitidas. Permitir versões anteriores resulta em sérios riscos de segurança de dados e torna os sistemas vulneráveis a ataques.

O parâmetro é exibido em estado ✅ se somente as versões 1.2 e 1.3 do protocolo TLS forem permitidas.

O parâmetro é exibido em estado ❌ se as versões do TLS desatualizadas, anteriores a 1.2, forem permitidas.

Para resolver o problema, você deve definir o sinalizador `SrvUseStrictSslSettings` para o valor `4` ou `5`.

Todos os dispositivos são gerenciados

Você pode usar esse parâmetro para identificar dispositivos que podem estar fora de controle.

Este parâmetro é exibido com o status quando uma das seguintes condições é atendida:

- Você não tem direitos de acesso aos dispositivos.
- Você tem a permissão **Ler** na área funcional **Recursos gerais → Funcionalidade básica**, os dispositivos estão no grupo **Dispositivos gerenciados** e uma conexão foi estabelecida entre o Servidor de Administração e o Agente de Rede nos dispositivos.

  Esta condição deve ser atendida em todos os dispositivos aos quais você tem acesso, exceto: dispositivos cujas informações apareceram no Servidor de Administração há menos de 24 horas e dispositivos que se conectaram ao Servidor de Administração pela última vez há sete ou mais dias.

Este parâmetro é exibido com o status se houver pelo menos um dispositivo que atenda a uma das condições abaixo.

Você deve clicar no botão **Exibir dispositivos** e executar as ações descritas na tabela para os dispositivos exibidos.

Condição	Solução
O Agente de Rede não está instalado em um dispositivo incluído no grupo **Dispositivos gerenciados**.	Instale o Agente de Rede.
O Servidor de Administração detecta um dispositivo gerenciado durante uma verificação de rede, mas esse dispositivo não se conectou ao Servidor de Administração por três intervalos de sincronização consecutivos.	Faça o seguinte: 1. Execute o utilitário klnagchk no dispositivo com problemas para verificar se o serviço está em execução e se o Agente de Rede consegue se conectar ao Servidor de Administração. 2. Verifique a acessibilidade de rede do Servidor de Administração e dos gateways de conexão. 3. Restabeleça a conexão do dispositivo com o Servidor de Administração usando o utilitário klmover. 4. Remova os dispositivos obsoletos dos grupos de administração. Se você tiver uma infraestrutura não padrão, siga estas etapas para os dispositivos com problemas: a. Verifique se o dispositivo é gerenciado pelo Servidor de Administração. b. Mova esse dispositivo para um grupo de administração separado. c. Nesse grupo de administração, atribua ao evento **O dispositivo está sem gerenciamento** qualquer status diferente de *Crítico*.

Eventos e seleções de eventos

Esta seção fornece informações sobre eventos e seleções de eventos, sobre os tipos de eventos que ocorrem nos componentes do Kaspersky Security Center Linux e sobre como gerenciar o bloqueio de eventos frequentes.

Sobre eventos no Kaspersky Security Center Linux

O Kaspersky Security Center Linux permite que o usuário receba informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nos dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração.

Eventos por tipo

No Kaspersky Security Center Linux, há os seguintes tipos de eventos:

- Eventos gerais. Esses eventos ocorrem em todos os aplicativos Kaspersky gerenciados. Um exemplo de um evento geral é um Surto de vírus. Eventos gerais têm sintaxe e semântica estritamente definidas. Eventos gerais são usados, por exemplo, em relatórios e painéis.
- Eventos gerenciados específicos de aplicativos Kaspersky. Cada aplicativo Kaspersky gerenciado tem o seu próprio conjunto de eventos.

Eventos por origem

É possível ver a lista completa dos eventos que podem ser gerados por um aplicativo na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar a lista de eventos nas propriedades do Servidor de Administração.

Os eventos podem ser gerados pelos seguintes aplicativos:

- Componentes do Kaspersky Security Center Linux:
  - Servidor de Administração
  - Agente de Rede
- Aplicativos gerenciados pela Kaspersky

  Para obter detalhes sobre os eventos gerados pelos aplicativos gerenciados pela Kaspersky, consulte a documentação do aplicativo correspondente.

Eventos por nível de importância

Cada evento tem o seu próprio nível de importância. Dependendo das condições da sua ocorrência, a um evento pode ser atribuídos diversos níveis de importância. Há quatro níveis de importância de eventos:

- Um *evento crítico* é um evento que indica a ocorrência de um problema crítico que pode levar à perda de dados, um funcionamento operacional ruim ou um erro crítico.
- Uma *falha funcional* é um evento que indica a ocorrência de um problema sério, erro ou funcionamento incorreto durante a operação do aplicativo ou ao executar um procedimento.
- Um *aviso* é um evento que não necessariamente é sério, mas no entanto indica um problema potencial no futuro. A maior parte de eventos são indicados como avisos se o aplicativo puder ser restaurado sem perda dos dados ou capacidades funcionais após a ocorrência de tais eventos.
- Um evento *de informação* é um evento que ocorre para fins de informar sobre conclusão bem sucedida de uma operação, funcionamento apropriado do aplicativo ou conclusão de um procedimento.

Cada evento tem um prazo de armazenamento definido, durante o qual você pode exibi-lo ou modificá-lo no Kaspersky Security Center Linux. Alguns eventos não são salvos no banco de dados do Servidor de Administração por padrão porque o seu prazo de armazenamento definido é zero. Somente os eventos que serão armazenados no banco de dados do Servidor de Administração por ao menos um dia podem ser exportados aos sistemas externos.

Eventos dos componentes do Kaspersky Security Center Linux

Cada componente do Kaspersky Security Center Linux tem o seu próprio conjunto de tipos de evento. Esta seção lista os tipos de eventos que ocorrem no Servidor de Administração e no Agente de Rede. Os tipos de eventos que ocorrem nos aplicativos Kaspersky não são listados nesta seção.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Estrutura de dados da descrição do tipo de evento

Para cada tipo de evento, seu nome de exibição, o identificador (ID), o código alfabético, a descrição e o termo de armazenamento padrão são fornecidos.

- **Nome de exibição do tipo de evento**. Este texto é exibido no Kaspersky Security Center Linux quando você configura eventos e quando eles ocorrem.
- **ID do tipo de evento**. Este código numérico é usado quando você processa eventos usando ferramentas de terceiros para a análise de eventos.
- **Tipo de evento** (código alfabético). Este código é usado quando você percorre e processa eventos usando vistas públicas fornecidas no banco de dados do Kaspersky Security Center Linux e quando os eventos são exportados para um sistema SIEM.

- **Descrição**. Este texto contém as situações nas quais um evento ocorre e o que você pode fazer nesses casos.
- **Prazo de armazenamento padrão**. É o número de dias durante os quais o evento é armazenado no banco de dados do Servidor de Administração e é exibido na lista de eventos no Servidor de Administração. Após o término desse período, o evento é excluído. Se o valor do prazo de armazenamento do evento for 0, os eventos são detectados, mas não são exibidos na lista de eventos no Servidor de Administração. Se você configurou para salvar os eventos no log de eventos do sistema operacional, poderá encontrá-los nesse local.

  Você pode alterar o prazo de armazenamento para eventos: Definir o prazo de armazenamento para um evento.

Eventos do Servidor de Administração

Esta seção contém informações sobre os eventos relativos ao Servidor de Administração.

Eventos críticos do Servidor de Administração

A tabela abaixo exibe os eventos do Servidor de Administração com a gravidade **Crítico**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos críticos do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O certificado do Servidor de Administração para dispositivos móveis expirou	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	Eventos deste tipo ocorrem quando os certificados do Servidor de Administração para dispositivos móveis e dispositivos com UEFI expiram. Você precisa atualizar o certificado expirado.	180 dias
Auditoria: falha na exportação para SIEM	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Eventos desse tipo ocorrem quando a exportação de eventos para o sistema SIEM falha devido a um erro de conexão com o sistema SIEM.	180 dias
O dispositivo está sem gerenciamento	4111	KLSRV_HOST_OUT_CONTROL	Eventos deste tipo ocorrem se um dispositivo gerenciado está visível na rede, mas não se conectou ao Servidor de Administração por um período específico. Descubra o que impede o funcionamento apropriado do Agente de Rede no dispositivo. As causas possíveis incluem problemas de rede e a remoção do Agente de Rede do dispositivo.	180 dias
O status do dispositivo é Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Eventos deste tipo ocorrem quando um dispositivo gerenciado é atribuído com o status *Crítico*. Você pode configurar as condições sob as quais o status do dispositivo é alterado para *Crítico*.	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
A licença expira em breve	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Eventos desse tipo ocorrem quando a data de expiração da licença comercial está se aproximando. Uma vez ao dia, o Kaspersky Security Center Linux verifica se a data de expiração da licença está próxima. Eventos deste tipo são publicados 30 dias, 15 dias, 5 dias e 1 dia antes da data de expiração da licença. Este número de dias não pode ser alterado. Se o Servidor de Administração é desativado no dia especificado antes da data de expiração da licença, o evento não será publicado até o próximo dia. Quando a licença comercial expirar, o Kaspersky Security Center Linux fornecerá apenas a funcionalidade básica. Você pode responder ao evento nas seguintes maneiras: • Certifique-se de que uma chave reserva de licença seja adicionada ao Servidor de Administração. • Caso use uma assinatura, certifique-se de renová-la. Uma assinatura ilimitada será automaticamente renovada, caso tenha sido pré-paga ao provedor de serviços na data devida.	180 dias
O limite da licença foi excedido	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Uma vez por dia o Kaspersky Security Center Linux verifica se um limite de licenciamento foi excedido. Eventos desse tipo ocorrem quando o Servidor de Administração detecta que alguns limites da licença foram excedidos pelos aplicativos da Kaspersky instalados nos dispositivos clientes e se o número de unidades de licenciamento atualmente usadas e abrangidas por uma única licença excede 110% do número total de unidades abrangidas pela licença. Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. • Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração). O Kaspersky Security Center Linux determina as regras para gerar eventos quando um limite de licenciamento é excedido.	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Modo de funcionalidade limitada	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Eventos desse tipo ocorrem quando o Kaspersky Security Center Linux começa a operar com a funcionalidade básica, sem o Gerenciamento de patches e vulnerabilidades e sem os recursos de Gerenciamento de Dispositivos Móveis. A seguir se encontram as causas de, e as respostas apropriadas, do evento: • Termo da licença expirado. Forneça uma licença para usar o modo de funcionalidade completa do Kaspersky Security Center Linux (adicione um código de ativação ou um arquivo de chave válido no Servidor de Administração). • O Servidor de Administração gerencia mais dispositivos do que o especificado pelo limite da licença. Mover dispositivos dos grupos de administração de um Servidor de Administração para aqueles de outro Servidor (se o limite da licença do outro Servidor de Administração o permitir).	180 dias
O certificado do MDM expirou	4132	KLSRV_CERTIFICATE_EXPIRED	Eventos desse tipo ocorrem quando o certificado de cliente de dispositivos móveis expira.	180 dias
O arquivo de chave foi adicionado à lista de bloqueio	4124	KLSRV_LICENSE_BLACKLISTED	Eventos deste tipo ocorrem quando a Kaspersky tiver adicionado o código de ativação ou arquivo de chave usado por você à lista de proibição. Entre em contato com o Suporte Técnico para obter mais detalhes.	180 dias
As atualizações dos módulos do aplicativo da Kaspersky foram revogadas	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Eventos deste tipo ocorrem se atualizações tiverem sido revogadas por especialistas da Kaspersky, por exemplo, para substituí-las por versões mais recentes. Para essas atualizações, o status é *Revogado*. O evento diz respeito aos patches do Kaspersky Security Center Linux e não aos módulos de aplicativos gerenciados da Kaspersky. O evento fornece o motivo da não instalação das atualizações racionais.	180 dias
Surto de vírus	• 26 (para Proteção Contra Ameaças ao Arquivo) • 27 (para Proteção Contra Ameaças ao Correio) • 28 (para Firewall)	GNRL_EV_VIRUS_OUTBREAK	Eventos desse tipo ocorrem quando a quantidade de objetos maliciosos detectada em diversos dispositivos gerenciados exceder o limite dentro de um curto período. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	

Eventos de falha funcional do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração com o nível de importância **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Falha ao copiar as atualizações para a pasta especificada	4123	KLSRV_UPD_REPL_FAIL	Eventos deste tipo ocorrem quando as atualizações do software são copiadas para uma pasta adicional compartilhada. Você pode responder ao evento nas seguintes maneiras: • Verifique se a conta de usuário que está sendo empregada para obter o acesso às pastas tem permissão de gravação. • Verifique se um nome de usuário e/ou senha para a(s) pasta(s) foi/está alterado. • Verifique a conexão com a internet, já que isso pode ser a causa do evento. Siga as instruções para atualizar bancos de dados e módulos do software.	180 dias
Falha ao amostrar o segmento da nuvem	4143	KLSRV_KLCLOUD_SCAN_ERROR	Os eventos desse tipo ocorrem quando o Servidor de Administração falha na sondagem de um segmento de rede em um ambiente em nuvem. Leia os detalhes na descrição do evento e responda de acordo.	Não armazenado
O limite de instalações foi excedido para um dos grupos de aplicativos licenciados	4126	KLSRV_INVLICPROD_EXCEDED	O Servidor de Administração gera periodicamente eventos deste tipo (a cada hora). Eventos deste tipo ocorrem se no Kaspersky Security Center Linux você gerencia chaves de licença de aplicativos de terceiros e o número de instalações excedeu o limite definido pela chave de licença do aplicativo de terceiro. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua o aplicativo de terceiro dos dispositivos nos quais o aplicativo não está em uso. • Use uma licença de terceiro para mais dispositivos. Você pode gerenciar chaves de licença de aplicativos de terceiros usando a funcionalidade de grupos de aplicativos licenciados. Um grupo de aplicativos licenciados inclui aplicativos de terceiros que atendem os critérios definidos por você.	180 dias
Nenhum espaço livre em disco	4107	KLSRV_DISK_FULL	Eventos deste tipo ocorrem quando o disco rígido do dispositivo onde o Servidor de Administração está instalado fica sem espaço. Libere espaço em disco no dispositivo.	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Espaço insuficiente no banco de dados do Servidor de Administração	4110	KLSRV_DATABASE_FULL	Eventos deste tipo ocorrem quando não houver nenhum espaço livre no banco de dados do Servidor de Administração. O Servidor de Administração não funciona quando seu banco de dados alcançou sua capacidade e quando o registro no banco de dados não for possível. A seguir estão as causas deste evento, dependendo do DBMS que você usa, e as respostas apropriadas ao evento: • Limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração. • No banco de dados do Servidor de Administração, há muitos eventos enviados pelo componente Controle de Aplicativos. É possível alterar as configurações da política do Kaspersky Endpoint Security relacionadas ao armazenamento de eventos do Controle de Aplicativos no banco de dados do Servidor de Administração. Revise as informações na seleção do DBMS.	180 dias
Erro do tempo de execução	4125	KLSRV_RUNTIME_ERROR	Eventos deste tipo ocorrem devido a problemas desconhecidos. Mais frequentemente estes são problemas de DBMS, problemas de rede e outros problemas de software e hardware. Os detalhes do evento podem ser encontrados na descrição do evento.	180 dias
A pasta compartilhada não está disponível	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Eventos deste tipo ocorrem se a pasta compartilhada do Servidor de Administração não estiver disponível. Você pode responder ao evento nas seguintes maneiras: • Verifique se o Servidor de Administração (onde a pasta compartilhada está localizada) está ativado e disponível. • Verifique se um nome de usuário e/ou senha para a pasta foi/está alterado. • Verifique a conexão à rede.	180 dias
O banco de dados do Servidor de Administração está indisponível	4109	KLSRV_DATABASE_UNAVAILABLE	Eventos deste tipo ocorrem se o banco de dados do Servidor de Administração s tornar indisponível. Você pode responder ao evento nas seguintes maneiras: • Verifique se o servidor remoto que tem o DBMS instalado está disponível. • Visualize os registros do DBMS para descobrir o motivo da indisponibilidade de banco de dados do Servidor de Administração.	180 dias

Eventos de aviso do Servidor de Administração

A tabela abaixo demonstra os eventos do Agente de Rede que têm o nível de gravidade **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O certificado do Servidor de Administração para dispositivos móveis está prestes a expirar	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	Eventos deste tipo ocorrem quando o certificado do Servidor de Administração para dispositivos móveis e dispositivos com UEFI expira. Você precisa atualizar o certificado expirado.	90 dias
O certificado de APNs expira em breve	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Eventos deste tipo ocorrem quando faltam menos de 14 dias para a expiração do certificado de APNs. Quando o certificado de APNs expirar, você precisará renová-lo manualmente e instalá-lo em um servidor de MDM do iOS. Recomendamos que você agende a renovação do certificado de APNs antes da data de expiração.	Não armazenado
O certificado de APNs expirou	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Eventos deste tipo ocorrem quando um certificado de APNs expira. Você precisa renovar manualmente o certificado de APNs e instalá-lo em um servidor de MDM do iOS.	Não armazenado
Auditoria: teste de conexão malsucedido com o servidor SIEM	5120	KLAUD_EV_SIEM_TEST_FAILED	Eventos desse tipo ocorrem quando um teste de conexão automática com o servidor SIEM falha.	90 dias
O certificado foi removido	4134	KLSRV_CERTIFICATE_REMOVED	Eventos deste tipo ocorrem quando um administrador remove qualquer tipo de certificado (Geral, Correio, VPN) para Gerenciamento de Dispositivos Móveis. Depois de remover um certificado, os dispositivos móveis conectados por meio deste certificado não conseguirão se conectar ao Servidor de Administração. Este evento pode ser útil ao investigar falhas associadas ao gerenciamento de dispositivos móveis.	90 dias
O certificado foi solicitado	4133	KLSRV_CERTIFICATE_REQUESTED	Eventos deste tipo ocorrem quando um certificado para Gerenciamento de Dispositivos Móveis não é reemitido automaticamente. Seguem abaixo as possíveis causas e as respostas apropriadas para o evento: • A reemissão automática foi iniciada para um certificado para o qual a opção **Reemitir o certificado automaticamente se possível** está desativada. Isso pode ser devido a um erro ocorrido durante a criação do certificado. Pode ser necessária a reemissão manual do certificado. • Se você usar uma integração com uma infraestrutura de chave pública, a causa pode ser a ausência de um atributo SAM-Account-Name na conta usada para integração com PKI e para emissão do certificado. Revise as propriedades da conta.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Conflito de nomes de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Eventos desse tipo ocorrem quando o Servidor de Administração considera dois ou mais dispositivos gerenciados como um único dispositivo. Na maioria das vezes, isso acontece quando um disco rígido clonado foi usado para implantação de software em dispositivos gerenciados, sem alterar o Agente de Rede para o modo de clonagem de disco dedicado em um dispositivo de referência. Para evitar este problema, altere o Agente de Rede para o modo de clonagem de disco em um dispositivo de referência antes de clonar o disco rígido desse dispositivo.	90 dias
A conexão com o Servidor de Administração principal foi interrompida	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Eventos deste tipo ocorrem quando uma conexão com o Servidor de Administração primário é interrompida. Leia o log do sistema operacional no dispositivo onde o Servidor de Administração primário estiver instalado e responda adequadamente.	90 dias
A conexão com o Servidor de Administração secundário foi interrompida	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Eventos deste tipo ocorrem quando uma conexão com o Servidor de Administração secundário é interrompida. Leia o log do sistema operacional no dispositivo onde o Servidor de Administração secundário estiver instalado e responda adequadamente.	90 dias
O dispositivo permaneceu inativo na rede por muito tempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Eventos desse tipo ocorrem quando um dispositivo gerenciado fica em inatividade por algum tempo. Na maioria das vezes, isso acontece quando um dispositivo gerenciado é desativado. Você pode responder ao evento nas seguintes maneiras: • Remova manualmente o dispositivo da lista de dispositivos gerenciados. Especifique o intervalo de tempo após o qual o evento **O dispositivo permaneceu inativo na rede por muito tempo** é criado usando o Kaspersky Security Center Web Console. • Especifique o intervalo de tempo após o qual o dispositivo é removido automaticamente do grupo usando o Kaspersky Security Center Web Console.	90 dias
O status do dispositivo é Advertência	4114	KLSRV_HOST_STATUS_WARNING	Eventos deste tipo ocorrem quando à um dispositivo gerenciado for atribuído o status de *Aviso*. Você pode configurar as condições sob as quais o status do dispositivo é alterado para *Aviso*.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Falha ao baixar o arquivo para o dispositivo	4165	KLSRV_FILE_DOWNLOAD_FAILED	Eventos desse tipo ocorrem nos seguintes casos: • Você tenta baixar um arquivo para o contêiner corporativo, mas um contêiner corporativo não foi criado. • Não há espaço suficiente no dispositivo. • Houve falha ao baixar as informações sobre o arquivo presentes no servidor. • Houve falha ao baixar o conteúdo do arquivo presente no servidor. • A pasta não pôde ser criada no dispositivo. • A permissão de acesso ao arquivo está ausente no dispositivo pessoal. • A permissão de acesso ao arquivo está ausente no contêiner corporativo.	90 dias
Falha ao enviar a mensagem FCM para o servidor FCM	4140	KLSRV_GCM_GENERAL_ERROR	Eventos deste tipo ocorrem devido a erros inesperados no Servidor de Administração ao trabalhar com o protocolo HTTP do Google Firebase Cloud Messaging. Leia os detalhes na descrição do evento e responda de acordo. Se você não conseguir solucionar o problema sozinho, é recomendável entrar em contato com o Suporte Técnico da Kaspersky.	90 dias
Falha ao enviar a mensagem FCM para o dispositivo móvel	4138	KLSRV_GCM_DEVICE_ERROR	Eventos desse tipo ocorrem quando o Gerenciamento de Dispositivos Móveis está configurado para usar o Google Firebase Cloud Messaging (FCM) para se conectar a dispositivos móveis gerenciados com um sistema operacional Android e o Servidor FCM não consegue processar algumas das solicitações recebidas do Servidor de Administração. Isso significa que alguns dos dispositivos móveis gerenciados não receberão uma notificação push. Leia o código HTTP nos detalhes da descrição do evento e responda de acordo. Para obter mais informações sobre os códigos HTTP recebidos do Servidor de FCM e erros relacionados, consulte a documentação do serviço Google Firebase (em especial, o capítulo "Códigos de resposta de erro de mensagens downstream").	90 dias
Eventos frequentes detectados		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Eventos desse tipo ocorrem quando o Servidor de Administração detecta um evento frequente em um dispositivo gerenciado. Consulte a seguinte seção para obter detalhes: Bloqueio de eventos frequentes.	90 dias
O disco rígido está quase cheio	4105	KLSRV_NO_SPACE_ON_VOLUMES	Eventos deste tipo ocorrem quando o disco rígido do dispositivo onde o Servidor de Administração está instalado fica praticamente sem espaço livre. Libere espaço em disco no dispositivo.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Ocorreu um erro de HTTP ao enviar a mensagem FCM para o servidor FCM	4139	KLSRV_GCM_HTTP_ERROR	Eventos desse tipo ocorrem quando o Gerenciamento de Dispositivos Móveis está configurado para usar o Google Firebase Cloud Messaging (FCM) para se conectar a dispositivos móveis gerenciados com sistema operacional Android e o Servidor FCM responde à solicitação do Servidor de Administração com um código HTTP diferente de 200 (OK). Seguem abaixo as possíveis causas e as respostas apropriadas para o evento: • Problemas no lado do servidor FCM. Leia o código HTTP nos detalhes da descrição do evento e responda de acordo. Para obter mais informações sobre os códigos HTTP recebidos do Servidor de FCM e erros relacionados, consulte a documentação do serviço Google Firebase (em especial, o capítulo "Códigos de resposta de erro de mensagens downstream"). • Problemas no lado do servidor proxy (se estiver usando servidor proxy). Leia o código HTTP nos detalhes da descrição do evento e responda de acordo.	90 dias
O limite da licença foi excedido	4098	KLSRV_EV_LICENSE_CHECK_100_110	Uma vez por dia o Kaspersky Security Center Linux verifica se um limite de licenciamento foi excedido. Eventos desse tipo ocorrem quando o Servidor de Administração detecta que alguns limites da licença foram excedidos pelos aplicativos da Kaspersky instalados nos dispositivos clientes e se o número de unidades de licenciamento atualmente usadas e abrangidas por uma única licença corresponde entre 100% e 110% do número total de unidades abrangidas pela licença. Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. • Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração). O Kaspersky Security Center Linux determina as regras para gerar eventos quando um limite de licenciamento é excedido.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O limite de instalações será atingido para um dos grupos de aplicativos licenciados	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Esse tipo de evento ocorre quando uma das chaves de licença de aplicativos de terceiros, incluída em um grupo de aplicativos licenciados, está prestes a expirar. Como resultado, o limite de instalação para um dos grupos será reduzido. Você pode responder ao evento nas seguintes maneiras: • Se o aplicativo de terceiros não estiver em uso em alguns dos dispositivos gerenciados, exclua o aplicativo desses dispositivos. • Se você espera que o número de instalações do aplicativo de terceiros ultrapasse o máximo permitido em um futuro próximo, considere obter uma licença de terceiros para um número maior de dispositivos com antecedência. Você pode gerenciar chaves de licença de aplicativos de terceiros usando a funcionalidade de grupos de aplicativos licenciados.	90 dias
Novas atualizações para os módulos do aplicativo da Kaspersky foram registradas	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Eventos deste tipo ocorrem quando o Servidor de Administração registra novas atualizações para o software Kaspersky instalado em dispositivos gerenciados que requerem aprovação para instalação. Aprove ou recuse as atualizações usando o Kaspersky Security Center Web Console.	90 dias
Espaço insuficiente no banco de dados do Servidor de Administração	4106	KLSRV_NO_SPACE_IN_DATABASE	Eventos deste tipo ocorrem se o espaço no banco de dados do Servidor de Administração for muito limitado. Se você não remediar a situação, em breve o banco de dados do Servidor de Administração alcançará sua capacidade e o Servidor de Administração não funcionará. A seguir estão as causas deste evento, dependendo do DBMS que estiver usando, e as respostas apropriadas ao evento. • Não limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração Revise as informações na seleção do DBMS.	90 dias
O limite de eventos no banco de dados foi excedido. A exclusão dos eventos foi iniciada	4145	KLSRV_EVP_DB_TRUNCATING	Eventos deste tipo ocorrem quando a exclusão de eventos antigos do banco de dados do Servidor de Administração começou após a capacidade do banco de dados do Servidor de Administração ter sido alcançada. Você pode responder ao evento nas seguintes maneiras: • Alterar o número máximo de eventos armazenados no banco de dados do Servidor de Administração • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração	Não armazenado

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O limite de eventos no banco de dados foi excedido. Os eventos foram excluídos	4146	KLSRV_EVP_DB_TRUNCATED	Eventos deste tipo ocorrem quando a exclusão de eventos antigos do banco de dados do Servidor de Administração começou após a capacidade do banco de dados do Servidor de Administração ter sido alcançada. Você pode responder ao evento nas seguintes maneiras: • Altere o número máximo de eventos armazenados permitidos no banco de dados do Servidor de Administração • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração	Não armazenado

Eventos informativos do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração com o nível de importância **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O certificado do Servidor de Administração para dispositivos móveis está sendo renovado	6127	KLSRV_EV_SRV_CERT_RENEWED	Este evento ocorre quando o certificado do Servidor de Administração é renovado.	30 dias
Auditoria: O comando foi enviado para o dispositivo	4170	KLAUD_EV_COMMAND_SENT	Eventos desse tipo ocorrem quando o usuário envia um comando para o dispositivo móvel.	30 dias
Auditoria: a conexão com o Servidor de Administração foi encerrada	4151	KLAUD_EV_SERVERDISCONNECT		30 dias
Auditoria: a conexão com o Servidor de Administração foi estabelecida	4147	KLAUD_EV_SERVERCONNECT	Eventos desse tipo ocorrem quando um usuário se conecta ao Servidor de Administração por meio do Kaspersky Security Center Web Console. Esses eventos incluem o endereço IP do dispositivo no qual o Kaspersky Security Center Web Console Server está instalado.	30 dias
Auditoria: chaves de criptografia importadas/exportadas	5100	KLAUD_EV_DPEKEYSEXPORT	Por exemplo, esse evento ocorre durante a migração.	30 dias
Auditoria: as configurações do grupo foram modificadas	4149	KLAUD_EV_ADMGROUP_CHANGED	Eventos desse tipo ocorrem quando um grupo de segurança é editado.	30 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Auditoria: o objeto foi modificado	4148	KLAUD_EV_OBJECTMODIFY	Este evento acompanha mudanças nos seguintes objetos: • Grupo de administração • Grupo de segurança • Usuário • Dispositivo gerenciado • Pacote • Tarefa • Política • Servidor • Servidor virtual	30 dias
Auditoria: as propriedades do objeto foram modificadas	4152	KLAUD_EV_OBJECTPROPMODIFIED	Este evento rastreia as mudanças nas seguintes propriedades: • Usuário • Licença • Servidor • Servidor virtual	30 dias
Auditoria: o status do objeto foi alterado	4150	KLAUD_EV_TASK_STATE_CHANGED	Por exemplo, este evento ocorre quando uma tarefa falha com um erro.	30 dias
Auditoria: teste de conexão bem-sucedido com o servidor SIEM	5110	KLAUD_EV_SIEM_TEST_SUCCESS	Eventos desse tipo ocorrem quando uma conexão de teste com o servidor SIEM foi bem-sucedida.	30 dias
Auditoria: as permissões do usuário foram modificadas	4153	KLAUD_EV_OBJECTACLMODIFIED	Este evento ocorre quando as permissões do usuário são modificadas	30 dias
A conexão com o Servidor de Administração principal foi estabelecida	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 dias
A conexão com o Servidor de Administração secundário foi estabelecida	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Consulte o seguinte artigo para obter detalhes: Criação de uma hierarquia de Servidores de Administração: adição de um Servidor de Administração secundário.	30 dias
Os bancos de dados foram atualizados	4144	KLSRV_UPD_BASES_UPDATED	Eventos desse tipo ocorrem quando a tarefa **Baixar atualizações no repositório do Servidor de Administração** conclui a atualização dos bancos de dados.	30 dias
O dispositivo foi migrado automaticamente de acordo com uma regra	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	Eventos desse tipo ocorrem quando os dispositivos foram movidos para grupos de administração usando regras de movimentação de dispositivos. Um evento separado é publicado para cada dispositivo movido.	30 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O dispositivo foi removido do grupo: inativo na rede por muito tempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	Eventos desse tipo ocorrem quando dispositivos são automaticamente removidos de um grupo por inatividade.	30 dias
A ID da Instância FCM foi alterada neste dispositivo móvel	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	Eventos desse tipo ocorrem quando o token do Firebase Cloud Messaging é alterado no dispositivo. Para obter informações sobre a rotação de tokens do FCM, consulte a documentação do serviço Firebase.	30 dias
Arquivo carregado no Servidor de Administração	4162	KLSRV_FILE_UPLOADED	Eventos desse tipo ocorrem se o administrador tiver carregado um arquivo na lista **Gerenciamento de ativos → Mobile → Apps & files → Files**.	30 dias
Arquivo excluído do Servidor de Administração	4163	KLSRV_FILE_REMOVED	Eventos desse tipo ocorrem se o administrador tiver excluído um arquivo da lista **Gerenciamento de ativos → Mobile → Apps & files → Files**.	30 dias
Arquivo baixado no dispositivo	4164	KLSRV_FILE_DOWNLOADED	Eventos desse tipo ocorrem nos seguintes casos: • O administrador baixou um arquivo da lista **Gerenciamento de ativos → Mobile → Apps & files → Files** no Web Console para a estação de trabalho do administrador. • Um arquivo da lista **Gerenciamento de ativos → Mobile → Apps & files → Files** foi baixado para um dispositivo no qual o Kaspersky Endpoint Security for Android está instalado.	30 dias
Falha ao baixar o arquivo para o dispositivo	4165	KLSRV_FILE_DOWNLOAD_FAILED	Eventos desse tipo ocorrem nos seguintes casos: • Ocorreu um erro quando o administrador tentou baixar um arquivo da lista **Gerenciamento de ativos → Mobile → Apps & files → Files** do Web Console para a estação de trabalho do administrador. • Ocorreu um erro ao baixar um arquivo da lista **Gerenciamento de ativos → Mobile → Apps & files → Files** para um dispositivo no qual o Kaspersky Endpoint Security for Android está instalado.	30 dias
Foram encontrados arquivos para serem enviados para análise pela Kaspersky	4131	KLSRV_APS_FILE_APPEARED		30 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O limite de instalações está prestes a ser excedido (mais de 90% já foram utilizados) para um dos grupos de aplicativos licenciados	4127	KLSRV_INVLICPROD_FILLED	Eventos deste tipo ocorrem quando o número de instalações de aplicativos de terceiros incluídos em um grupo de aplicativos licenciados atinge 90% do valor máximo permitido especificado nas propriedades da chave de licença. Você pode responder ao evento nas seguintes maneiras: • Se o aplicativo de terceiros não estiver em uso em alguns dos dispositivos gerenciados, exclua o aplicativo desses dispositivos. • Se você espera que o número de instalações do aplicativo de terceiros ultrapasse o máximo permitido em um futuro próximo, considere obter uma licença de terceiros para um número maior de dispositivos com antecedência. Você pode gerenciar chaves de licença de aplicativos de terceiros usando a funcionalidade de grupos de aplicativos licenciados.	30 dias
Novo dispositivo detectado	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	Eventos desse tipo ocorrem quando novos dispositivos em rede são descobertos.	30 dias
Mais de 90% desta chave de licença foram usados	4097	KLSRV_EV_LICENSE_CHECK_90	Eventos desse tipo ocorrem quando o Servidor de Administração detecta que alguns limites da licença foram excedidos pelos aplicativos da Kaspersky instalados nos dispositivos clientes e se o número de unidades de licenciamento atualmente usadas e abrangidas por uma única licença excede 90% do número total de unidades abrangidas pela licença. Mesmo quando um limite de licenciamento é excedido, os dispositivos clientes ficam protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. • Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração). O Kaspersky Security Center Linux determina as regras para gerar eventos quando um limite de licenciamento é excedido.	30 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O certificado de reserva do Servidor de Administração para dispositivos móveis foi criado	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	Este evento ocorre quando um certificado do Servidor de Administração é criado.	30 dias
As atualizações foram copiadas com êxito para a pasta especificada	4122	KLSRV_UPD_REPL_OK	Eventos desse tipo ocorrem quando a tarefa **Baixar atualizações no repositório do Servidor de Administração** conclui a cópia de arquivos para uma pasta especificada.	30 dias

Os eventos **Certificado reserva criado** e **Renovação de certificado** são publicados automaticamente pelo Servidor de Administração e somente aparecem no Console de Administração quando as operações correspondentes são executadas para os certificados do Servidor de Administração usados em dispositivos móveis e UEFI.

Eventos do Agente de Rede

Esta seção contém informações sobre os eventos relativos ao Agente de Rede.

Eventos de falha funcional do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center Linux que têm o nível de gravidade **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Falha ao instalar os certificados raiz	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	O evento contém a descrição do erro de instalação dos certificados.	30 dias
Falha ao instalar a atualização de software de terceiros	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Eventos desse tipo acontecem se o recurso Gerenciamento de patches e vulnerabilidades estiver ativo e uma atualização de software de terceiros não tiver tido êxito. Verificar se o link para o software de terceiros é válido. Leia a descrição do evento.	30 dias
Falha ao instalar as atualizações do Windows	7717	KLNAG_EV_WUA_INSTALL_ERROR	Eventos deste tipo ocorrem se a atualizações do Windows não tiverem êxito. Leia a descrição do evento. Procure o erro na Base de Dados de Conhecimento da Microsoft. Entre em contato com o Suporte Técnico da Microsoft se você não conseguir resolver o problema você mesmo.	30 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Falha ao remover os certificados raiz	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	O evento contém a descrição do erro de remoção de certificados.	30 dias
Falha ao restaurar o arquivo sudoers para o valor de referência	7726	KLNAG_EV_SUDOER_RESTORED_ERR	O evento contém a descrição do erro de substituição do arquivo sudoers.	30 dias
Erro de instalação da atualização	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Eventos deste tipo ocorrem se a atualização e correção automática para os componentes do Kaspersky Security Center Linux não teve êxito. O evento não contém atualizações dos aplicativos gerenciados da Kaspersky. Leia a descrição do evento. Um problema do Windows no Servidor de Administração poderá ser o motivo desse evento. Se descrição mencionar qualquer problema da configuração do Windows, solucione o problema.	30 dias
Gerenciamento de usuários: erros	7723	KLNAG_EV_USR_MNG_ERR	Evento de advertência geral.	30 dias

Eventos de aviso do Agente de Rede

A tabela abaixo demonstra os eventos do Agente de Rede que têm o nível de gravidade **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Proxy da KSN iniciado. Falha ao verificar a disponibilidade da KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	Eventos desse tipo ocorrem quando a conexão de teste falha para a conexão proxy KSN configurada.	30 dias
Ocorreu um problema de segurança	549	GNRL_EV_APP_INCIDENT_OCCURED	Eventos desse tipo ocorrem quando um incidente é encontrado em um dispositivo. Por exemplo, esse evento ocorre quando o dispositivo tem pouco espaço em disco.	30 dias
O arquivo sudoers encontrado não corresponde ao valor de referência	7724	KLNAG_EV_SUDOER_DIFFERENT	Eventos desse tipo ocorrem quando há uma incompatibilidade entre o arquivo sudoers e o arquivo de referência.	30 dias
A instalação da atualização do software de terceiros foi adiada	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Por exemplo, eventos desse tipo ocorrem quando o EULA para a instalação da atualização de terceiros é recusado.	30 dias
A instalação da atualização do software de terceiros foi concluída com uma advertência	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Baixe os arquivos de rastreamento e verifique o valor do campo KLRI_PATCH_RES_DESC para obter mais detalhes.	30 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Gerenciamento de usuários: advertências	7722	KLNAG_EV_USR_MNG_WRN	Evento de advertência geral.	30 dias
Uma advertência foi retornada durante a instalação da atualização dos módulos de software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Baixe os arquivos de rastreamento e verifique o valor do campo KLRI_PATCH_RES_DESC para obter mais detalhes.	30 dias

Eventos informativos do Agente de Rede

A tabela abaixo demonstra os eventos do Agente de Rede que têm o nível de gravidade **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Aplicativo instalado	7703	KLNAG_EV_INV_APP_INSTALLED	30 dias
Aplicativo desinstalado	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 dias
O certificado foi recebido para a porta HTTPS do servidor Web	—	WEB_SERVER_CERTIFICATE_RENEWED	30 dias
O dispositivo foi autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dias
Novo dispositivo detectado	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dias
Dispositivo removido	7709	KLNAG_EV_DEVICE_REMOVE	30 dias
A instalação da atualização dos módulos de software foi iniciada	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 dias
Proxy da KSN iniciado. A verificação de disponibilidade da KSN foi concluída com êxito	7719	KSNPROXY_STARTED_CON_CHK_OK	30 dias
Proxy da KSN parado	7720	KSNPROXY_STOPPED	30 dias
O aplicativo monitorado foi instalado	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 dias
O aplicativo monitorado foi desinstalado	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 dias
Novo dispositivo adicionado	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dias
Certificados raiz instalados	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 dias
Certificados raiz removidos	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 dias
Arquivo sudoers restaurado com êxito para o valor de referência	7725	KLNAG_EV_SUDOER_RESTORED	30 dias
O aplicativo de terceiros foi instalado	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 dias
A atualização do software de terceiros foi instalada com êxito	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 dias
A instalação da atualização de software de terceiros foi iniciada	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 dias
A atualização dos módulos de software foi instalada com êxito	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 dias
Gerenciamento de usuários: informações	7721	KLNAG_EV_USR_MNG_INF	30 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Servidor Web iniciado no host	—	WEB_SERVER_STARTED	30 dias
Servidor Web interrompido no host	—	WEB_SERVER_STOPPED	30 dias
Windows Desktop Sharing: aplicativo iniciado	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 dias
Windows Desktop Sharing: o arquivo foi modificado	7713	KLUSRLOG_EV_FILE_MODIFIED	30 dias
Windows Desktop Sharing: o arquivo foi lido	7712	KLUSRLOG_EV_FILE_READ	30 dias
Windows Desktop Sharing: iniciado	7715	KLUSRLOG_EV_WDS_BEGIN	30 dias
Windows Desktop Sharing: parado	7716	KLUSRLOG_EV_WDS_END	30 dias

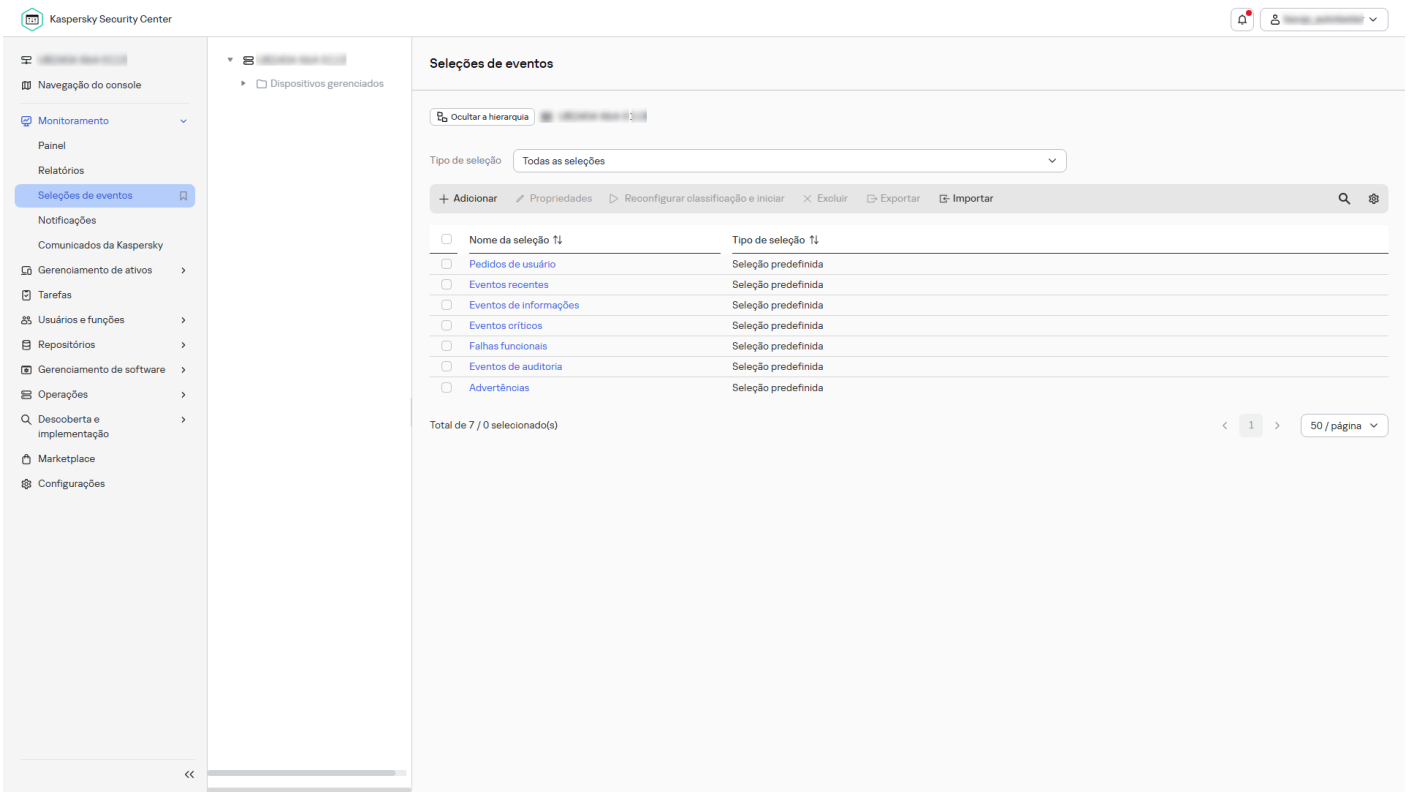
Usar as seleções de eventos

As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. Esses conjuntos de eventos são agrupados de acordo com as seguintes categorias:

- Por nível de importância – **Eventos críticos**, **Falhas funcionais**, **Advertências** e **Eventos de informações**
- Por tempo – **Eventos recentes**
- Por tipo – **Pedidos de usuário** e **Eventos de auditoria**

Você pode criar e visualizar seleções de eventos definidas pelos usuários baseado nas configurações disponíveis para configuração na interface do Kaspersky Security Center Web Console.

As seleções de eventos estão disponíveis no Kaspersky Security Center Web Console, na seção **Monitoramento**, clicando em **Seleções de eventos**.



A lista de seleções de eventos

Por padrão, as seleções de eventos incluem informações dos últimos sete dias.

O Kaspersky Security Center Linux tem um conjunto padrão de seleções de eventos (predefinidas):

- Eventos com níveis de importância diferentes:
  - **Eventos críticos**
  - **Falha funcional**
  - **Advertências**
  - **Eventos informativos**
- **Solicitações de usuário** (eventos de aplicativos gerenciados)
- **Eventos recentes** (na semana passada)
- Eventos de auditoria.

Também é possível criar e configurar seleções adicionais definidas pelo usuário. Em seleções definidas pelos usuários, é possível filtrar eventos pelas propriedades dos dispositivos dos quais se originaram (nomes de dispositivos, conjuntos de IPs e grupos de administração), por tipos de evento e níveis de gravidade, por aplicativo e nome do componente e por intervalo de tempo. Também é possível incluir resultados da tarefa no escopo de pesquisa. Você também pode usar um campo de pesquisa simples em que uma palavra ou várias palavras podem ser digitadas. São exibidos todos os eventos que contêm alguma das palavras digitadas em qualquer lugar nos seus atributos (como nome do evento, descrição, nome do componente).

Para seleções predefinidas e definidas pelos usuários, você pode limitar o número de eventos exibidos ou o número de registros para pesquisar. Ambas as opções afetam o tempo necessário para o Kaspersky Security Center Linux exibir os eventos. Quanto maior for o banco de dados, mais demorado será o processo.

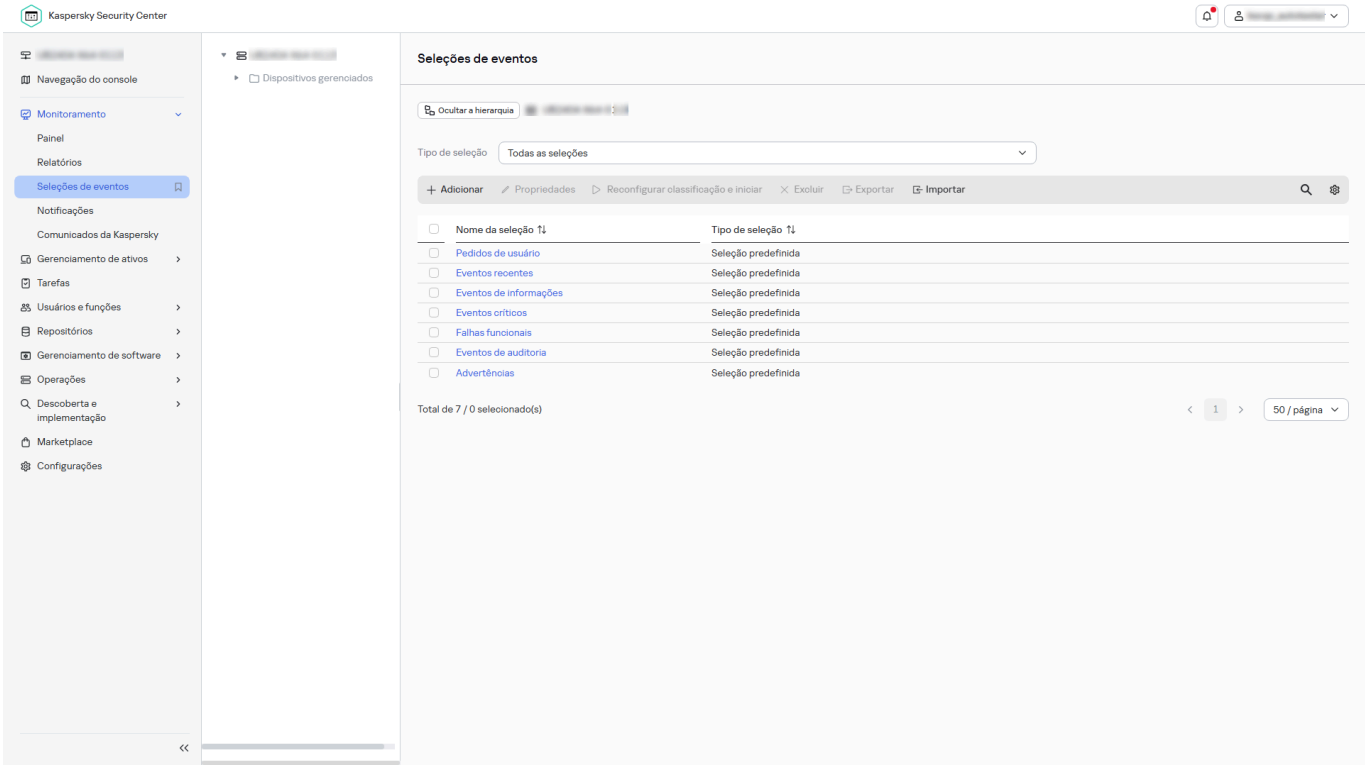
Você pode fazer o seguinte:

- Editar propriedades das seleções de eventos
- Gerar seleções de eventos
- Visualizar detalhes das seleções de eventos
- Excluir seleções de eventos
- Excluir eventos do banco de dados do Servidor de Administração

Criar uma seleção de eventos

Para criar uma seleção de eventos:

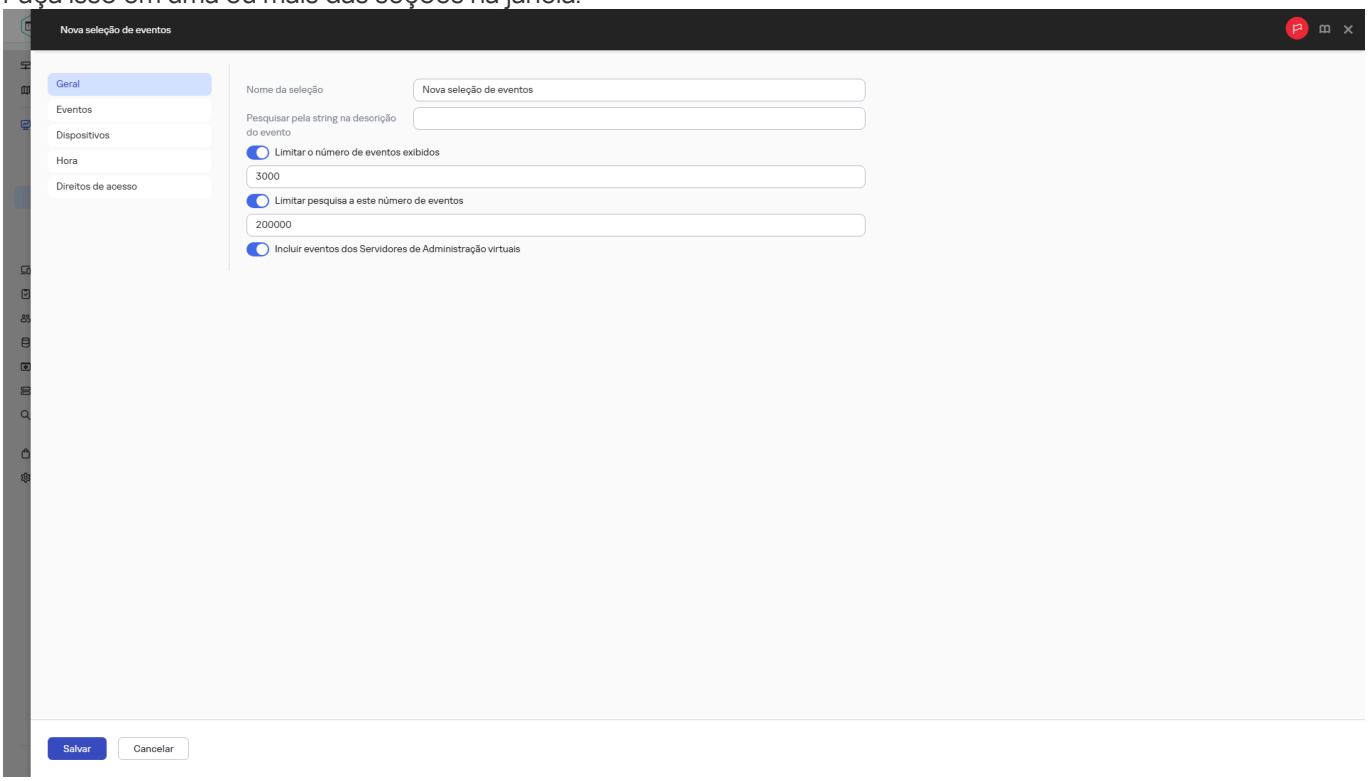
1. No menu principal, vá para **Monitoramento → Seleções de eventos**.



A lista de seleções de eventos

2. Clique em **Adicionar**.

3. Na janela **Nova seleção de eventos** que se abre, especifique as configurações da nova seleção de eventos. Faça isso em uma ou mais das seções na janela.



Criação de uma nova seleção de eventos

4. Clique em **Salvar** para salvar as alterações.

   Uma janela de confirmação é exibida.

5. Para visualizar o resultado da seleção de eventos, mantenha a caixa de seleção **Ir para o resultado da seleção** selecionada.

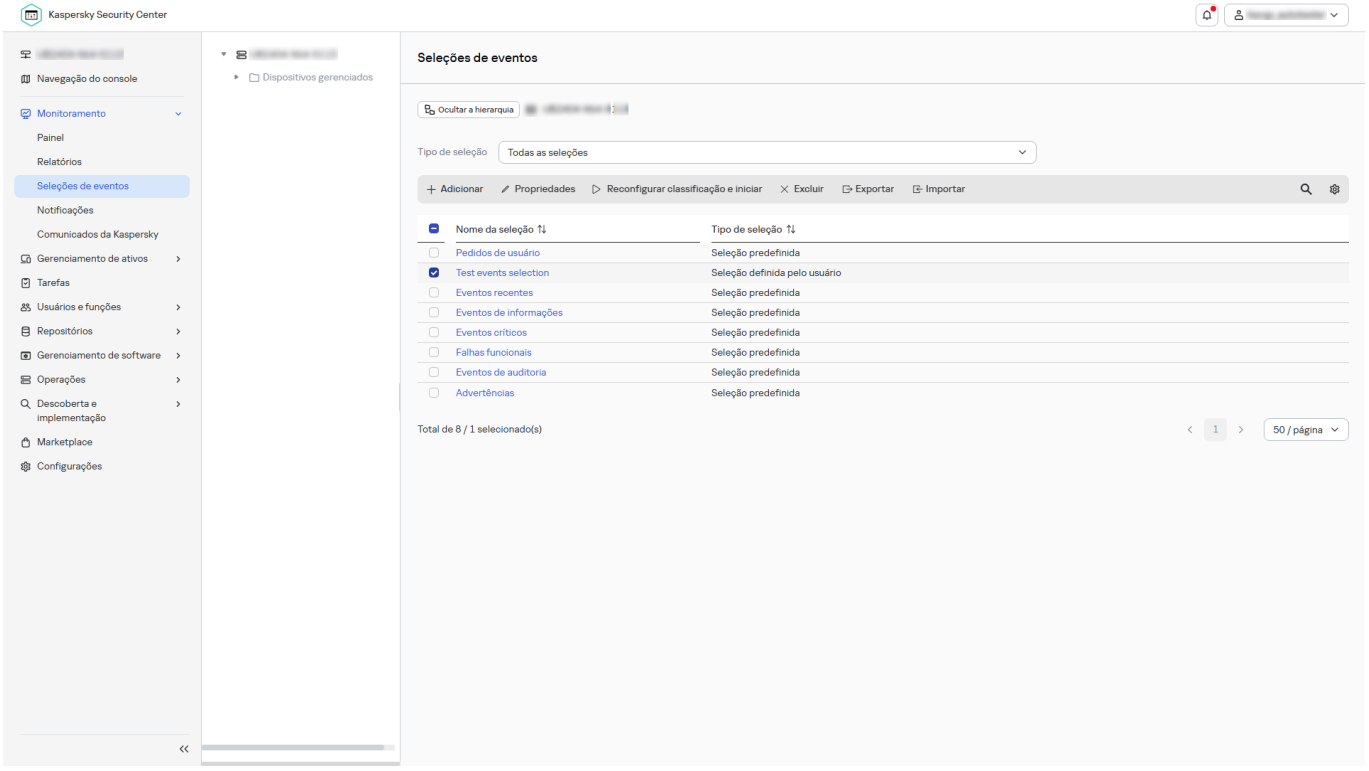
6. Clique em **Salvar** para confirmar a criação da seleção de eventos.

Se você tiver mantido a caixa de seleção **Ir para o resultado da seleção** selecionada, o resultado da seleção de eventos será exibido. Caso contrário, a nova seleção de eventos será exibida na lista de seleção de eventos.

Editar uma seleção de eventos

Para editar uma seleção de eventos:

1. No menu principal, vá para **Monitoramento → Seleções de eventos**.
2. Marque a caixa de seleção ao lado da seleção de eventos que deseja editar.



A lista de seleções de eventos

3. Clique no botão **Propriedades**.

   Uma janela de configurações de seleção de eventos é aberta.

4. Edite as propriedades da seleção de eventos.

   > Para seleções de eventos predefinidas, você pode editar somente as propriedades nas seguintes guias: **Geral** (exceto o nome de seleção), **Hora** e **Direitos de acesso**.

   Para seleções definidas pelos usuários, você pode editar todas as propriedades.

5. Clique em **Salvar** para salvar as alterações.

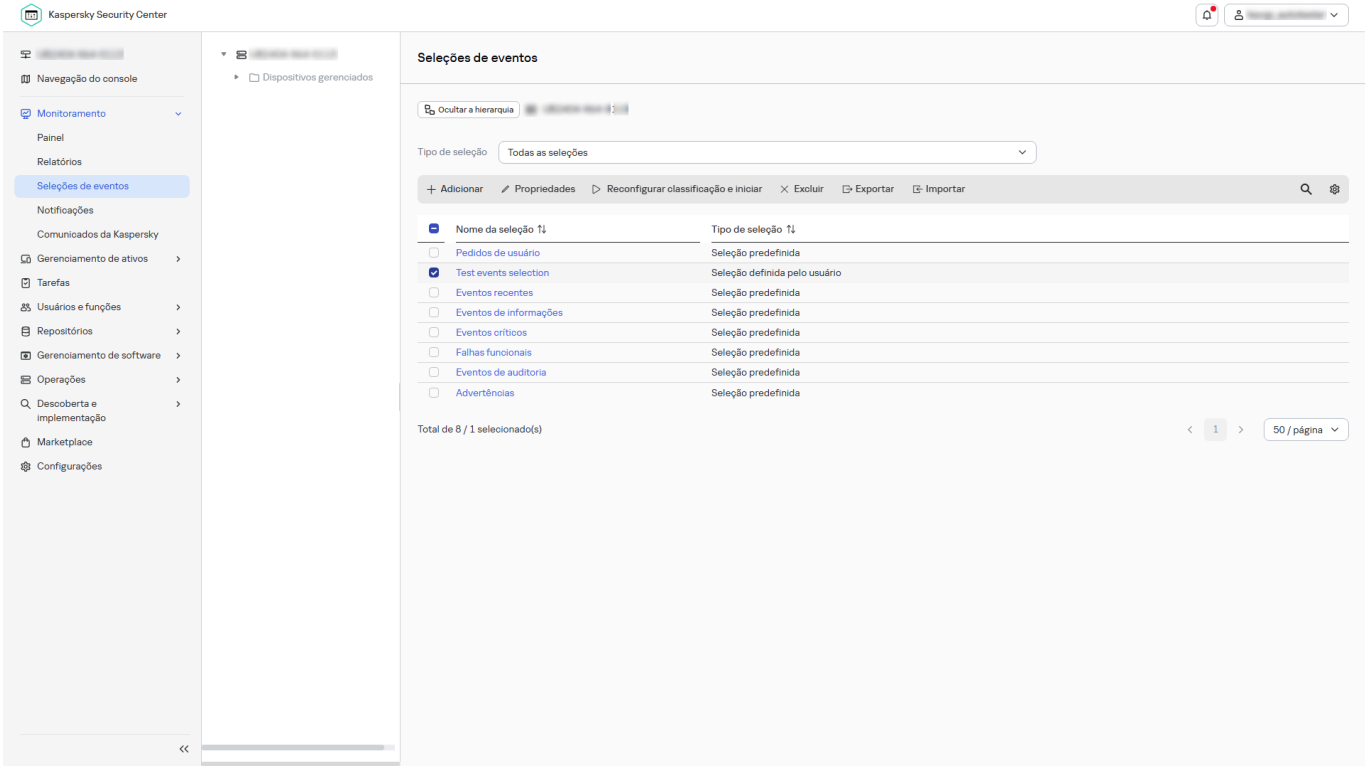
A seleção de eventos editada é mostrada na lista.

Visualizando uma lista de uma seleção de eventos

Para visualizar a seleção de eventos:

1. No menu principal, vá para **Monitoramento → Seleções de eventos**.

2. Marque a caixa de seleção ao lado da seleção de eventos que deseja iniciar.



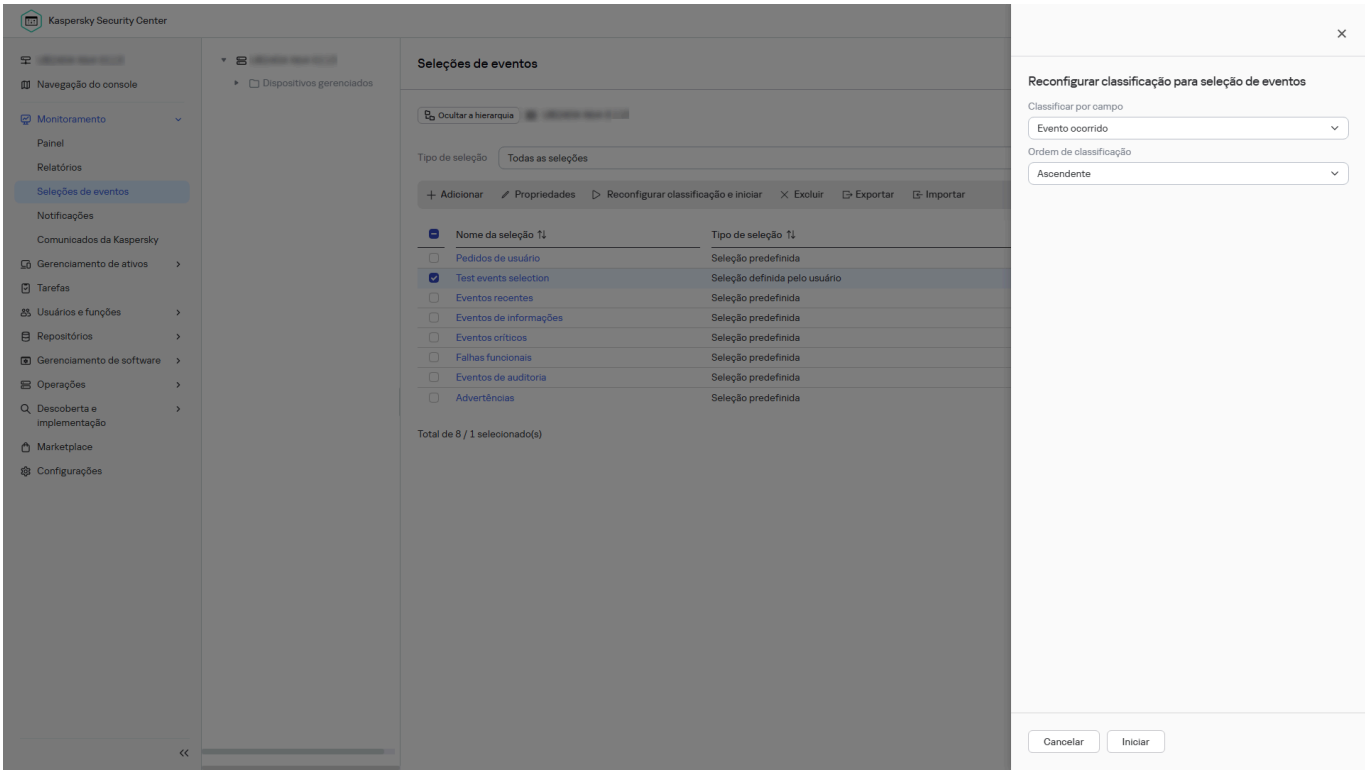
A lista de seleções de eventos

3. Execute uma das seguintes ações:

- Se você quiser configurar a classificação no resultado da seleção de eventos, faça o seguinte:

  a. Clique no botão **Reconfigurar classificação e iniciar**.

  b. Na janela exibida **Reconfigurar classificação para seleção de eventos**, especifique as configurações de classificação.

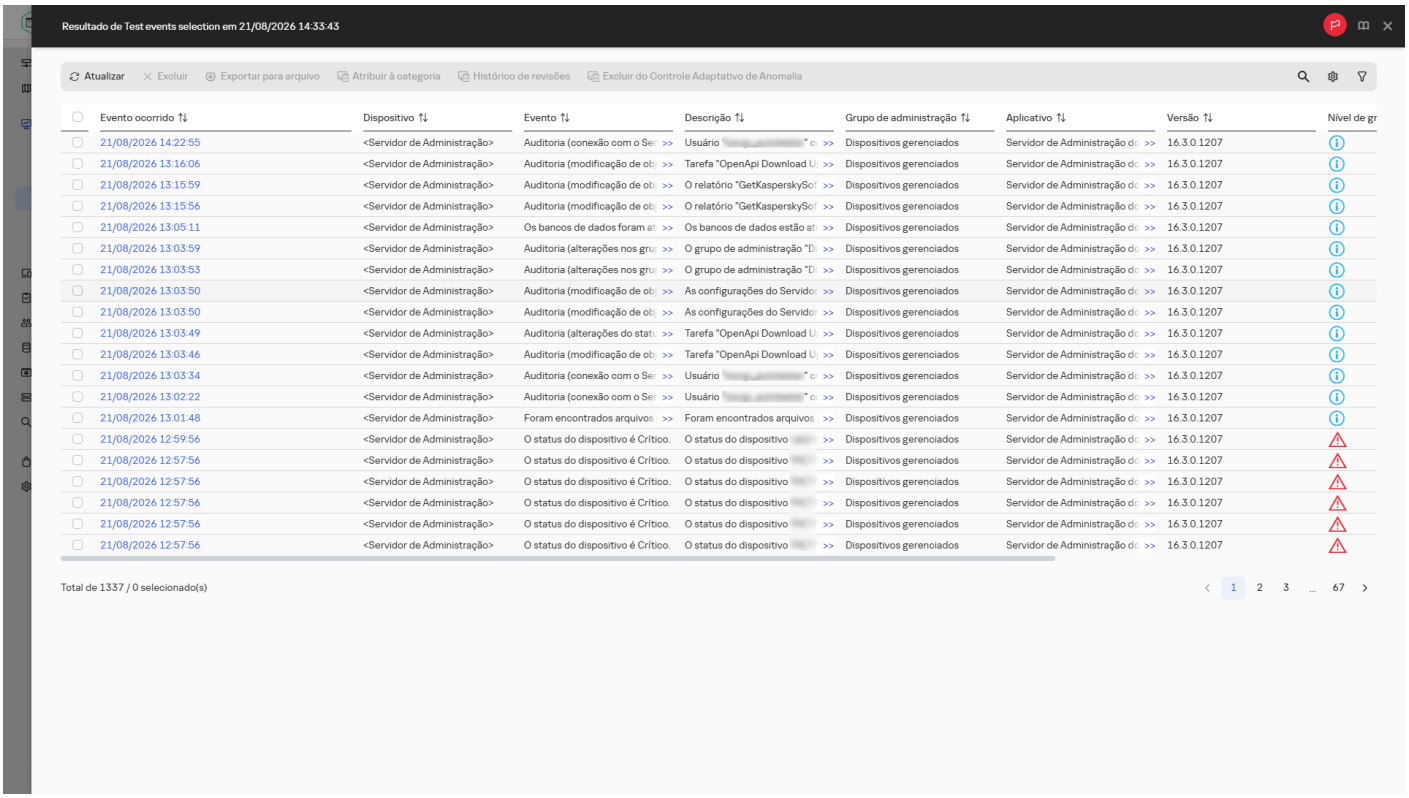


Especificação das configurações de ordenação da seleção de eventos

  a. Clique no nome da seleção.

- Caso contrário, se você quiser visualizar a lista de eventos e como eles estão classificados no Servidor de Administração, clique no nome da seleção.

O resultado da seleção de eventos é exibido.



O resultado da seleção de eventos

Exportar uma seleção de eventos

O Kaspersky Security Center Linux permite salvar uma seleção de eventos e suas configurações em um arquivo KLO. É possível usar esse arquivo KLO para importar a seleção de eventos salva para o Kaspersky Security Center Windows e para o Kaspersky Security Center Linux.

Observe que é possível exportar apenas as seleções de eventos definidas pelo usuário. As seleções de eventos do conjunto padrão do Kaspersky Security Center Linux (seleções predefinidas) não podem ser salvas em um arquivo.

Para exportar a seleção de eventos:

1. No menu principal, acesse **Monitoramento** → **Seleções de eventos**.
2. Marque a caixa de seleção ao lado da seleção de eventos você deseja iniciar.

   Não é possível exportar as várias seleções de eventos ao mesmo tempo. Caso selecione mais de uma tarefa, o botão **Exportar** será desabilitado.
3. Clique no botão **Exportar**.
4. Na janela aberta **Salvar como**, especifique o nome e o caminho do arquivo de seleção de eventos e clique no botão **Salvar**.

   A janela **Salvar como** é exibida apenas se você usar Google Chrome, Microsoft Edge ou Opera. Caso outro navegador seja usado, o arquivo de seleção de eventos será salvo automaticamente na pasta **Downloads**.

Importar uma seleção de eventos

O Kaspersky Security Center Linux permite importar uma seleção de eventos de um arquivo KLO. O arquivo KLO contém a seleção de eventos exportada e suas configurações.

Para importar uma seleção de eventos:

1. No menu principal, acesse **Monitoramento** → **Seleções de eventos**.
2. Clique no botão **Importar** e escolha um arquivo de seleção de eventos que deseja importar.
3. Na janela aberta, especifique o caminho para o arquivo KLO e clique no botão **Abrir**. Observe que é possível selecionar apenas um arquivo de seleção de eventos.

   O processamento da seleção de eventos é iniciado.

A notificação com os resultados da importação é exibida. Caso a seleção de eventos seja importada com êxito, será possível clicar no link **Exibir detalhes da importação** para exibir as propriedades da seleção de eventos.

Após a importação ser concluída com êxito, a seleção de eventos será exibida na lista de seleção. As configurações da seleção de eventos também são importadas.

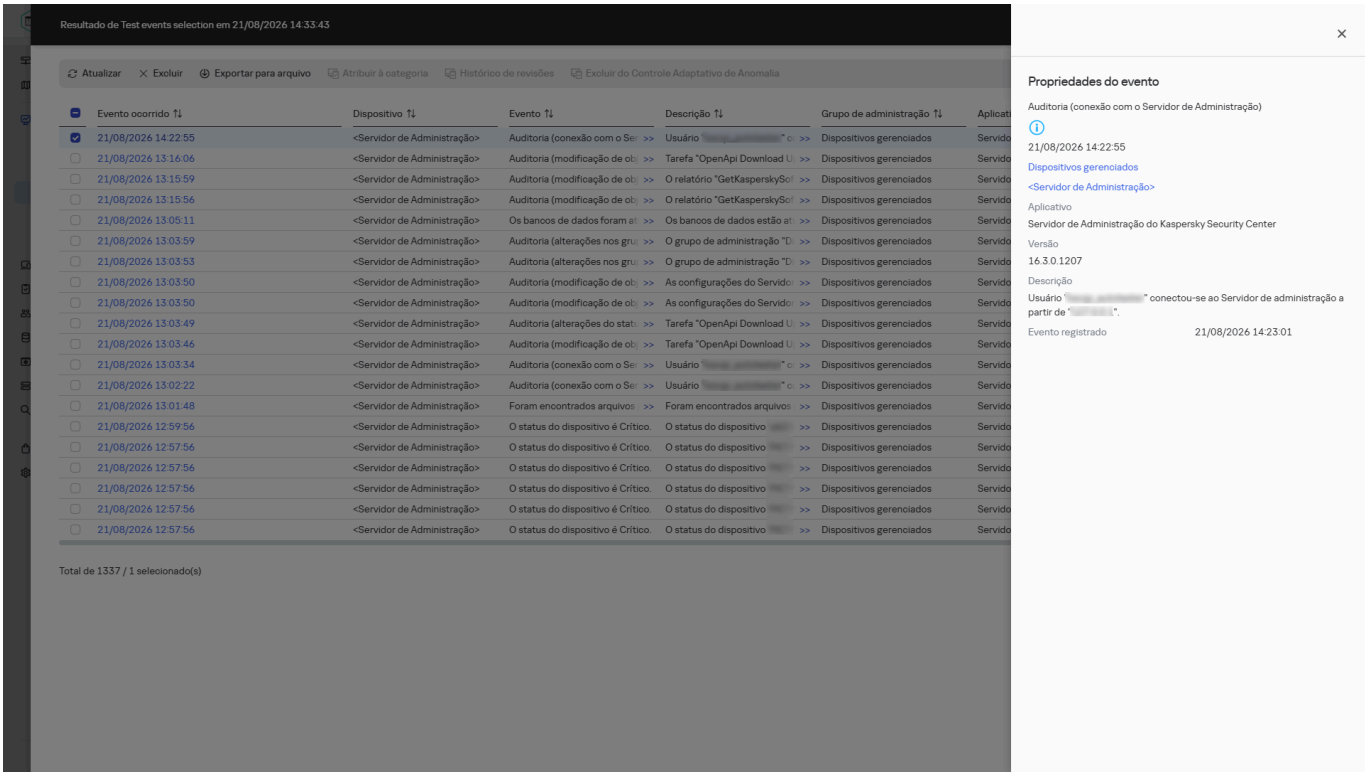
Caso a seleção de eventos recém-importada tenha um nome idêntico ao de seleção de eventos existente, o nome da seleção importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Visualização das áreas de detalhes do evento

Para visualizar detalhes de um evento:

1. Nova seleção de eventos.
2. Clique na hora do evento necessário.

A janela **Propriedades do evento** se abre.



A janela de propriedades do evento

3. Na janela exibida, você pode fazer o seguinte:

   - Visualizar as informações sobre o evento selecionado
   - Ir ao dispositivo no qual o evento ocorreu
   - Ir ao grupo de administração que inclui o dispositivo no qual o evento ocorreu
   - Para um evento relacionado a uma tarefa, vá às propriedades da tarefa

Exportar eventos para um arquivo

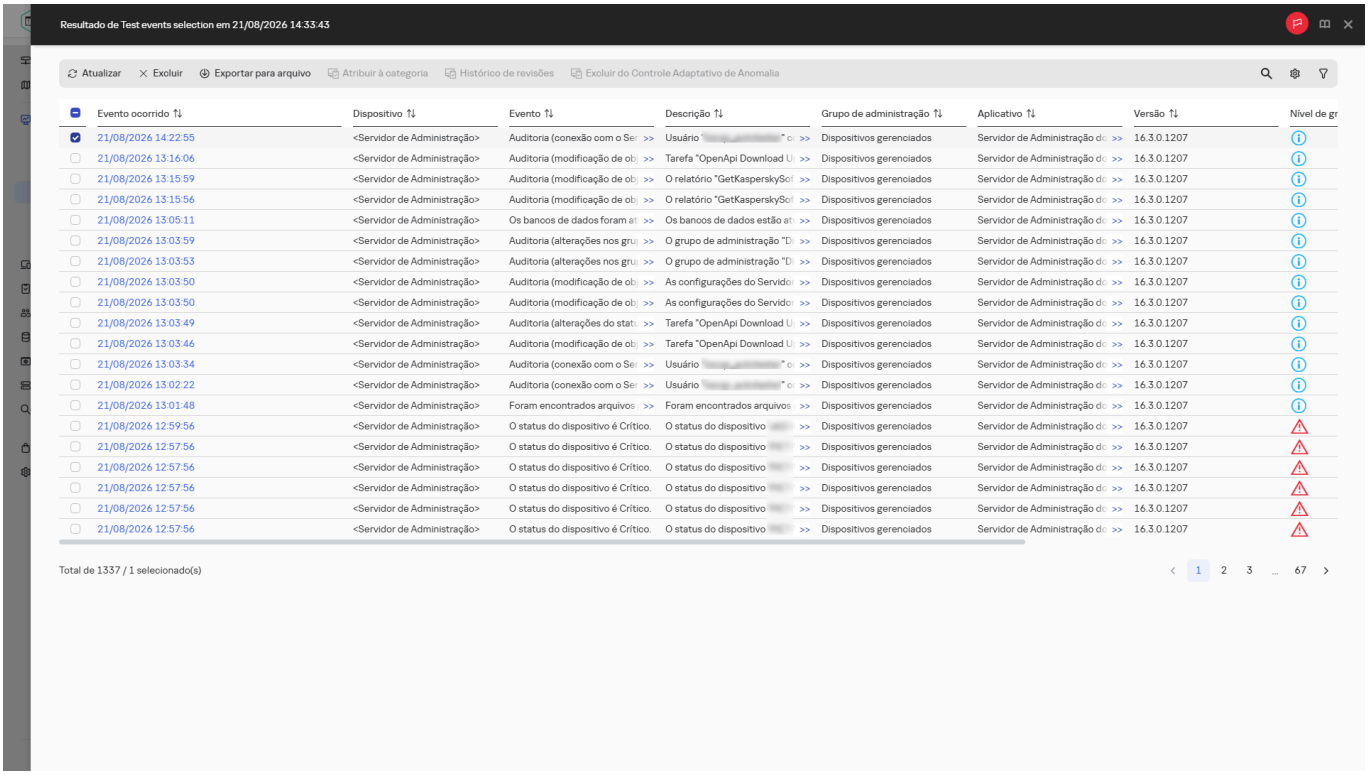
O Kaspersky Security Center Linux pode salvar eventos em um arquivo CSV ou TXT.

Para exportar eventos de uma seleção de eventos:

1. No menu principal, vá para **Monitoramento** → **Seleções de eventos**.
2. Clique no nome da seleção desejada.

3. Selecione os eventos:

- Se quiser exportar um ou vários eventos, marque as caixas de seleção ao lado dos eventos.
- Se quiser exportar todos os eventos na página atual, marque a caixa de seleção acima da lista de eventos e clique em **Selecionar todos na página atual**.
- Se quiser exportar todos os eventos de uma seleção, marque a caixa de seleção acima da lista de eventos e clique em **Selecionar tudo**.



O resultado da seleção de eventos

4. Clique no botão **Exportar** e selecione **Exportar para CSV** ou **Exportar para TXT**.

Para exportar eventos da lista de eventos de um dispositivo:

1. Abra a lista de dispositivos.
   - Para dispositivos gerenciados: **Gerenciamento de ativos** → **Dispositivos gerenciados**.
   - Para dispositivos não atribuídos: **Gerenciamento de ativos** → **Dispositivos não atribuídos**.
2. Na lista de dispositivos, clique no link com o nome do dispositivo desejado e vá para a guia **Eventos**.

3. Selecione os eventos:

   - Se você quiser excluir um ou vários eventos, marque as caixas de seleção ao lado dele(s).
   - Se quiser excluir todos os eventos na página atual, marque a caixa de seleção acima da lista de eventos e clique na opção **Selecionar todos na página atual**.
   - Se quiser excluir todos os eventos de uma seleção, marque a caixa de seleção acima da lista de eventos e clique na opção **Selecionar tudo**.

4. Clique no botão **Exportar** e selecione **Exportar para CSV** ou **Exportar para TXT**.

Todas as informações sobre os eventos selecionados incluídas na tabela são exportadas.

Visualização de um histórico de eventos a partir de um evento

De um evento de criação ou modificação de um objeto que não tem suporte no gerenciamento de revisão, você pode alternar para o histórico de revisões do objeto.

Para visualizar o histórico de revisões de um evento:

1. Nova seleção de eventos.
2. Selecione a caixa de seleção junto ao evento necessário.
3. Clique no botão **Histórico de revisões**.

O histórico de revisões do objeto é aberto.

Excluir os eventos

Para excluir eventos de uma seleção:

1. Nova seleção de eventos.
2. Selecione os eventos:

   - Se você quiser excluir um ou vários eventos, marque as caixas de seleção ao lado dele(s).
   - Se quiser excluir todos os eventos na página atual, marque a caixa de seleção acima da lista de eventos e clique na opção **Selecionar todos na página atual**.
   - Se quiser excluir todos os eventos de uma seleção, marque a caixa de seleção acima da lista de eventos e clique na opção **Selecionar tudo**.

3. Clique no botão **Excluir**.
4. Na janela exibida, clique em **Excluir**.

Para excluir eventos de uma lista de eventos de dispositivo:

1. Abra a lista de dispositivos.
   - Para dispositivos gerenciados: **Gerenciamento de ativos** → **Dispositivos gerenciados**.
   - Para dispositivos não atribuídos: **Gerenciamento de ativos** → **Dispositivos não atribuídos**.
2. Na lista de dispositivos, clique no link com o nome do dispositivo desejado e vá para a guia **Eventos**.
3. Selecione os eventos:
   - Se você quiser excluir um ou vários eventos, marque as caixas de seleção ao lado dele(s).
   - Se quiser excluir todos os eventos na página atual, marque a caixa de seleção acima da lista de eventos e clique na opção **Selecionar todos na página atual**.
   - Se quiser excluir todos os eventos de uma seleção, marque a caixa de seleção acima da lista de eventos e clique na opção **Selecionar tudo**.
4. Clique em **Excluir** e confirme a ação.
5. Na janela exibida, clique em **Excluir**.

Os eventos selecionados são excluídos e não podem ser restaurados.

Excluir as seleções de eventos

Você pode excluir apenas as seleções de eventos definidas pelo usuário. As seleções de eventos predefinidas não podem ser excluídas.

Para excluir uma ou várias seleções de eventos:

1. No menu principal, acesse **Monitoramento** → **Seleções de eventos**.
2. Marque as caixas de seleção ao lado das seleções de eventos que deseja excluir.
3. Clique no botão **Excluir**.
4. Na janela que se abre, clique em **OK**.

A seleção de eventos é excluída.

Configuração do termo de armazenamento de um evento

O Kaspersky Security Center Linux permite que o usuário receba informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nos dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração. Você pode precisar armazenar alguns eventos por um período maior ou menor do que o especificado pelos valores padrão. Você pode alterar as configurações padrão do período de armazenamento de um evento.

Se não desejar em armazenar alguns eventos no banco de dados do Servidor de Administração, poderá desativar a respectiva configuração na política do Servidor de Administração e na política do aplicativo Kaspersky, ou nas propriedades do Servidor de Administração (apenas para eventos do Servidor de Administração). Isso reduzirá o número de tipos de evento no banco de dados.

Quanto mais longo o prazo de armazenamento de um evento, mais rápido o banco de dados atingirá sua capacidade máxima. No entanto, um prazo de armazenamento mais longo de um evento permite executar tarefas de monitoramento e relatório por um período maior.

Para definir o prazo de armazenamento de um evento no banco de dados do Servidor de Administração:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política necessária.

   Você pode selecionar uma política de um aplicativo gerenciado, Agente de Rede ou Servidor de Administração da Kaspersky. Para o Servidor de Administração, também é possível configurar o período de armazenamento dos eventos ao clicar no nome do Servidor de Administração.
3. Selecione a guia **Configuração de eventos**.

   Uma lista de tipos de evento relacionados à seção **Crítico** é exibida. Se necessário, você pode mover para as seções **Falha funcional**, **Advertência** ou **Informações**.
4. Na lista de tipos de eventos no painel direito, clique no link do evento cujo prazo de armazenamento deseja alterar.

   Na seção **Registro de eventos** da janela, o botão de alternância **Armazenar no banco de dados do Servidor de Administração por (dias)** está ativado.
5. Na caixa de edição abaixo desse botão de alternar, insira o número de dias para armazenar o evento.
6. Caso não deseje armazenar um evento no banco de dados do Servidor de Administração, desative a opção **Armazenar no banco de dados do Servidor de Administração por (dias)**.

   > Se você configurar eventos do Servidor de Administração na janela de propriedades do Servidor de Administração e se as configurações do evento estiverem bloqueadas na política do Servidor de Administração, não será possível redefinir o valor do período de armazenamento para um evento.
7. Clique em **OK** e clique no botão **Salvar** quando o painel direito for fechado.

   A janela de propriedades da política é fechada.

A partir de agora, quando o Servidor de Administração receber e armazenar os eventos do tipo selecionado, eles terão o prazo de armazenamento alterado. O Servidor de Administração não altera o prazo de armazenamento de eventos recebidos anteriormente.

Bloqueio de eventos frequentes

Esta seção fornece informações sobre como gerenciar e remover o bloqueio de eventos frequentes.

Sobre o bloqueio de eventos frequentes

Um aplicativo gerenciado, por exemplo, Kaspersky Endpoint Security for Linux, instalado em um ou vários dispositivos gerenciados, pode enviar muitos eventos do mesmo tipo ao Servidor de Administração. Receber eventos frequentes pode sobrecarregar o banco de dados do Servidor de Administração e sobrepor-se a outros eventos. O Servidor de Administração começa a bloquear os eventos mais frequentes quando o número de todos os eventos recebidos excede o limite especificado para o banco de dados.

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes. Você não pode bloquear os eventos frequentes ou escolher quais eventos bloquear.

Caso queira saber se um evento está bloqueado, é possível visualizar a lista de notificações ou visualizar se o evento está presente na seção **Bloqueando eventos frequentes** das propriedades do servidor de administração. Se o evento estiver bloqueado, você pode fazer o seguinte:

- Se deseja evitar a substituição do banco de dados, pode continuar bloqueando o recebimento desse tipo de evento.
- Se deseja, por exemplo, localizar o motivo do envio de eventos frequentes ao Servidor de Administração, pode desbloquear os eventos frequentes e continuar recebendo os eventos deste tipo de qualquer maneira.
- Se quiser continuar recebendo os eventos frequentes até que sejam bloqueados novamente, pode remover o bloqueio dos eventos frequentes.

Gerenciando o bloqueio de eventos frequentes

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes, mas você pode desbloquear e continuar a recebê-los. Você também pode bloquear o recebimento de eventos frequentes que desbloqueou anteriormente.

Para gerenciar o bloqueio de eventos frequentes:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Bloquear eventos frequentes**.

3. Na seção **Bloquear eventos frequentes**:

   - Se deseja desbloquear o recebimento de eventos frequentes:

     a. Selecione os eventos frequentes que deseja desbloquear e clique no botão **Excluir**.

     b. Clique no botão **Salvar**.

   - Se deseja bloquear o recebimento de eventos frequentes:

     a. Selecione os eventos frequentes que deseja bloquear e clique no botão **Bloquear**.

     b. Clique no botão **Salvar**.

O Servidor de Administração recebe os eventos frequentes desbloqueados e não recebe os eventos frequentes bloqueados.

Removendo o bloqueio de eventos frequentes

Você pode remover o bloqueio de eventos frequentes e começar a recebê-los até que o Servidor de Administração os bloqueie novamente.

Para remover o bloqueio de eventos frequentes:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Bloquear eventos frequentes**.

3. Na seção **Bloquear eventos frequentes**, selecione os tipos de eventos frequentes os quais deseja remover o bloqueio.

4. Clique no botão **Remover do bloqueio.**

O evento frequente é removido da lista de eventos frequentes. O Servidor de Administração receberá eventos deste tipo.

Processamento e armazenamento do evento no Servidor de Administração

As informações sobre eventos durante a operação do aplicativo gerenciado e de dispositivos gerenciados são salvas no banco de dados do Servidor de Administração. Cada evento é atribuído a um determinado tipo e nível de gravidade (*Evento crítico*, *Falha funcional*, *Advertência* ou *Informativo*). Dependendo das condições sob as quais um evento ocorreu, o aplicativo pode atribuir diferentes níveis de gravidade aos eventos do mesmo tipo.

Você pode visualizar os tipos e níveis de gravidade atribuídos aos eventos na seção **Configuração do evento** da janela Propriedades do Servidor de Administração. Na seção **Configuração do evento**, você também poderá configurar o processamento de cada evento pelo Servidor de Administração:

- O registro de eventos no Servidor de Administração e nos registros de evento do sistema operacional em um dispositivo cliente e no Servidor de Administração.
- Método usado para notificar o administrador sobre um evento (por exemplo, um SMS ou mensagem de e-mail).

Na seção **Repositório de eventos** da janela Propriedades do Servidor de Administração, você pode editar as configurações de armazenamento do evento no banco de dados do Servidor de Administração ao limitar o número de registros de evento ou o tempo de armazenamento do registro. Quando você especifica o número máximo de eventos, o aplicativo calcula um volume aproximado do espaço de armazenamento necessário para o número especificado. Você pode usar esse cálculo aproximado para avaliar se você tem espaço livre suficiente no disco para evitar sobrecarga do banco de dados. A capacidade padrão do banco de dados do Servidor de Administração é de 400.000 eventos. A capacidade máxima recomendada do banco de dados é de 45 milhões de eventos.

O aplicativo verifica o banco de dados a cada 10 minutos. Caso o número de eventos atinja o valor máximo especificado em mais de 10.000, o aplicativo exclui os eventos mais antigos para que apenas o número máximo de eventos especificado permaneça.

Quando o Servidor de Administração exclui eventos antigos, não pode salvar novos eventos no banco de dados. Durante esse período, as informações sobre eventos rejeitados são gravadas no log do sistema operacional. Os novos eventos são colocados em fila e salvos no banco de dados depois que a operação de exclusão é concluída. Por padrão, a fila de eventos é limitada a 20 mil eventos. É possível personalizar o limite da fila ao editar o valor do sinalizador KLEVP_MAX_POSTPONED_CNT.

Notificações e status do dispositivo

Esta seção contém informações sobre como visualizar notificações, configurar a entrega de notificações, usar os status do dispositivo e habilitar a alteração de status do dispositivo.

Sobre notificações

As notificações informam sobre eventos importantes e ajudam você a responder rapidamente a eles executando as ações recomendadas ou outras ações apropriadas.

Dependendo do método de notificação selecionado, os seguintes tipos de notificações estão disponíveis:

- Notificações na tela
- Notificações por SMS
- Notificações por e-mail
- Notificações por arquivo executável ou script

Notificações na tela

As notificações na tela estão disponíveis no painel suspenso que é aberto ao clicar no ícone de notificações ( ) e no Centro de notificações. Elas recebem uma das seguintes categorias de importância: **Crítico**, **Advertência** ou **Informações**.

Se o ícone de notificações tiver um ponto vermelho, há notificações não lidas.

As notificações na tela são agrupadas nos seguintes tipos:

- **Exigem atenção**

  Notificações que requerem sua atenção. As notificações da categoria **Crítico** são exibidas no painel principal, além de serem exibidas no Centro de notificações.

- **Sistema**

  Notificações do sistema. Elas são divididas nas seguintes categorias:

  - **Implementação**
  - **Dispositivos**
  - **Proteção**
  - **Atualizações** (inclui notificações sobre aplicativos da Kaspersky disponíveis para download, notificações sobre atualizações de banco de dados do antivírus baixadas e notificações sobre dispositivos, se houver, que precisam ser reiniciados após uma atualização do Agente de Rede)
  - **Prevenção de Exploits**
  - **Servidor de Administração** (inclui somente eventos relacionados ao Servidor de Administração)

- **Comunicados**

  Notificações que fornecem informações relacionadas à sua versão do Kaspersky Security Center Linux e aos aplicativos gerenciados instalados nos dispositivos gerenciados.

Você pode monitorar a rede da sua organização visualizando notificações na tela e dando resposta a elas em tempo real.

Notificações por e-mail, por SMS e por arquivo executável ou um script

O Kaspersky Security Center Linux oferece a capacidade de controlar a rede da sua organização enviando notificações sobre qualquer evento que você considera importante. Para qualquer evento, você pode configurar notificações por e-mail, SMS ou executando um arquivo executável ou um script.

Para receber notificações por e-mail ou SMS, você pode decidir a sua resposta para um evento. Essa resposta deve ser a mais apropriada para a rede da sua organização. Executando um arquivo executável ou um script, você predefine uma resposta para um evento. Você também pode considerar a execução de um arquivo executável ou um script como uma resposta primária para um evento. Após a execução do arquivo executável, você pode tomar outras medidas para responder ao evento.

Visualizar notificações que exigem atenção

As notificações que requerem atenção informam sobre eventos que podem exigir sua atenção. Elas recebem uma das seguintes categorias de importância: **Crítico**, **Advertência** ou **Informações**.

As notificações da categoria **Crítico** são exibidas na Web Console e no Centro de Notificações. Se houver várias notificações críticas, a Web Console exibirá uma única notificação com o número total de notificações críticas.

Você pode visualizar as notificações que requerem atenção de uma das seguintes maneiras:

- No painel suspenso

  Somente as notificações não lidas que requerem atenção são exibidas no painel suspenso. Se não houver notificações não lidas que requeiram atenção, a guia **Exigem atenção** não será exibida.

- No Centro de Notificações

  O Centro de Notificações exibe todas as notificações que requerem atenção, tanto lidas quanto não lidas. Se não houver notificações que requeiram atenção, a guia **Exigem atenção** não será exibida.

Para visualizar as notificações que requerem atenção no painel suspenso:

1. Na parte superior da Web Console, clique no ícone de notificação ( ).

   O painel suspenso **Notificações** será aberto.

2. Na guia **Exigem atenção**, visualize as notificações não lidas.

3. Se necessário, marque as notificações que requerem atenção como lidas de uma das seguintes maneiras:

   - Para marcar uma notificação como lida, clique no ícone de fechar (×) ao lado da notificação.

   - Para marcar todas as notificações como lidas, clique em **Marcar tudo como lido**.

Depois de revisar as notificações que requerem atenção e marcá-las como lidas, a guia **Exigem atenção** não será mais exibida no painel suspenso **Notificações**. Você pode visualizar no Centro de Notificações todas as notificações lidas que requerem atenção.

Para visualizar as notificações que requerem atenção no Centro de Notificações:

1. Na parte superior da Web Console, clique no ícone de notificação ( ).

2. No painel suspenso **Notificações** que é aberto, clique no botão **Ir para a Central de Notificações**.

   A janela **Central de Notificações** se abre.

3. Na guia **Exigem atenção**, selecione uma das seguintes seções:

   - **Todas as notificações que exigem atenção** – Exibe todas as notificações que requerem atenção, independentemente da categoria.
   - **Crítico** – Exibe as notificações da categoria **Crítico**.
   - **Advertência** – Exibe as notificações da categoria **Advertência**.
   - **Informações** – Exibe as notificações da categoria **Informações**.

4. Para exibir somente as notificações não lidas, ative o botão de alternância **Mostrar apenas não lidas**.
5. Na lista de notificações, clique em uma notificação para visualizar a mensagem correspondente. A notificação completa é exibida no painel de detalhes à direita.

   Quando você visualiza uma notificação, ela é automaticamente marcada como lida.

6. Para marcar as notificações como lidas manualmente, execute uma das seguintes ações:

   - Para marcar uma notificação como lida, selecione-a na lista de notificações e clique no botão **Marcar como lida**.
   - Para marcar todas as notificações como lidas, clique no botão **Marcar tudo como lido**.

7. Se necessário, você pode marcar uma notificação como não lida selecionando-a na lista de notificações e clicando no botão **Marcar como não lida**.

As notificações que requerem atenção são revisadas.

Visualizar notificações do sistema

As notificações do sistema informam sobre eventos relacionados ao Web Console e aos dispositivos gerenciados. As notificações do sistema são agrupadas por tipo e recebem uma das seguintes categorias de importância: **Crítico**, **Advertência** ou **Informações**.

Você pode visualizar as notificações do sistema de uma das seguintes maneiras:

- No painel suspenso
- No Centro de Notificações

Para visualizar as notificações do sistema no painel suspenso:

1. Na parte superior da Web Console, clique no ícone de notificação ( ).

   O painel suspenso **Notificações** será aberto.

2. Na guia **Sistema**, visualize as notificações não lidas.

3. Se necessário, marque as notificações do sistema como lidas de uma das seguintes maneiras:

   - Para marcar uma notificação como lida, clique no ícone de fechar (×) ao lado da notificação.
   - Para marcar todas as notificações como lidas, clique em **Marcar tudo como lido**.

Depois de revisar todas as notificações do sistema e marcá-las como lidas, o painel suspenso **Notificações** exibe uma mensagem indicando que não há novas notificações. Você pode visualizar todas as notificações do sistema, tanto as lidas quanto as não lidas, no Centro de notificações.

Para visualizar as notificações do sistema no Centro de notificações:

1. Na parte superior da Web Console, clique no ícone de notificação (🔔).
2. No painel suspenso **Notificações** que é aberto, clique no botão **Ir para a Central de Notificações**.

   A janela **Central de Notificações** se abre.
3. Na guia **Sistema**, selecione uma das seguintes seções:

   - **Todas as notificações do sistema**
   - **Implementação**
   - **Dispositivos**
   - **Proteção**
   - **Atualizações**
   - **Prevenção de Exploits**
   - **Servidor de Administração**
4. Para exibir somente as notificações não lidas, ative o botão de alternância **Mostrar apenas não lidas**.
5. Na lista de notificações, clique em uma notificação para visualizar a mensagem correspondente. A notificação completa é exibida no painel de detalhes à direita.

   Quando você visualiza uma notificação, ela é automaticamente marcada como lida.
6. Para marcar as notificações como lidas manualmente, execute uma das seguintes ações:

   - Para marcar uma notificação como lida, selecione-a na lista de notificações e clique no botão **Marcar como lida**.
   - Para marcar todas as notificações como lidas, clique no botão **Marcar tudo como lido**.
7. Se necessário, você pode marcar uma notificação como não lida selecionando-a na lista de notificações e clicando no botão **Marcar como não lida**.

As notificações do sistema foram revisadas.

Visualizar informativos

Os comunicados são um tipo de notificação que fornece informações sobre sua versão do Kaspersky Security Center Linux e os aplicativos Kaspersky instalados nos dispositivos gerenciados. Somente os comunicados relevantes para o Servidor de Administração conectado no momento e para os aplicativos Kaspersky instalados nos dispositivos gerenciados desse Servidor de Administração são exibidos. Os comunicados são exibidos separadamente para cada Servidor de Administração, seja ele primário, secundário ou virtual.

Se vários administradores usam o Kaspersky Security Center Linux e definem diferentes idiomas de interface, o Kaspersky Security Center Linux exibe os comunicados Kaspersky em todos os idiomas usados pelos administradores. Ao alterar o idioma da interface, os comunicados Kaspersky no idioma selecionado são adicionados à seção automaticamente, após você sair da Web Console e entrar novamente.

Os comunicados incluem os seguintes tipos de informações:

- Informações relacionadas à segurança

  Os comunicados relacionados à segurança incluem atualizações críticas, correções de vulnerabilidades e recomendações para resolver problemas nos aplicativos Kaspersky. Informativos relacionados à segurança são ativados por padrão. Se não deseja receber os comunicados relacionados à segurança, pode desativar este recurso.

  Você não pode desativar os comunicados relacionados à segurança no modo de avaliação do Kaspersky Security Center Linux.

  Para fornecer informações relevantes à sua configuração de proteção de rede, o Kaspersky Security Center Linux envia dados aos servidores em nuvem da Kaspersky e recebe apenas comunicados relacionados aos aplicativos Kaspersky instalados na rede. Os dados que podem ser enviados aos servidores são descritos no Contrato de Licença de Usuário Final aceito por você ao instalar o Kaspersky Security Center Linux.

- Informações de marketing

  Os comunicados de marketing incluem ofertas especiais, notícias sobre produtos e anúncios relacionados aos aplicativos Kaspersky. Os comunicados de marketing estão disponíveis somente se a Kaspersky Security Network (KSN) estiver ativada. Você pode desativar os informativos de marketing desativando a KSN.

  Para fornecer informações que podem ajudar você a proteger seus dispositivos de rede e realizar tarefas diárias, o Kaspersky Security Center Linux envia dados aos servidores em nuvem da Kaspersky e recebe comunicados relevantes. Os dados que podem ser enviados aos servidores são descritos na seção Dados processados da Declaração da KSN.

Os comunicados são atribuídos a uma das seguintes categorias de importância: **Crítico**, **Advertência** ou **Informações**.

Você pode visualizar os comunicados de uma das seguintes maneiras:

- No painel suspenso
- No Centro de Notificações

Para visualizar os comunicados no painel suspenso:

1. Na parte superior da Web Console, clique no ícone de notificação ( ).

   O painel suspenso **Notificações** será aberto.

2. Na guia **Comunicados**, visualize as notificações não lidas.

3. Se necessário, marque as notificações como lidas de uma das seguintes maneiras:

   - Para marcar uma notificação como lida, clique no ícone de fechar (×) ao lado da notificação.
   - Para marcar todas as notificações como lidas, clique em **Marcar tudo como lido**.

Depois de revisar todas as notificações e marcá-las como lidas, o painel suspenso **Notificações** exibe uma mensagem indicando que não há novas notificações. Você pode visualizar todas as notificações, lidas e não lidas, no Centro de notificações.

Para visualizar os comunicados no Centro de notificações:

1. Na parte superior da Web Console, clique no ícone de notificação ( ).

2. No painel suspenso **Notificações** que é aberto, clique no botão **Ir para a Central de Notificações**.

   A janela **Central de Notificações** se abre.

3. Na guia **Comunicados**, selecione uma das seguintes seções:

   - **Todos os anúncios** – Exibe todas as notificações, independentemente da categoria.
   - **Crítico** – Exibe as notificações da categoria **Crítico**.
   - **Advertência** – Exibe as notificações da categoria **Advertência**.
   - **Informações** – Exibe as notificações da categoria **Informações**.

4. Para exibir somente as notificações não lidas, ative o botão de alternância **Mostrar apenas não lidas**.

5. Na lista de notificações, clique em uma notificação para visualizar a mensagem correspondente. A notificação completa é exibida no painel de detalhes à direita.

   Quando você visualiza uma notificação, ela é automaticamente marcada como lida.

6. Para marcar as notificações como lidas manualmente, execute uma das seguintes ações:

   - Para marcar uma notificação como lida, selecione-a na lista de notificações e clique no botão **Marcar como lida**.
   - Para marcar todas as notificações como lidas, clique no botão **Marcar tudo como lido**.

7. Se necessário, você pode marcar uma notificação como não lida selecionando-a na lista de notificações e clicando no botão **Marcar como não lida**.

Os anúncios são revisados.

Desativando o recebimento de Novidades Kaspersky

A seção Novidades Kaspersky (**Monitoramento → Novidades Kaspersky**) apresenta as últimas novidades sobre a sua versão do Kaspersky Security Center Linux e sobre os aplicativos gerenciados e instalados nos dispositivos gerenciados. Se não deseja receber informações de novidades sobre a Kaspersky, pode desativar este recurso.

Os informativos da Kaspersky incluem dois tipos de informações: informativos relacionados à segurança e de marketing.

Para desativar informativos relacionados à segurança:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Novidades Kaspersky**.

3. Use o botão de alternância para mudar para a posição **Novidades relacionadas à segurança** estão desativadas.

4. Clique no botão **Salvar**.

   O recebimento de novidades sobre a Kaspersky está desativado.

Informativos de marketing estão desativados por padrão. Você recebe informativos de marketing apenas se ativou a Kaspersky Security Network (KSN). Você pode desativar este tipo de informativo desativando a KSN.

A desativação da KSN pode afetar os aplicativos gerenciados da Kaspersky que usam os serviços da KSN. Esses aplicativos podem não conseguir mais se comunicar com a Kaspersky para enviar ou receber dados de reputação, telemetria ou estatísticas.

Configurar a alternância dos status do dispositivo

Você pode alterar as condições para atribuir o status *Crítico* ou *Advertência* para um dispositivo.

Para ativar a alteração do status do dispositivo para Crítico:

1. No menu principal, vá para **Gerenciamento de ativos → Hierarquia de grupos**.

2. Vá para as propriedades do grupo de administração para o qual você deseja alterar os status do dispositivo de uma das seguintes formas:

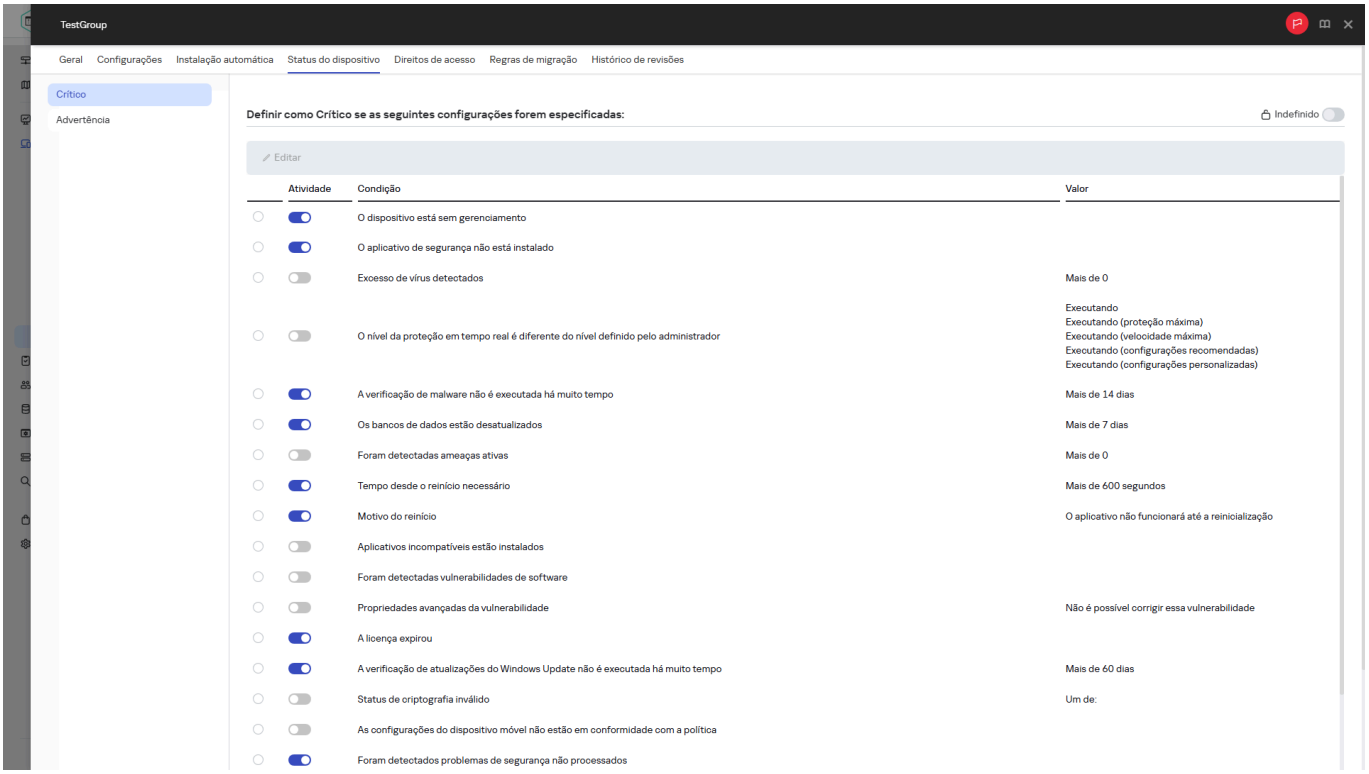
   - Clique no nome do grupo de administração.
   - Clique no botão **Mostrar a hierarquia** na parte superior da página. No painel de navegação exibido, passe o cursor do mouse sobre o nome do grupo desejado e clique no ícone de configurações (⚙).

   A janela Propriedades do grupo de administração é aberta.

3. Na janela de propriedades, selecione a guia **Status do dispositivo**.

4. No painel esquerdo, selecione **Crítico**.

5. No painel direito, na seção **Definir como Crítico se as seguintes configurações forem especificadas**, ative a condição para alterar o status de um dispositivo para *Crítico*.



No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.
9. Clique em **OK**.
10. Clique em **Salvar** para salvar as alterações.

Quando condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Crítico*.

Para ativar a alteração do status do dispositivo para Advertência:

1. No menu principal, vá para **Gerenciamento de ativos** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Advertência**.

5. No painel direito, na seção **Definir como Advertência se as seguintes configurações forem especificadas**, ative a condição para alterar o status de um dispositivo para *Advertência*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.

9. Clique em **OK**.
10. Clique em **Salvar** para salvar as alterações.

Quando as condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Advertência*.

Configurar a entrega de notificações

Você pode configurar a notificação sobre eventos que ocorrem no Kaspersky Security Center Linux. Dependendo do método de notificação selecionado, os seguintes tipos de notificações estão disponíveis:

- E-mail – Sempre que ocorre um evento, Kaspersky Security Center Linux envia uma notificação para os endereços de e-mail especificados.
- SMS – Sempre que ocorre um evento, Kaspersky Security Center Linux envia uma notificação para os números de telefone especificados.
- Arquivo executável – sempre que ocorre um evento, o arquivo executável é executado no Servidor de Administração.

Para configurar a entrega de notificação de eventos que ocorrem no Kaspersky Security Center Linux:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Clique na seção **Notificação** e, no painel direito, selecione a guia do método de notificação desejado:

   - **E-mail**

     A guia **E-mail** permite-lhe configurar a notificação do evento por e-mail.

     No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

     - Endereço IPv4 ou IPv6
     - Nome de DNS do servidor SMTP

     No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Se você ativar a opção **Usar consulta de DNS MX**, pode usar vários registros MX dos endereços IP para o mesmo nome DNS do servidor SMTP. O mesmo nome DNS pode ter vários registros de MX com valores diferentes de prioridade de recebimento de mensagens de e-mail. O Servidor de Administração tenta enviar notificações por e-mail ao servidor SMTP em ordem crescente de prioridade dos registros MX.

Se você ativar **Usar consulta de DNS MX** e não ativar o uso de configurações TLS, recomendamos que use as configurações DNSSEC em seu dispositivo de servidor como uma medida adicional de proteção para o envio de notificações por e-mail.

Caso a opção **Usar a autenticação ESMTP** seja ativada, será possível especificar as configurações de autenticação ESMTP nos campos **Nome do usuário** e **Senha**. Por padrão, a opção estiver desativada, e as configurações da autenticação ESMTP não estão disponíveis.

Você pode especificar as configurações de TLS de conexão com um servidor SMTP:

- **Não usar TLS**

Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.

- **Usar TLS se compatível com servidor SMTP**

Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.

- **Sempre usar TLS e verificar a validade do certificado do servidor**

Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se você selecionar o valor **Sempre usar TLS e verificar a validade do certificado do servidor**, pode especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar certificados para uma conexão TLS clicando no link **Especificar certificados**:

- Procurar por um arquivo de certificado do servidor SMTP:

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center Linux verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center Linux não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

- Procurar um arquivo de certificado de cliente:

Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer CA confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

- Certificado X-509:

Você deve especificar um arquivo com o certificado e um arquivo com a chave privada. Os dois arquivos são independentes um do outro. A ordem em que os arquivos são carregados não importa. Quando os dois arquivos são carregados, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- Contêiner pkcs12:

Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

Clicar no botão **Enviar mensagem de teste** permite verificar se você configurou as notificações apropriadamente: o aplicativo envia uma notificação de teste aos endereços de e-mail que você especificou.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula.

No campo **Assunto**, insira o assunto do e-mail usando parâmetros de substituição, por exemplo: `[KSC-SAMARA-1] [%SEVERITY%] %EVENT%`. Exemplo de como fica a linha de assunto no caso de uma ameaça detectada: `[KSC-SAMARA-1] [Critical] Threat detected`. Você pode deixar este campo vazio.

Na lista suspensa **Modelo de assunto**, selecione o modelo do seu assunto. Uma variável determinada pelo modelo selecionado é colocada automaticamente no campo **Assunto**. Você pode criar um assunto de e-mail selecionando vários modelos de assunto.

No campo **Endereço de e-mail do remetente: se essa configuração não for especificada, o endereço do destinatário será usado em vez disso. Advertência: não é recomendável usar um endereço de e-mail fictício**, especifique o endereço de e-mail do remetente. Se você deixar este campo vazio, por padrão, o endereço do destinatário é usado. Não é recomendável usar endereços de e-mail fictícios.

O campo **Mensagem de notificação** contém o texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto inclui parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio. Você pode editar o texto da mensagem adicionando outros parâmetros substitutos com detalhes mais relevantes sobre o evento.

Exemplo de valor do campo

```
Sender - KSC-SAMARA-1

Host: %COMPUTER%

Product: %KL_PRODUCT%

Version: %KL_VERSION%

Occurred at: %RISE_TIME%

Event: %EVENT%

Details:

%DESCR%
```

A string `Sender` é opcional. Por exemplo, se você tiver vários Servidores de Administração, poderá especificar o nome do Servidor de Administração do qual a notificação foi recebida: `Sender - KSC-SAMARA-1`.

Exemplo de como o texto da notificação é exibido:

```
Sender - KSC-SAMARA-1

Host: nb-123456.example.net

Product: Kaspersky Endpoint Security 12.5 for Linux
```

```
Version: 12.5.0.1569

Occurred at: 2026-08-17T13:15:36

Event: Threat detected

Details:

Initiator: Product; Task type: ODS; ID of running task: 107; User receiving access:
root; Object type: File; File owner: user; Detection certainty: Sure; File:
/home/user/eicar_com.zip//eicar.com; Detected object name: EICAR-Test-File; Detected
object type: Virware; MD5 hash: <hash>; Unique ID: <ID>
```

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clicar no link **Configurar limite numérico de notificações** permite-lhe especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

- **SMS**

A guia **SMS** permite-lhe configurar a transmissão de notificações por SMS de vários eventos para um telefone celular. As mensagens SMS são enviadas por meio de um gateway de correio.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome da rede Windows (nome NetBIOS) do dispositivo
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Caso a opção **Usar a autenticação ESMTP** seja ativada, será possível especificar as configurações de autenticação ESMTP nos campos **Nome do usuário** e **Senha**. Por padrão, a opção estiver desativada, e as configurações da autenticação ESMTP não estão disponíveis.

Você pode especificar as configurações de TLS de conexão com um servidor SMTP:

- **Não usar TLS**

Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.

- **Usar TLS se compatível com servidor SMTP**

Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.

- **Sempre usar TLS e verificar a validade do certificado do servidor**

Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se você selecionar o valor **Sempre usar TLS e verificar a validade do certificado do servidor**, pode especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar o arquivo de certificado do servidor SMTP clicando no link **Especificar certificados**:

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center Linux verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center Linux não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula. As notificações serão entregues aos números de telefone associados aos endereços de e-mail especificados.

No campo **Assunto**, especifique o assunto do e-mail.

Na lista suspensa **Modelo de assunto**, selecione o modelo do seu assunto. Uma variável segundo o modelo selecionado é inserida no campo **Assunto**. Você pode criar um assunto de e-mail selecionando vários modelos de assunto.

No campo **Endereço de e-mail do remetente: se essa configuração não for especificada, o endereço do destinatário será usado em vez disso. Advertência: não é recomendável usar um endereço de e-mail fictício**, especifique o endereço de e-mail do remetente. Se você deixar este campo vazio, por padrão, o endereço do destinatário é usado. Não é recomendável usar endereços de e-mail fictícios.

No campo **Números de telefone dos destinatários de mensagens SMS**, especifique os números de celular dos destinatários da notificação de SMS.

O campo **Mensagem de notificação**, especifique um texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto pode incluir parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio.

> Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clique no link **Configurar limite numérico de notificações** para especificar a quantidade máxima de notificações que o aplicativo pode enviar ao longo do intervalo de tempo especificado.

Clique em **Enviar mensagem de teste** para verificar se você configurou as notificações adequadamente: o aplicativo envia uma notificação de teste ao destinatário especificado.

- **Arquivo executável a ser executado**

  O arquivo executável deve conter as variáveis de ambiente do evento que você deseja que o Administrador receba.

  No campo **O arquivo executável que será executado no Servidor de Administração quando um evento ocorrer**, especifique a pasta e o nome do arquivo a ser executado.

  Exemplo de valor de campo:

  ```
  /opt/scripts/notifications.sh
  ```

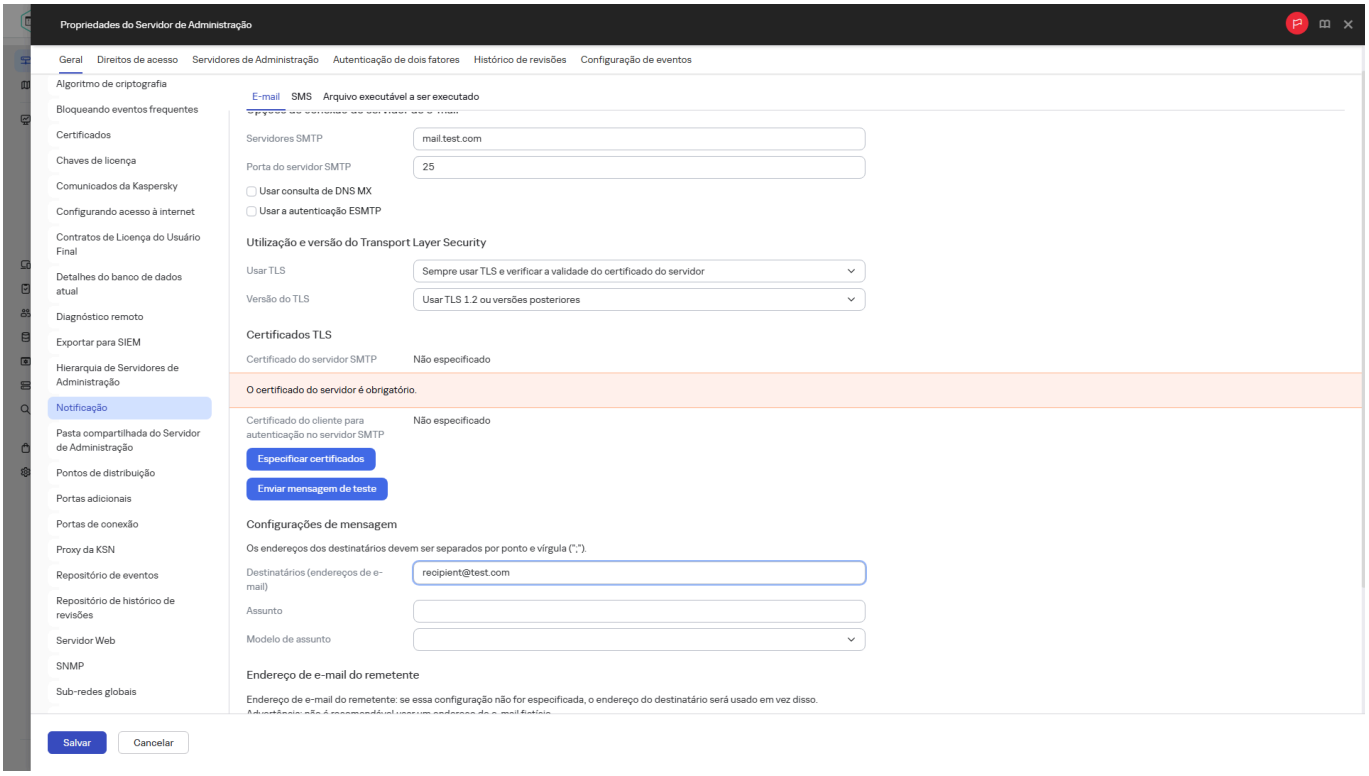
  O arquivo deve ser preparado com antecedência, especificando parâmetros de substituição que representam as informações do evento que serão enviadas na mensagem. A pasta e o arquivo devem estar localizados no Servidor de Administração.

  Exemplo de script para teste ou depuração:

  ```
  #!/usr/bin/env bash
  touch /tmp/ksc_notification.txt
  ```

```
echo "$RISE_TIME $COMPUTER $EVENT" >> /tmp/ksc_notification.txt
```

Clicar no link **Configurar limite numérico de notificações** permite-lhe especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.



Seleção do método de notificação

3. Na guia, defina as configurações de notificação.

4. Clique em **Salvar** para salvar as alterações e fechar a janela de propriedades do Servidor de Administração.

   As configurações de entrega de notificação salvas são aplicadas a todos os eventos que ocorrem no Kaspersky Security Center Linux.

Você pode ignorar as configurações de entrega de notificações para certos eventos na seção **Configuração de eventos** das configurações do Servidor de Administração, de uma política ou de um aplicativo.

Testar as notificações

Para verificar se as notificações de eventos foram enviadas, o aplicativo usa a notificação da detecção de vírus de teste EICAR em dispositivos cliente.

Para verificar o envio das notificações de eventos:

1. Interrompa a tarefa de proteção em tempo real do sistema de arquivos no dispositivo cliente e copie o vírus de teste EICAR para o dispositivo cliente. Em seguida, ative novamente a proteção em tempo real no sistema de arquivos.

2. Execute uma tarefa de verificação para dispositivos cliente em um grupo de administração ou para dispositivos específicos, inclusive um com o vírus EICAR.

   Se a tarefa de verificação estiver configurada corretamente, o vírus de teste será detectado. Se as notificações estiverem configuradas corretamente, você será notificado que um vírus foi detectado.

Para abrir um registro da detecção de vírus de teste:

1. No menu principal, vá para **Monitoramento → Seleções de eventos**.
2. Clique no nome da seleção **Eventos recentes**.

   A notificação sobre o vírus de teste é exibida na janela que se abre.

O vírus de teste de EICAR não contém nenhum código que possa danificar seu dispositivo. No entanto, a maioria dos aplicativos de segurança de fabricantes identifica esse arquivo como um vírus. É possível fazer download do vírus de teste no site oficial da EICAR.

Sobre os status do dispositivo

O Kaspersky Security Center Linux atribui um status a cada dispositivo gerenciado. O status específico depende se as condições definidas pelo usuário são atendidas. Em alguns casos, ao atribuir um status a um dispositivo, o Kaspersky Security Center Linux leva em consideração o sinalizador de visibilidade do dispositivo na rede (consulte a tabela abaixo). Por exemplo, se um dispositivo gerenciado recebeu o status *Crítico* porque a condição *Os bancos de dados estão desatualizados* foi atendida e, posteriormente, o sinalizador de visibilidade foi definido para esse dispositivo, ele passa a receber o status *OK*. Se o Kaspersky Security Center Linux não encontrar um dispositivo na rede dentro de duas horas, o sinalizador de visibilidade do dispositivo será definido como *Não visível*.

Os status são os seguintes:

- *Crítico* ou *Crítico/Visível*
- *Advertência* ou *Advertência/Visível*
- *OK* ou *OK/Visível*

A tabela abaixo lista as condições padrão que devem ser atendidas para atribuir o status *Crítico* ou *Advertência* a um dispositivo, com todos os valores possíveis.

Condições para atribuir um status a um dispositivo

Condição	Descrição da condição	Valores disponíveis
O aplicativo de segurança não está instalado	O Agente de Rede é instalado no dispositivo, mas um aplicativo de segurança não é instalado.	• O botão de alternar é ativado. • O botão de alternar é desativado.
Excesso de vírus detectados	Alguns vírus foram encontrados no dispositivo por uma tarefa de detecção de vírus, por exemplo, a tarefa de verificação de malware, e o número de vírus encontrados excede o valor especificado.	Mais de 0.
O nível da proteção em tempo real é diferente do nível definido pelo administrador	O dispositivo está visível na rede, mas o nível de proteção em tempo real difere do nível definido (na condição) pelo administrador para o status do dispositivo.	• Parado. • Suspenso. • Executando.
A verificação de malware não é executada há muito tempo	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas nem a tarefa de *verificação de malware* nem a verificação local foram executadas dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 7 dias ou antes.	Mais de 1 dia.
Os bancos de dados estão desatualizados	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas os bancos de dados antivírus não foram atualizados neste dispositivo dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 1 dia ou antes.	Mais de 1 dia.

Condição	Descrição da condição	Valores disponíveis
Não conectado há muito tempo	O Agente de Rede está instalado no dispositivo, mas o dispositivo não se conectou a um Servidor de Administração dentro do intervalo de tempo especificado, porque o dispositivo estava desativado.	Mais de 1 dia.
Foram detectadas ameaças ativas	O número de objetos não processados na pasta **Ameaças ativas** excede o valor especificado.	Mais de 0 itens.
Tempo desde o reinício necessário	O dispositivo está visível na rede, mas um aplicativo está aguardando uma reinicialização por mais tempo do que o intervalo de tempo especificado.	Mais de 0 minuto.
Motivo do reinício	O dispositivo está visível na rede, mas um aplicativo requer a reinicialização do dispositivo por um dos motivos selecionados.	• Motivo desconhecido • O aplicativo não funcionará até a reinicialização • É necessário reiniciar para concluir a atualização; o aplicativo está em execução • É necessário reiniciar para iniciar a atualização • É necessário reiniciar para concluir a verificação ou a desinfecção • A reinicialização é necessária para concluir a instalação/desinstalação remota • Concluindo a criptografia de dados no disco
Aplicativos incompatíveis estão instalados	O dispositivo está visível na rede, mas o inventário de software executado pelo Agente de Rede detectou aplicativos incompatíveis instalados no dispositivo.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Foram detectadas vulnerabilidades de software	O dispositivo está visível na rede, e o Agente de Rede está instalado no dispositivo, mas a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* detectou vulnerabilidades com o nível de gravidade especificado nos aplicativos instalados no dispositivo.	• Crítico. • Alto. • Médio. • Ignorar se a vulnerabilidade não puder ser corrigida. • Ignorar se uma atualização for atribuída para instalação.
A licença expirou	O dispositivo está visível na rede, mas a licença expirou.	• O botão de alternar é desativado. • O botão de alternar é ativado.
A licença expira em breve	O dispositivo está visível na rede, mas a licença expirará no dispositivo em tempo menor que o número especificado de dias.	Mais de 0 dias.

Condição	Descrição da condição	Valores disponíveis
A verificação de atualizações do Windows Update não é executada há muito tempo	O dispositivo está visível na rede, mas a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* não foi executada no intervalo de tempo especificado.	Mais de 1 dia.
Status de criptografia inválido	O Agente de Rede está instalado no dispositivo, mas o resultado da criptografia de dispositivo é igual ao valor especificado.	• Não está em conformidade com a política devido à recusa do usuário (somente para dispositivos externos). • Não está em conformidade com a política devido a um erro. • Reiniciar é necessário ao aplicar a política. • Nenhuma política de criptografia está especificada. • Sem suporte. • Ao aplicar a política.
As configurações do dispositivo móvel não estão em conformidade com a política	As configurações do dispositivo móvel são diferentes das especificadas na política do Kaspersky Endpoint Security for Android durante a verificação das regras de conformidade.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Foram detectados problemas de segurança não processados	Alguns problemas de segurança não processados foram encontrados no dispositivo. Os problemas de segurança podem ser criados automaticamente pelos aplicativos da Kaspersky gerenciados e instalados no dispositivo cliente ou manualmente pelo administrador.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Status do dispositivo definido pelo aplicativo	O status do dispositivo é definido pelo aplicativo gerenciado. Os dispositivos gerenciados podem ter um status definido por aplicativos gerenciados, independentemente das configurações do Kaspersky Security Center Linux. Depois que esse status retorna um dos status definidos pelo Kaspersky Security Center Linux, o Servidor Administração atribui ao dispositivo gerenciado o status mais crítico entre aqueles retornados pelo aplicativo gerenciado e o atribuído pelo próprio Servidor de Administração. Os status definidos pelos aplicativos gerenciados têm suas descrições transferidas por esses próprios aplicativos. Você pode visualizar essas descrições na lista de dispositivos gerenciados, na coluna **Descrição de status**.	• O botão de alternar é desativado. • O botão de alternar é ativado.
O dispositivo está com espaço em disco insuficiente	O espaço livre em disco no dispositivo é menor do que o valor especificado ou o dispositivo não pôde ser sincronizado com o Servidor de Administração. O status *Crítico* ou *Advertência* é alterado para o status *OK* quando o dispositivo é sincronizado com sucesso com o Servidor de Administração, e o espaço livre no dispositivo é maior que ou igual ao valor especificado.	Mais de 0 MB.
O dispositivo está sem gerenciamento	Durante a descoberta de dispositivos, o dispositivo foi reconhecido como visível na rede, mas houve falha em mais de três tentativas de sincronizar com o Servidor de Administração.	• O botão de alternar é desativado. • O botão de alternar é ativado.
A proteção está desativada	O dispositivo é visível na rede, mas o aplicativo de segurança no dispositivo foi desativado por um tempo mais longo do que o intervalo de tempo especificado. Nesse caso, o estado do aplicativo de segurança é *interrompido* ou *com falha* e diferente de: *iniciando*, *em execução* ou *suspenso*.	Mais de 0 minuto.
O aplicativo de segurança não está em execução	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas não está em execução.	• O botão de alternar é desativado. • O botão de alternar é ativado.

O Kaspersky Security Center Linux permite definir a troca automática do status de um dispositivo em um grupo de administração quando as condições especificadas forem atendida. Quando as condições especificadas forem atendidas, ao dispositivo cliente é atribuído um dos seguintes status: *Crítico* ou *Aviso*. Quando as condições especificadas não são atendidas, o dispositivo cliente recebe o status *OK*.

Diferentes status poderão corresponder a diferentes valores de uma condição. Por exemplo, por padrão, se a condição **Os bancos de dados estão desatualizados** possuir o valor **Mais de 3 dias**, o dispositivo cliente receberá o status *Advertência*. Se o valor for **Mais de 7 dias**, será atribuído o status *Crítico*.

Se você atualizar o Kaspersky Security Center Linux a partir da versão anterior, os valores da condição **Os bancos de dados estão desatualizados** para a atribuição do status *Crítico* ou *Advertência* não mudam.

Parâmetros e variáveis de ambiente para descrever um evento

Ao configurar notificações sobre eventos do Kaspersky Security Center Linux, você pode usar parâmetros e variáveis de ambiente para descrever os eventos (consulte a tabela abaixo).

Se você optou por executar um arquivo executável como método de notificação, use variáveis ao criar o arquivo.

Se quiser enviar notificações sobre eventos por e-mail ou SMS, você também pode especificar variáveis nos campos **Assunto** e **Mensagem de notificação** ao configurar as notificações na guia correspondente.

Parâmetros e variáveis de ambiente para descrever um evento

Parâmetro de substituição (para uso em notificações)	Variável de ambiente (para uso em scripts)	Descrição da variável do ambiente
%SEVERITY%	$SEVERITY	Gravidade do evento. Valores possíveis: • **Informações** • **Advertência** • **Erro** • **Crítico**
%COMPUTER%	$COMPUTER	Nome do dispositivo onde ocorreu o evento. O comprimento máximo do nome do dispositivo é de 256 caracteres.
%DOMAIN%	$DOMAIN	Nome de domínio do dispositivo onde o evento ocorreu.
%EVENT%	$EVENT	Nome do tipo de evento. O comprimento máximo do nome do tipo de evento é de 50 caracteres.
%DESCR%	$DESCR	Descrição de evento. O comprimento máximo da descrição é de mil caracteres.
%RISE_TIME%	$RISE_TIME	Tempo de criação do evento.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	$KLCSAK_EVENT_TASK_DISPLAY_NAME	Nome da tarefa. O comprimento máximo do nome da tarefa é de 100 caracteres.
%KL_PRODUCT%	$KL_PRODUCT	Nome do aplicativo.
%KL_VERSION%	$KL_VERSION	Número da versão do aplicativo.
%$KLCSAK_EVENT_SEVERITY_NUM%	$KLCSAK_EVENT_SEVERITY_NUM	Número da gravidade do evento. Valores possíveis: • 1 - **Informações** • 2 - **Advertência** • 3 - **Erro** • 4 - **Crítico**
%HOST_IP%	$HOST_IP	Endereço IP do dispositivo onde o evento ocorreu.
%HOST_CONN_IP%	$HOST_CONN_IP	Endereço IP da conexão do dispositivo onde o evento ocorreu.

Visualizando informações sobre detecção de ameaças

É possível ativar ou desativar a exibição de informações sobre alertas.

Depois de ativar o Servidor de Administração com uma licença do Kaspersky Extended Detection and Response Optimum ou do Kaspersky Next XDR Optimum, o Kaspersky Security Center Web Console exibe automaticamente a subseção **Alertas** na seção **Monitoramento** do menu principal.

*Para ativar ou desativar a exibição da seção **Alertas** no menu principal:*

1. No menu principal, vá para **Configurações** → **Opções da interface**.
2. Ative ou desative a opção **Mostrar alertas EDR**.
3. Clique no botão **Salvar**.

Quando a opção **Mostrar alertas EDR** está ativada, o console exibe a subseção **Alertas** na seção **Monitoramento** do menu principal. Na subseção **Alertas**, você pode ver informações sobre a detecção de ameaças nos dispositivos de endpoints.

Além disso, você pode adicionar um widget que exibe informações sobre alertas.

Para exibir corretamente as informações detalhadas sobre as ameaças detectadas no cartão de alerta, é necessário instalar o plug-in do Kaspersky Endpoint Agent e a versão compatível do plug-in do Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux 12.1 ou posterior, Kaspersky Endpoint Security for Mac 12.1 ou posterior, ou Kaspersky Endpoint Security for Windows 12.6 ou posterior).

Use o menu **Filtro** para filtrar alertas por data e valores de campo.

O campo **Tipo de objeto** contém os seguintes valores:

- desconhecido
- Link de phishing
- vírus
- Cavalo de Troia
- ferramenta maliciosa
- backdoor
- worm
- outro aplicativo
- Adware
- Pornware

- Programa perigoso empacotado
- Comportamento perigoso

O campo **Resposta automática** contém os seguintes valores:

- Objeto malicioso detectado
- Objeto excluído
- Objeto desinfectado
- Falha ao desinfectar o objeto
- Objeto colocado em quarentena
- Arquivo comprimido protegido por senha detectado
- Vírus detectado

Integrações para responder a alertas

Se tiver o licenciamento do Kaspersky Next XDR Optimum, poderá configurar integrações com as seguintes soluções para responder a ameaças:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Essas integrações estarão disponíveis se você tiver ativado o Servidor de Administração com uma licença do Kaspersky Next XDR Optimum.
Para executar ações de resposta, você deve implantar a chave de licença do Kaspersky Next XDR Optimum nos aplicativos gerenciados.
Ao usar a funcionalidade Kaspersky Next XDR Optimum com uma licença de avaliação, você deve primeiro adicionar um Servidor de Administração físico secundário, ativá-lo com a licença de avaliação e, depois, implantar a chave de licença nos dispositivos gerenciados por esse Servidor de Administração.

Se estiver usando o licenciamento do Kaspersky Next EDR Optimum, não é necessário ativar os aplicativos instalados nos dispositivos gerenciados sob o licenciamento do Kaspersky Next XDR Optimum. Isso deve ser feito apenas para novos dispositivos, se houver.

Como a licença do Kaspersky Next XDR Optimum permite a multilocação, você pode distribuir centralmente a chave de licença para aplicativos gerenciados. A distribuição automática da licença para Servidores de Administração secundários e virtuais não é compatível.

Para configurar as integrações, você deve ter os direitos **Ler** e **Gravar** para os **recursos Gerais: Área funcional Integração de aplicativos**.

Configurar a integração com o Active Directory para executar ações de resposta

A integração com o Active Directory permite executar ações de resposta para usuários do Active Directory afetados ou envolvidos no alerta.

Para configurar a integração com o Active Directory para responder a alertas, você deve usar o Servidor de Administração Kaspersky Security Center Linux versão 15.4 ou posterior.

A integração com o Active Directory para responder a alertas e as configurações para verificar o controlador de domínio do Active Directory (o endereço e as credenciais do usuário do controlador de domínio) especificadas ao configurar uma sondagem do controlador de domínio são duas configurações diferentes. Você deve garantir que o usuário para o qual uma ação de resposta deve ser executada tenha uma conta do Active Directory. Para isso, deve configurar ambas as integrações: para verificação e para responder. A ordem não é relevante.

As configurações de integração não são herdadas e são aplicadas somente ao Servidor de Administração (servidor físico ou virtual) no qual você define essas configurações.

Para configurar a integração com o Active Directory para responder a alertas:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Execute uma das seguintes ações:

   - Selecione a seção **Pontos de distribuição**, clique no nome do ponto de distribuição desejado e, na janela de propriedades exibida, selecione a seção **Active Directory**.

   - Selecione a seção **Resposta do Active Directory**.

3. No painel direito, ative o botão de alternância **Integração do Active Directory**.

   Posteriormente, se você quiser desativar a integração, só poderá fazê-lo para todas as conexões desativando o botão de alternância **Integração do Active Directory**. Você não pode desativar a integração para uma conexão separada. Em vez disso, pode excluir a conexão.

   > Ao ativar ou desativar o botão de alternância **Integração do Active Directory**, a configuração é aplicada tanto à seção **Resposta do Active Directory** quanto à seção **Pontos de distribuição**.

4. Crie uma conexão com o controlador de domínio do Active Directory, clicando no botão **Adicionar**.

5. Na janela aberta, especifique os seguintes parâmetros para a conexão:

   - **Endereço do controlador de domínio**

     Nome do computador, por exemplo: `server.mycompany.com`.

     Você pode especificar vários endereços. Todos os controladores de domínio cujos endereços você especificar devem pertencer ao mesmo domínio.

   - **Nome de domínio do Active Directory**

     Nome de domínio DNS totalmente qualificado, por exemplo: `mycompany.com`

Além disso, você pode especificar um nome SAM ou NetBIOS, por exemplo: `mycompany`

Use letras minúsculas. Se você criar várias conexões para o Servidor de Administração ou um ponto de distribuição, especifique nomes diferentes para cada conexão.

> Para executar ações de resposta, o nome de domínio do Active Directory especificado neste campo deve corresponder ao nome de domínio do Active Directory especificado no alerta.

- **Login**

  Login da conta do Active Directory com direitos de administrador sob os quais as ações de resposta devem ser executadas.

- **Senha**

  Senha da conta do Active Directory com direitos de administrador sob a qual as ações de resposta devem ser executadas.

6. Se quiser verificar o status da conexão, clique no botão **Verificar conexão**.

   Se a conexão for estabelecida com êxito, o status **Conectado** é exibido. Caso contrário, o status será **Falhou** e uma mensagem de erro será exibida com os controladores de domínio aos quais você não conseguiu se conectar.

> Você deve considerar como a conexão com o Active Directory é feita: **de um dispositivo Linux ou de um dispositivo Windows**.

Conectando via dispositivo Linux

Por padrão, ao conectar e autenticar em um controlador de domínio via um dispositivo Linux, a lógica é a seguinte:

1. O Servidor de Administração ou um ponto de distribuição tenta se conectar ao controlador de domínio através do LDAPS.

   A verificação rigorosa do certificado do servidor LDAP é executada.

2. Você deve colocar a parte pública do certificado do controlador de domínio no repositório de certificados do sistema para validar o certificado válido.

   O caminho dependente do SO para a autorização de certificação (CA) do sistema é usado para acessar a cadeia de certificados.

   Por exemplo:

   - /etc/ssl/certs/ca-certificates.crt — Caminho para sistemas operacionais baseados em Debian (Debian, Ubuntu, Astra).

   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — Caminho para CentOS ou Red Hat.

3. Se a conexão LDAPS falhar, ocorrerá um erro e nenhum outro protocolo de conexão será usado.

> Em caso de problemas com o LDAP, você pode entrar em contato com o Suporte Técnico da Kaspersky.

Se não quiser instalar o certificado no repositório de certificados do sistema, poderá usar o sinalizador KLNAG_LDAP_SSL_CACERT para definir o caminho para o certificado do controlador de domínio. Para isso, execute o comando:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

onde `</path/to/domain-controller/cert>` é o caminho para a parte pública do certificado do controlador de domínio.

Por exemplo, se o caminho for `"/var/opt/kaspersky/ldap_cert.crt"`, o comando será `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Conectando via dispositivo Windows

Ao conectar e autenticar em um controlador de domínio via um dispositivo Windows, as configurações de conexão são definidas pelo domínio.

Você deve garantir que:

- O LDAP está ativado e a porta 636 está disponível no dispositivo.
- Você permite conexões com o controlador de domínio através de um firewall ou de um servidor proxy.

7. Clique no botão **Salvar**.

A janela é fechada e a conexão é exibida na tabela de conexões.

Na barra de conexões, você pode fazer o seguinte:

- Edite os parâmetros de conexão.

  Para fazer isso, clique no link com o parâmetro **Endereço do controlador de domínio** para a conexão necessária. Na janela exibida, adicione as fontes necessárias e clique no botão **Salvar**.

  Você pode editar somente os parâmetros **Login** e **Senha**.

- Exclua as conexões.

  Para fazer isso, marque a caixa de seleção ao lado da conexão que deseja excluir, clique no botão **Remover** na barra de ferramentas e confirme a exclusão da conexão.

Configurando a integração com a Kaspersky Automated Security Awareness Platform

Integração com a Kaspersky Automated Security Awareness Platform (aqui também referida como KASAP) permite atribuir cursos de aprendizagem KASAP para usuários associados a alertas.

As configurações de integração não são herdadas e são aplicadas somente ao Servidor de Administração (servidor físico ou virtual) no qual você define essas configurações.

Antes de configurar uma integração no Kaspersky Security Center Web Console, você deve criar um token de autorização e obter um URL para solicitações de API no KASAP.

Para configurar a integração com a Kaspersky Automated Security Awareness Platform:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Selecione a seção **KASAP**.

3. No painel direito, ative o seletor de **Integração KASAP**.

4. Especifique as configurações a serem usadas para as Conexões com a KASAP:

   - **Token API** — Token que você criou para acessar a Open API da KASAP.
   - **URL** — URL para solicitações da API que você obteve ao criar o token da API.
   - **Usar um servidor proxy** — Defina o alternante para permitir o uso de um servidor proxy ao conectar-se ao KASAP.

     O seletor fica desativado por padrão.

5. Se necessário, verifique as configurações especificadas clicando no botão **Verificar conexão**.

   O status da conexão é exibido.

6. Clique no botão **Salvar**.

A integração com a Kaspersky Automated Security Awareness Platform está configurada.

Depois que as configurações de integração KASAP forem salvas, você poderá visualizar a lista de grupos de aprendizado KASAP clicando no botão **Exibir grupos**.

Se necessário, quando a lista de grupos for exibida, você poderá atualizá-la clicando no botão **Atualizar grupos**.

Você não pode ocultar a lista depois de abri-la. Se você desativar o botão de alternância **Integração KASAP**, a lista de grupos KASAP não será exibida.

Configurando a integração com o Kaspersky Threat Intelligence Portal Sandbox

Integração com o Kaspersky Threat Intelligence Portal (aqui também referido como Kaspersky TIP) permite executar os arquivos movidos para a seção **Quarentena** usando o Kaspersky Sandbox —um ambiente seguro isolado de sua rede corporativa.

As configurações de integração não são herdadas e são aplicadas somente ao Servidor de Administração (servidor físico ou virtual) no qual você define essas configurações.

Antes de configurar a integração, você deve obter um token de autorização para solicitações de API no Kaspersky TIP.

Para configurar a integração com o Kaspersky TIP Sandbox:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Selecione **Kaspersky TIP**.

3. No painel direito, ative o alternante **Integração**.

   As configurações para a conexão com o Kaspersky TIP são exibidas.

   Se, depois de configurar e salvar as configurações de integração, você desativar o botão de alternância **Integração**, as configurações não serão excluídas, mas a resposta não poderá ser executada.

4. Clique no botão **Adicionar token** e, na janela exibida, especifique o token obtido anteriormente no Kaspersky TIP. Em seguida, clique no botão **Adicionar**.

   A janela é fechada e o token da API é adicionado.

5. Se quiser usar um servidor proxy ao se conectar ao Kaspersky TIP, ative o alternante **Usar um servidor proxy**.

   O seletor fica desativado por padrão.

6. Clique no botão **Salvar**.

A integração com o Kaspersky TIP Sandbox está configurada.

Agora, você pode enviar arquivos do **Quarentena** seção para o Kaspersky TIP Sandbox para análise de ameaças. O tamanho máximo de um arquivo é de 100 MB.

Como a licença do Kaspersky Next XDR Optimum suporta multilocação, os arquivos colocados em **Quarentena** são divididos por locações. Essa separação em nível de tenant também se aplica ao enviar arquivos para o Kaspersky TIP Sandbox e exibir os resultados se o administrador usar uma conta TIP dedicada e um token de API relacionado a cada tenant. No entanto, o gerenciamento centralizado da seção **Quarentena** para todos os tenants não é possível, pois a lista de quarentena não exibe objetos de acordo com a hierarquia do servidor.

Agrupando alertas por atributos

A agregação de alertas ajuda a identificar alertas que podem estar relacionados ao mesmo incidente, simplificando o processo de investigação.

Para ativar a funcionalidade de agregação de alertas, você deve fazer o seguinte:

- Ative a subseção **Alertas** no menu principal.
- Ative o Servidor de Administração com uma licença do Kaspersky Next XDR Optimum e, em seguida, implemente a chave de Licenciamento do Kaspersky Next XDR Optimum nos aplicativos gerenciados.

  Ao usar a funcionalidade Kaspersky Next XDR Optimum com uma licença de avaliação no modo de teste, você deve primeiro adicionar um Servidor de Administração físico secundário e, depois, ativar esse servidor com esta licença.

Se estiver usando o licenciamento do Kaspersky Next EDR Optimum, não é necessário ativar os aplicativos instalados nos dispositivos gerenciados sob o licenciamento do Kaspersky Next XDR Optimum. Isso deve ser feito apenas para novos dispositivos, se houver.
Como a licença do Kaspersky Next XDR Optimum permite a multilocação, você pode distribuir centralmente a chave de licença para aplicativos gerenciados. A distribuição automática da licença para Servidores de Administração secundários e virtuais não é compatível.

Você pode agregar alertas por nome de dispositivo, conta ou nome de hash (SHA256).

> Os alertas são agregados por um atributo somente se esse atributo não estiver vazio.

Os alertas são agregados se compartilharem pelo menos um atributo e ocorrerem dentro de 24 horas após qualquer outro alerta no grupo.

Para agregar alertas por atributos:

1. No menu principal, vá para **Monitoramento** → **Alertas**.
2. Execute uma das seguintes ações:
   - Ative o alternante **Agrupamento de alertas** e selecione um ou mais atributos para agregar alertas por:
     - **Nome do dispositivo**
     - **Conta**
     - **Hash de arquivo (SHA256)**

     Os atributos **Nome do dispositivo** e **Conta** são selecionados por padrão.
   - Clique no ícone de configurações (⚙). No painel aberto **Configurações da tabela**, vá para a guia **Agrupamento**. Selecione o **ID do grupo de agregação** e clique em **Aplicar**.

Quando a agregação estiver ativada, os alertas são classificados por **Hora do evento** do mais novo ao mais antigo. As opções de classificação adicionais não são compatíveis. Selecione um grupo de opções diferente desativará a agregação.

A tabela exibe alertas agregados por atributos. Os alertas não agregados são exibidos na parte inferior da tabela.

Cada alerta é atribuído a apenas um grupo após a agregação.

Cloud Discovery

O Kaspersky Security Center Linux permite monitorar o uso de serviços em nuvem em dispositivos gerenciados que executam o Windows e bloquear o acesso a serviços em nuvem que você considera indesejados. A Cloud Discovery rastreia as tentativas do usuário de obter acesso a esses serviços por meio de navegadores e aplicativos desktop. Ele também rastreia as tentativas do usuário de obter acesso aos serviços em nuvem por meio de conexões não criptografadas (por exemplo, usando o protocolo HTTP). Esse recurso ajuda você a detectar e interromper o uso de serviços em nuvem por meio de shadow IT.

A capacidade de bloqueio estará disponível somente se o usuário tiver ativado o Kaspersky Security Center Linux sob uma licença do Kaspersky Next EDR Optimum ou do Kaspersky Next XDR Expert.

O recurso de bloqueio está disponível somente se você usar o Kaspersky Endpoint Security 11.2 for Windows ou posterior. As versões anteriores do aplicativo de segurança só permitem monitorar o uso de serviços em nuvem.

É possível ativar o recurso Cloud Discovery e selecionar as políticas ou perfis de segurança para os quais se deseja ativar o recurso. Você também pode ativar ou desativar o recurso separadamente em cada política ou perfil de segurança. É possível bloquear o acesso a serviços em nuvem que não se deseja que os usuários acessem.

Para poder bloquear o acesso a serviços em nuvem indesejados, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- Você usa o Kaspersky Endpoint Security 11.2 for Windows ou posterior. As versões anteriores do aplicativo de segurança só permitem monitorar o uso de serviços em nuvem.
- Você comprou o nível de licença Kaspersky Next que inclui a capacidade de bloquear o acesso aos serviços em nuvem indesejados. Para obter detalhes, consulte a Ajuda do Kaspersky Next.

O widget do Cloud Discovery e os relatórios do Cloud Discovery exibem informações sobre tentativas bem-sucedidas e bloqueadas de obter acesso a serviços em nuvem. O widget também exibe o nível de risco de cada serviço em nuvem. O Kaspersky Security Center Linux obtém informações sobre o uso de serviços em nuvem de todos os dispositivos gerenciados que são protegidos apenas pelos perfis de segurança que possuem o recurso ativado.

Como ativar o Cloud Discovery usando o widget

O recurso Cloud Discovery permite a você obter informações sobre o uso de serviços em nuvem de todos os dispositivos gerenciados protegidos somente pelas políticas de segurança e que tenham o recurso ativado. Você pode ativar ou desativar o Cloud Discovery somente para a política do Kaspersky Endpoint Security for Windows.

Há duas maneiras de ativar o recurso Cloud Discovery:

- Por meio do widget do Cloud Discovery.
- Nas propriedades da política do Kaspersky Endpoint Security for Windows.

  Para obter detalhes sobre como ativar o recurso Cloud Discovery nas propriedades da política do Kaspersky Endpoint Security for Windows, consulte a seção Cloud Discovery da ajuda do Kaspersky Endpoint Security for Windows.

Observe que você pode desativar o recurso Cloud Discovery somente nos parâmetros da política do Kaspersky Endpoint Security for Windows.

Para ativar o Cloud Discovery, é necessário ter direitos de **Gravar** na área funcional **Recursos gerais: Funcionalidade básica**.

Para ativar o recurso Cloud Discovery usando o widget Cloud Discovery:

1. Acesse o Kaspersky Security Center Linux.
2. No menu principal, vá para **Monitoramento** → **Painel**.
3. No widget do **Cloud Discovery**, clique no botão **Ativar**.

   Se você tiver o Kaspersky Endpoint Security for Windows versão 12.4 instalado, ative o recurso Cloud Discovery nas propriedades da política do Kaspersky Endpoint Security for Windows. Para obter detalhes, consulte a seção Cloud Discovery da Ajuda do Kaspersky Endpoint Security for Windows.

   Se você tiver o Kaspersky Endpoint Security for Windows anterior à versão 12.4, atualize o plug-in do Kaspersky Endpoint Security for Windows para a versão 12.5.

4. Na janela **Ativar o Cloud Discovery** exibida, selecione as políticas de segurança para as quais você deseja ativar o recurso e clique no botão **Ativar**.

   As seguintes configurações de política serão ativadas automaticamente: **Injetar script no tráfego da Web para interagir com páginas da Web**, **Monitor de sessão da Web** e **Verificação de conexões criptografadas**.

O recurso Cloud Discovery será ativado e o widget será adicionado ao painel.

Como adicionar o widget do Cloud Discovery ao painel

Você pode adicionar o widget do **Cloud Discovery** ao painel para monitorar o uso de serviços em nuvem em dispositivos gerenciados.

Para adicionar o widget do Cloud Discovery ao painel, é preciso ter direitos de **Gravar** na área funcional **Recursos gerais: Funcionalidade básica**.

Para adicionar o widget do Cloud Discovery ao painel:

1. Acesse o Kaspersky Security Center Linux.
2. No menu principal, vá para **Monitoramento** → **Painel**.
3. Clique no botão **Adicionar ou restaurar widget**.
4. Na lista de widgets disponíveis, clique no ícone de divisa (>) ao lado da categoria **Outro**.
5. Selecione o widget do **Cloud Discovery** e clique no botão **Adicionar**.

   Caso o recurso Cloud Discovery esteja desativado, siga as instruções na seção ativar o Cloud Discovery usando o widget.

O widget selecionado é adicionado no final do painel.

Exibir informações sobre o uso de serviços em nuvem

Você pode exibir o widget do **Cloud Discovery**, que exibe informações sobre tentativas de obtenção de acesso aos serviços em nuvem. O widget também exibe o nível de risco de cada serviço em nuvem. O Kaspersky Security Center Linux obtém informações sobre o uso de serviços em nuvem de todos os dispositivos gerenciados que são protegidos apenas pelos perfis de segurança que possuem esse recurso ativado.

Antes de visualizar, certifique-se de que:

- O widget do Cloud Discovery foi adicionado ao painel.
- O recurso Cloud Discovery está ativado.
- Você tem os direitos de **Ler** na área funcional **Recursos gerais: Funcionalidade básica**.

Para visualizar o widget do Cloud Discovery:

1. Acesse o Kaspersky Security Center Linux.
2. No menu principal, vá para **Monitoramento** → **Painel**.

   O widget do **Cloud Discovery** será exibido no painel.

3. No lado esquerdo do widget do **Cloud Discovery**, selecione uma categoria de serviços em nuvem.

   A tabela no lado direito do widget exibe até cinco serviços da categoria selecionada, aos quais os usuários tentam obter acesso com mais frequência. As tentativas bem-sucedidas e bloqueadas são contabilizadas.

4. No lado direito do widget, selecione um serviço específico.

   A tabela abaixo exibe até dez dispositivos que tentam obter acesso ao serviço com mais frequência. Nesta tabela, você pode gerar dois tipos de relatórios: relatório sobre tentativas de acesso bem-sucedidas e relatório sobre tentativas de acesso bloqueadas.

   Além disso, nesta tabela, você pode bloquear o acesso ao serviço de nuvem para um dispositivo específico.

O widget exibe as informações solicitadas.

No widget exibido, você pode fazer o seguinte:

- Prossiga para a seção **Monitoramento** → **Relatórios** para visualizar os relatórios do Cloud Discovery.
- Bloquear ou permitir acesso ao serviço de nuvem selecionado.

A capacidade de bloqueio estará disponível somente se o usuário tiver ativado o Kaspersky Security Center Linux sob uma licença do Kaspersky Next EDR Optimum ou do Kaspersky Next XDR Expert.
O recurso de bloqueio está disponível somente se você usar o Kaspersky Endpoint Security 11.2 for Windows ou posterior. As versões anteriores do aplicativo de segurança só permitem monitorar o uso de serviços em nuvem.

Nível de risco de um serviço de nuvem

Para cada serviço em nuvem, o Cloud Discovery fornece um nível de risco. O nível de risco ajuda a determinar os serviços que não atendem aos requisitos de segurança de sua organização. Por exemplo, convém considerar o nível de risco ao decidir se deve bloquear o acesso a um determinado serviço.

O nível de risco é um índice estimado e não diz nada sobre a qualidade de um serviço em nuvem ou sobre o fabricante do serviço. O nível de risco é simplesmente uma recomendação dos especialistas da Kaspersky.

Os níveis de risco dos serviços em nuvem são exibidos no widget do Cloud Discovery e na lista de todos os serviços em nuvem monitorados.

Como bloquear o acesso a serviços de nuvem indesejados

Você pode bloquear o acesso a serviços em nuvem que outros usuários não devem acessar. Você também pode permitir o acesso a serviços em nuvem que foram bloqueados anteriormente.

Entre outras considerações, convém considerar o nível de risco ao decidir se o acesso a um determinado serviço deve ser bloqueado.

Você pode bloquear ou permitir o acesso aos serviços em nuvem para determinada política ou perfil de segurança.

Há duas maneiras de bloquear o acesso a serviços de nuvem indesejados:

- Por meio do widget do Cloud Discovery.

  Nesse caso, você pode bloquear o acesso aos serviços um por um.

- Nas propriedades da política do Kaspersky Endpoint Security for Windows.

  Nesse caso, é possível bloquear o acesso aos serviços um por um ou bloquear toda a categoria de uma só vez.

  Para obter detalhes sobre como ativar o recurso Cloud Discovery nas propriedades da política do Kaspersky Endpoint Security for Windows, consulte a seção Cloud Discovery da ajuda do Kaspersky Endpoint Security for Windows.

Para bloquear ou permitir o acesso a um serviço em nuvem usando o widget:

1. Abra o widget do Cloud Discovery e selecione o serviço em nuvem desejado.
2. No painel **Os 10 dispositivos que mais usam o serviço**, localize a política ou o perfil de segurança para o qual deseja bloquear ou permitir o serviço.
3. Na linha desejada na coluna **Status de acesso na política ou perfil**, execute uma das seguintes ações:
   - Para bloquear o serviço, selecione **Bloqueado** na lista suspensa.
   - Para permitir o serviço, selecione **Permitido** na lista suspensa.
4. Clique no botão **Salvar**.

O acesso ao serviço selecionado estará bloqueado ou permitido para a política ou o perfil de segurança.

Exportação de eventos para os sistemas SIEM

Esta seção descreve como configurar a exportação de eventos para os sistemas SIEM.

Configuração da exportação de eventos para sistemas SIEM

O Kaspersky Security Center Linux permite configurar a exportação de eventos para sistemas SIEM por um dos seguintes métodos: exportação para qualquer sistema SIEM que use o formato Syslog, exportação para os sistemas Kaspersky SIEM, QRadar, Splunk e ArcSight SIEM que usam os formatos LEEF e CEF, ou exportação de eventos para sistemas SIEM diretamente do banco de dados do Kaspersky Security Center. Ao concluir este cenário, o Servidor de Administração envia eventos para um sistema SIEM automaticamente.

Pré-requisitos

Antes de iniciar a exportação de configuração de eventos no Kaspersky Security Center Linux:

- Saiba mais sobre os métodos de exportação de eventos.
- Certifique-se de que tem conhecimento dos os valores das configurações do sistema.

Você pode executar as etapas deste cenário em qualquer ordem.

O processo de exportação de eventos para um sistema SIEM consiste nos seguintes passos:

- **Configurando o sistema SIEM para receber eventos do Kaspersky Security Center Linux**

  Instruções: Configurando a exportação de eventos em um sistema SIEM

- **Selecionando os eventos que deseja exportar para o sistema SIEM**

  Marcar quais eventos deseja exportar para o sistema SIEM. Primeiro, marque os eventos gerais que ocorrem em todos os aplicativos gerenciados da Kaspersky. Depois disso, é possível marcar os eventos para aplicativos gerenciados específicos da Kaspersky.

- **Configurando a exportação de eventos para o sistema SIEM**

  É possível exportar eventos usando um dos seguintes métodos:

  - Usar protocolos TCP, UDP ou TLS sobre TCP.
  - Exportar eventos diretamente do banco de dados do Kaspersky Security Center. O banco de dados do Kaspersky Security Center contém um conjunto de exibições públicas; você pode encontrar uma descrição dessas exibições públicas no documento klakdb.chm.

Resultados

Após configurar a exportação de eventos para um sistema SIEM, você pode ver os resultados de exportação se tiver selecionado eventos que deseja exportar.

Pré-requisitos

Ao configurar uma exportação automática de eventos no Kaspersky Security Center Linux, você deve especificar algumas das configurações do sistema SIEM. Recomenda-se que você verifique estas configurações com antecedência para preparar-se para configurar o Kaspersky Security Center Linux.

Para configurar corretamente o envio automático de eventos a um sistema SIEM, você deve conhecer as seguintes configurações:

- **Endereço do servidor do sistema SIEM**

  O endereço IP do servidor onde o sistema SIEM atualmente usado está instalado. Verifique este valor nas suas configurações de sistema SIEM.

- **Porta do servidor do sistema SIEM**

  O número da porta usada para estabelecer a conexão entre o Kaspersky Security Center Linux e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center Linux e nas configurações do receptor do seu sistema SIEM.

- **Protocolo**

  Protocolo usado para transferir mensagens do Kaspersky Security Center Linux ao seu sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center Linux e nas configurações do receptor do seu sistema SIEM.

Sobre a exportação de evento

O Kaspersky Security Center Linux permite que o usuário receba informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nos dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração.

Você pode usar a exportação de evento dentro de sistemas centralizados que tratam de questões de segurança em nível organizacional e técnico, que fornecem serviços de monitoramento da segurança e consolidam informações de diferentes soluções. Estes são sistemas SIEM, que fornecem a análise em tempo real de alertas de segurança e eventos gerados por hardware de rede e aplicativos ou Centros de Operação de Segurança (SOCs).

Estes sistemas recebem dados de muitas fontes, incluindo redes, segurança, servidores, bancos de dados e aplicativos. Os sistemas de SIEM também fornecem a funcionalidade para consolidar os dados monitorados para ajudá-lo a evitar faltar a eventos críticos. Além disso, os sistemas executam a análise automatizada de eventos correlacionados e alertas para notificar os administradores de problemas de segurança imediatos. Um alerta pode ser implementado através de um painel ou pode ser enviado por canais de terceiros, tal como por um e-mail.

O processo de exportar eventos do Kaspersky Security Center Linux para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center Linux) e um receptor do evento (sistema SIEM). Para exportar com sucesso eventos, você deve configurar isso no seu sistema SIEM e no Kaspersky Security Center Linux. Não importa que lado você configura primeiro. É possível configurar a transmissão de eventos no Kaspersky Security Center Linux e depois configurar o recebimento de eventos pelo sistema SIEM, ou vice-versa.

Métodos para enviar eventos do Kaspersky Security Center Linux

Há três métodos para enviar eventos do Kaspersky Security Center Linux aos sistemas externos:

- Enviando eventos sob o protocolo Syslog à qualquer sistema SIEM

  Usando o protocolo Syslog, você pode encaminhar qualquer evento que ocorre no Servidor de Administração e em aplicativos Kaspersky que são instalados em dispositivos gerenciados. O protocolo Syslog é um protocolo de registro de mensagem padrão. É possível usá-lo para exportar os eventos para qualquer sistema SIEM.

  Para isso, é preciso marcar os eventos que deseja retransmitir ao sistema SIEM. É possível marcar os eventos no Kaspersky Security Center Web Console. Apenas os eventos marcados serão retransmitidos para o sistema SIEM. Caso não tenha marcado nada, nenhum evento será retransmitido.

- Envio de eventos pelos protocolos CEF e LEEF para os sistemas Kaspersky SIEM, QRadar, Splunk e ArcSight

Você pode usar os protocolos CEF e LEEF para exportar eventos gerais. Ao exportar eventos sobre os protocolos CEF e LEEF, você não tem a capacidade de selecionar eventos específicos para exportar. Em vez disso, todos os eventos gerais são exportados. Para converter eventos do Kaspersky Security Center Linux em eventos no formato CEF e LEEF, você precisa usar o arquivo siem_conversion_rules.xml. Esse arquivo contém a lista de atributos de eventos do Kaspersky Security Center Linux e atributos correspondentes de eventos nos formatos CEF e LEEF. Além disso, o arquivo siem_conversion_rules.xml contém as regras para gerar mensagens correspondentes aos eventos. Esse arquivo está incluído no kit de distribuição do Kaspersky Security Center Linux.

Diferentemente do protocolo Syslog, os protocolos CEF e LEEF não são universais. CEF e LEEF são destinados aos sistemas SIEM apropriados (Kaspersky SIEM, QRadar, Splunk e ArcSight). Portanto, quando você escolhe exportar eventos através de um desses protocolos, você usa o analisador necessário no sistema SIEM.

- Diretamente do banco de dados do Kaspersky Security Center Linux para qualquer sistema SIEM

  Este método de exportar eventos pode ser usado para receber eventos diretamente das vistas públicas do banco de dados por meio de consultas SQL. Os resultados de uma consulta são salvos em um arquivo XML que pode ser usado como dados de entrada para um sistema externo. Somente os eventos disponíveis nas vistas públicas podem ser exportados diretamente do banco de dados.

Recebimento de eventos pelo sistema SIEM

O sistema SIEM deve receber e corretamente analisar os eventos recebidos do Kaspersky Security Center Linux. Para conseguir isso, você precisa configurar corretamente o sistema SIEM. A configuração depende do sistema SIEM específico utilizado. No entanto, há um número de etapas gerais na configuração de todos os sistemas SIEM, tal como a configuração do receptor e do analisador.

Sobre a configuração de exportação de eventos em um sistema SIEM

O processo de exportar eventos do Kaspersky Security Center Linux para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center Linux) e um receptor do evento (sistema SIEM). Você deve configurar a exportação de eventos no seu sistema SIEM e no Kaspersky Security Center Linux.

As configurações especificadas no sistema SIEM dependem de qual sistema que você estiver usando. Normalmente, para todos os sistemas SIEM você deve definir um receptor e, opcionalmente, um analisador de mensagem para analisar os eventos recebidos.

Configurar o receptor

Para poder receber eventos enviados pelo Kaspersky Security Center Linux, configure o receptor no seu sistema SIEM. Em geral, as seguintes configurações devem ser especificadas no sistema SIEM:

- **Protocolo para exportar**

  Um protocolo de transferência de mensagens, UDP, TCP ou TLS sobre TCP. Este protocolo deve ser o mesmo protocolo que você especificou no Kaspersky Security Center Linux.

- **Porta**

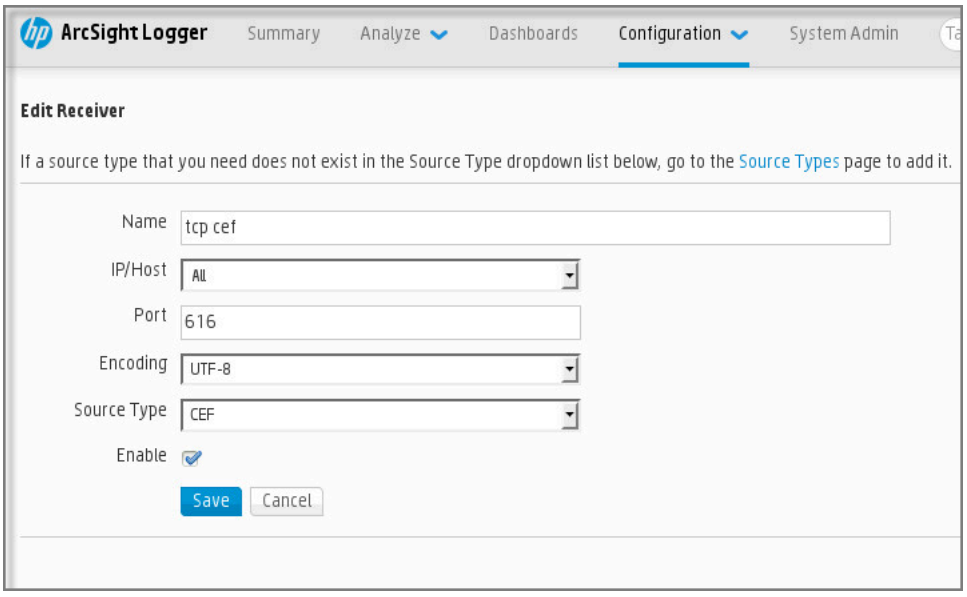
  Especifique o número da porta para se conectar ao Kaspersky Security Center Linux. A porta deve ser a mesma especificada no Kaspersky Security Center Linux durante a configuração com um sistema SIEM.

- **Formato de dados**

  Especifique o formato Syslog, CEF ou LEEF.

Dependendo do sistema SIEM usado, você pode ter que especificar algumas configurações adicionais de receptor.

A figura abaixo mostra tela de configuração de receptor no ArcSight.



Configuração do receptor no ArcSight

Analisador de mensagem

Os eventos exportados são passados aos sistemas SIEM como mensagens. Um analisador é então aplicado a essas mensagens para garantir que as informações do evento possam ser usadas pelo sistema SIEM. Um analisador de mensagem faz parte do sistema SIEM; ele é usado para dividir o conteúdo da mensagem em campos como código do evento, gravidade, descrição e parâmetros. Isto ativa o sistema SIEM para processar eventos recebidos do Kaspersky Security Center Linux para que eles possam ser armazenados no banco de dados do sistema SIEM.

Sobre a exportação de eventos usando formatos CEF e LEEF

Você pode usar os formatos CEF e LEEF para exportar para sistemas SIEM eventos gerais, eventos de alteração de política, bem como eventos transferidos pelos aplicativos da Kaspersky para o Servidor de Administração. O conjunto de eventos exportado é predefinido, e você não pode selecionar os eventos a ser exportados. Antes de enviar eventos ao sistema SIEM (Kaspersky SIEM, QRadar, ArcSight ou Splunk), é necessário interpretar os eventos do Kaspersky Security Center Linux para eventos no formato CEF e LEEF usando as regras especificadas no arquivo siem_conversion_rules.xml.

Selecione o formato de exportação com base no sistema SIEM usado. A tabela abaixo mostra os sistemas SIEM e os formatos de exportação correspondentes.

Formatos da exportação de eventos para um sistema SIEM

SIEM system	Formato de exportação
Kaspersky SIEM	CEF
ArcSight	CEF
Splunk	CEF
QRadar	LEEF

- O LEEF (Log Event Extended Format) é um formato de evento especializado para o IBM Security QRadar SIEM. O QRadar pode receber, identificar e processar eventos transmitidos pelo protocolo LEEF. Os eventos de LEEF devem usar a codificação de caractere UTF-8. Você pode encontrar as informações detalhadas sobre o protocolo LEEF no IBM Knowledge Center.

- CEF (Formato de Evento Comum) – Um padrão de gerenciamento de registro aberto que aprimora a interoperabilidade da informação relativa a segurança de diferentes dispositivos de segurança e de rede e aplicativos. O CEF lhe permite usar um formato de registro de evento comum para que os dados possam ser facilmente integrados e agregados para a análise por um sistema de gerenciamento corporativo. Os eventos de CEF devem usar a codificação de caractere UTF-8.

A exportação automática significa que o Kaspersky Security Center Linux envia eventos gerais ao sistema SIEM. A exportação automática de eventos inicia imediatamente após você a ativar. Esta seção explica detalhadamente como ativar a exportação automática de eventos.

Conversão de eventos para o formato CEF ou LEEF

Antes de enviar eventos ao sistema SIEM (Kaspersky SIEM, QRadar, ArcSight ou Splunk), é necessário interpretar os eventos do Kaspersky Security Center Linux para os formatos CEF e LEEF usando as regras especificadas no arquivo siem_conversion_rules.xml. Esse arquivo está incluído no kit de distribuição do Kaspersky Security Center Linux.

O arquivo siem_conversion_rules.xml contém as regras de interpretação predefinidas para converter eventos para o formato CEF e LEEF. Caso queira usar regras adicionais de interpretação de eventos, é possível adicioná-las manualmente ao arquivo.

O arquivo siem_conversion_rules.xml inclui as seguintes seções:

- `<product name="SP_QRADAR" vendor="IBM">`

  Esta seção contém regras para gerar eventos no formato LEEF que podem ser exportados para o sistema QRadar SIEM.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  Esta seção contém regras para gerar eventos no formato CEF que podem ser exportados para o sistema ArcSight ou Splunk SIEM.

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`.

  Esta seção contém as regras para gerar eventos no formato CEF, que podem ser exportados para KUMA.

Cada seção contém a subseção `<common>`, na qual estão localizados os atributos de eventos do Kaspersky Security Center Linux e os atributos correspondentes dos eventos no formato LEEF. Esses atributos comuns são usados para todos os tipos de eventos que podem ser exportados.

Além disso, cada seção tem subseções `<event>`. Cada subseção de `<event>` contém atributos adicionais que são adicionados àqueles listados na seção `<comum>`.

É possível adicionar manualmente uma nova regra de geração de eventos ao arquivo siem_conversion_rules.xml.

Para adicionar uma nova regra de geração de eventos:

1. Adicione uma nova subseção `<event>` à seção `<product name="SP_QRADAR" vendor="IBM">`, `<product name="SP_QRADAR" vendor="IBM">` ou `<product name="Kaspersky SIEM" vendor="Kaspersky">` e, em seguida, especifique os atributos adicionais do evento, se necessário.

2. Caso um evento consista apenas em atributos comuns, a subseção `<event>` estará vazia.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Marcando eventos para exportação para sistemas SIEM em formato Syslog

Após ativar a exportação automática de eventos, você deve selecionar quais eventos serão exportados ao sistema SIEM externo.

Você pode configurar a exportação de eventos em formato Syslog para um sistema externo com base em uma das seguintes condições:

- Marcando eventos gerais. Se você marcar eventos para exportar em uma política, nas configurações de um evento ou no Servidor de Administração, o sistema SIEM receberá os eventos marcados que ocorreram em todos os aplicativos gerenciados pela política específica. Se os eventos exportados foram selecionados na política, você não será capaz de redefini-los para um aplicativo individual gerenciado por esta política.

- Marcando eventos para um aplicativo individual. Se você marcar eventos para exportar para um aplicativo gerenciado instalado em um dispositivo gerenciado, o sistema SIEM somente receberá os eventos que ocorreram neste aplicativo.

Para eventos de alteração de política, somente é possível ativar ou desativar a exportação de todos esses eventos para um sistema SIEM.

Marcando eventos de um aplicativo da Kaspersky para exportação em formato Syslog

Se você desejar exportar eventos que ocorreram em um aplicativo gerenciado específico instalado nos dispositivos gerenciados, marque os eventos para exportação na política do aplicativo. Nesse caso, os eventos marcados são exportados de todos os dispositivos incluídos no escopo da política.

Para marcar eventos para exportação para um aplicativo gerenciado específico:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.
2. Clique na política do aplicativo para o qual você deseja marcar eventos.

   A janela Propriedades da política será aberta.
3. Siga para a seção **Configuração de eventos**.
4. Marque as caixas de seleção ao lado dos eventos que você deseja exportar para um sistema SIEM.
5. Clique no botão **Marcar exportação para o sistema SIEM usando o Syslog**.

   Também é possível marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, que é aberta ao clicar no link do evento.
6. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.
7. Clique no botão **Salvar**.

Os eventos marcados do aplicativo gerenciado estão prontos para serem exportados para um sistema SIEM.

É possível marcar quais eventos exportar para um sistema SIEM para um dispositivo gerenciado específico. Se os eventos exportados anteriormente foram marcados em uma política de aplicativo, não será possível redefinir os eventos marcados para um dispositivo gerenciado.

Para marcar eventos para exportação para um dispositivo gerenciado:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Clique no link com o nome do dispositivo desejado na lista de dispositivos gerenciados.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Siga para a seção **Aplicativos**.

4. Clique no link com o nome do aplicativo desejado na lista de aplicativos.

5. Siga para a seção **Configuração de eventos**.

6. Marque as caixas de seleção ao lado dos eventos que você deseja exportar para um sistema SIEM.

7. Clique no botão **Marcar exportação para o sistema SIEM usando o Syslog**.

   Também é possível marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, que é aberta ao clicar no link do evento.

8. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.

A partir de agora, o Servidor de Administração envia os eventos marcados para o sistema SIEM se a exportação para o sistema SIEM estiver configurada.

Marcando eventos gerais para exportação no formato Syslog

Você pode marcar eventos gerais que o Servidor de Administração exportará para os sistemas SIEM usando o formato Syslog.

Para configurar eventos gerais para um sistema SIEM:

1. No menu principal, execute uma das seguintes ações:

   - Clique no nome do Servidor de Administração.
   - Vá para **Gerenciamento de ativos** → **Políticas** e clique no link de uma política.

2. Na janela aberta, vá para **Configuração de eventos**.

3. Clique em **Marcar exportação para o sistema SIEM usando o Syslog**.

   Também é possível marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, que é aberta ao clicar no link do evento.

4. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.

A partir de agora, o Servidor de Administração envia os eventos marcados para o sistema SIEM se a exportação para o sistema SIEM estiver configurada.

Sobre a exportação de eventos usando o formato Syslog

Você pode usar o formato Syslog para exportar aos sistemas SIEM os eventos que ocorrem no Servidor de Administração e em outros aplicativos Kaspersky instalados em dispositivos gerenciados.

Syslog é um padrão para o protocolo de registro da mensagem. Isso permite a separação do software que gera mensagens, o sistema que as armazena e o software que os reporta e os analisa. Cada mensagem é legendada com um código de instalação, indicando o tipo de software que gera a mensagem e à mesma é atribuído um nível de gravidade.

O formato Syslog é definido por documentos de Solicitação de Comentários (RFC) publicados pela Internet Engineering Task Force (padrões da Internet). O padrão RFC 5424 é usado para exportar os eventos do Kaspersky Security Center Linux aos sistemas externos.

No Kaspersky Security Center Linux, você pode configurar a exportação dos eventos aos sistemas externos usando o formato Syslog.

O processo de exportação consistem em duas etapas:

1. Ativar a exportação automática do evento. Nesta etapa, o Kaspersky Security Center Linux é configurado para que ele envie eventos ao sistema SIEM. O Kaspersky Security Center Linux começa a enviar eventos imediatamente após você ativar a exportação automática.

2. Selecionar os eventos a ser exportados ao sistema externo. Nesta etapa, você seleciona qual evento exportar ao sistema SIEM.

Configurando o Kaspersky Security Center Linux para exportação de eventos para o sistema SIEM

Para exportar eventos para o sistema SIEM, você deve configurar o processo de exportação no Kaspersky Security Center Linux.

Antes de enviar eventos ao sistema SIEM (Kaspersky SIEM, QRadar, ArcSight ou Splunk), é necessário interpretar os eventos do Kaspersky Security Center Linux para os formatos CEF e LEEF usando as regras especificadas no arquivo siem_conversion_rules.xml.

Para configurar a exportação para sistemas SIEM no Kaspersky Security Center Web Console:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Exportar para SIEM**.

3. Clique no link **Configurar conexão**.

   A seção **Exportar as configurações** é aberta.

4. Especifique as configurações na seção **Exportar as configurações**:

- **Endereço do servidor do sistema SIEM**

  O endereço IP do servidor onde o sistema SIEM atualmente usado está instalado. Verifique este valor nas suas configurações de sistema SIEM.

- **Porta do sistema SIEM**

  O número da porta usada para estabelecer a conexão entre o Kaspersky Security Center Linux e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center Linux e nas configurações do receptor do seu sistema SIEM.

- **Protocolo**

  Selecione o protocolo a ser usado para transferir mensagens para o sistema SIEM. É possível selecionar os protocolos TCP, UDP ou TLS sobre TCP.

  Especifique as seguintes configurações de TLS se selecionar o protocolo TLS sobre TCP:

  - **Autenticação do servidor**

    No campo **Autenticação do servidor**, você pode selecionar os valores de **Certificados confiáveis** ou de **Impressões digitais SHA**:

    - **Certificados confiáveis**. Você pode receber uma cadeia de certificado completo (incluindo o certificado raiz) de uma autoridade de certificação (CA) confiável e carregá-lo para o Kaspersky Security Center Linux. O Kaspersky Security Center Linux verifica se a cadeia de certificado do servidor do sistema SIEM é assinada por uma CA confiável.

      Para adicionar um certificado confiável, clique no botão **Procurar arquivo de certificados CA** e, em seguida, carregue o certificado.

    - **Impressões digitais SHA**. Você pode especificar impressões digitais SHA1 da cadeia de certificados completa do sistema SIEM (incluindo o certificado raiz) no Kaspersky Security Center Linux. Para adicionar uma impressão digital SHA1, insira-a no campo **Impressões digitais** e, em seguida, clique no botão **Adicionar**.

    Ao usar a configuração **Adicionar autenticação do cliente**, é possível gerar um certificado para autenticar o Kaspersky Security Center Linux. Assim, um certificado autoassinado emitido pelo Kaspersky Security Center Linux será usado. Nesse caso, você pode usar um certificado confiável e uma impressão digital SHA para autenticar o servidor do sistema SIEM.

  - **Adicionar nome do assunto/Nome alternativo do assunto**

    Nome do assunto é um nome de domínio para o qual o certificado foi recebido. O Kaspersky Security Center Linux não pode se conectar ao servidor do sistema SIEM se o nome de domínio do servidor do sistema SIEM não corresponder ao nome da entidade do certificado do servidor do sistema SIEM. No entanto, o servidor do sistema SIEM pode alterar seu nome de domínio se o nome tiver sido alterado no certificado. Neste caso, você pode especificar nomes de assuntos no campo **Adicionar nome do assunto/Nome alternativo do assunto**. Se qualquer um dos nomes de assunto especificados corresponder ao nome do assunto do certificado do sistema SIEM, o Kaspersky Security Center Linux valida o certificado do servidor do sistema SIEM.

  - **Adicionar autenticação do cliente**

Para autenticação de cliente, é possível inserir o seu certificado ou gerá-lo no Kaspersky Security Center Linux.

- **Inserir certificado**. Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer CA confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

  - **Certificado X.509 PEM**. Carregue um arquivo com um certificado no campo **Arquivo com certificado** e um arquivo com uma chave privada no campo **Arquivo com chave**. Os dois arquivos são independentes um do outro. A ordem em que os arquivos são carregados não importa. Quando os dois arquivos forem carregados, especifique a senha para decodificar a chave privada no campo **Verificação de senha ou certificado**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

  - **Certificado X.509 PKCS12**. Carregue um único arquivo que contenha um certificado e sua chave privada no campo **Arquivo com certificado**. Quando o arquivo for carregado, especifique a senha para decodificar a chave privada no campo **Verificação de senha ou certificado**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- **Gerar chave**. É possível gerar um certificado autoassinado no Kaspersky Security Center Linux. Como resultado, o Kaspersky Security Center Linux armazena o certificado autoassinado gerado e você pode passar a parte pública do certificado ou a impressão digital SHA1 para o sistema SIEM.

- **Formato de data**

  Você pode selecionar os formatos de log do Kaspersky SIEM, IBM QRadar SIEM, ArcSight, Splunk ou do sistema, dependendo dos requisitos do sistema SIEM.

  Se você selecionar o formato de dados de log do sistema, deverá especificar o **Tamanho máximo da mensagem, em bytes**.

  Especifique o tamanho máximo (em bytes) de uma mensagem encaminhada ao sistema SIEM. Cada evento é encaminhado em uma mensagem. Se o comprimento real de uma mensagem exceder o valor especificado, a mensagem é truncada e os dados podem ser perdidos. O tamanho padrão é de 2.048 bytes. Este campo estará disponível somente se você selecionar o formato de log do sistema no campo **Protocolo**.

5. Se desejar, você pode exportar eventos arquivados do banco de dados do Servidor de Administração e definir a data de início da exportação de eventos arquivados:

   a. Clique no link **Definir a data de início da exportação**.

   b. Na seção aberta, especifique a data de início no campo **Data para início da exportação**.

   c. Clique em **OK**.

6. Ative a opção **Exportar eventos para o SIEM**.

7. Para enviar eventos de alteração de política ao SIEM, ative a opção **Exportar eventos estendidos para alterações de política no SIEM**. Um evento separado será enviado ao SIEM para cada configuração de política alterada.

8. Para verificar se a conexão do sistema SIEM foi configurada, clique no botão **Verificar conexão**.

   A conexão com o servidor do sistema SIEM é estabelecida e um evento de teste é enviado. O status da conexão será exibido.

9. Clique no botão **Salvar**.

A exportação para o sistema SIEM está configurada. A partir de agora, se você configurou o recebimento de eventos em um sistema SIEM, o Servidor de Administração exportará os eventos marcados ou os eventos de alteração de política para um sistema SIEM. Se você definir a data de início da exportação, o Servidor de Administração também exportará os eventos marcados armazenados no banco de dados do Servidor de Administração a partir da data especificada.

Monitoramento de alterações em políticas e perfis de política

Quando uma configuração de política é alterada, é gerado um evento de alteração de política, que pode ser exportado para um sistema SIEM para monitorar alterações de política e gerar alertas. Só é possível acessar os eventos de alteração de política por meio de um sistema SIEM.

Os eventos de alteração de política não são armazenados no banco de dados do Servidor de Administração após a geração e não podem ser visualizados na seção **Monitoramento → Seleções de eventos** do Kaspersky Security Center Web Console. Também não é possível especificar as configurações de notificação nem as configurações de armazenamento para esses eventos na guia **Configuração de eventos**.

Quando você cria uma política, é gerado um evento de alteração de política para cada configuração da política. Quando você altera uma política, é gerado um evento de alteração de política para cada configuração alterada. A exclusão de uma política gera um evento. Por exemplo, a criação de políticas do Kaspersky Security Center gera cerca de 1.000 eventos, e a criação de políticas do Kaspersky Endpoint Security gera mais de 7.000 eventos.

Condições para gerar eventos de alteração de política

Um evento de alteração de política é gerado sempre que um usuário realiza qualquer uma das seguintes ações com uma política ou um perfil de política:

- Criar, editar ou excluir uma política
- Criar, editar ou excluir um perfil de política
- Reverter a política para uma revisão selecionada
- Importar ou copiar uma política
- Importar ou copiar um perfil de política
- Mover uma política para outro grupo de administração

Um evento de modificação de política é gerado quando as seguintes condições são atendidas:

- As políticas dos seguintes aplicativos são alteradas:
  - Agente de Rede do Kaspersky Security Center
  - Servidor de Administração do Kaspersky Security Center
  - Kaspersky Endpoint Security for Windows 14.1 ou posterior
  - Kaspersky Endpoint Security for Linux 12.5 ou posterior

- Kaspersky Endpoint Security for Linux 12.4 ou posterior
- Kaspersky Endpoint Security for Mac 12.2.1 ou posterior

- A opção **Exportar eventos estendidos para alterações de política no SIEM** nas propriedades do Servidor de Administração está ativada.
- A política é modificada manualmente por meio da interface do Kaspersky Security Center Web Console.

Os eventos de alteração de política não são criados nos seguintes casos:

- As configurações gerais da política são modificadas.
- As configurações da política herdadas de uma política principal são modificadas.
- As configurações da política são alteradas por meio da OpenAPI do Kaspersky Security Center.
- As configurações do aplicativo da Kaspersky são modificadas diretamente no aplicativo.

Campos de eventos de alteração de política

A tabela abaixo mostra um conjunto de campos de eventos de alteração de política. A representação desses campos depende do formato do evento resultante (por exemplo, Syslog, CEF ou LEEF). Para obter os nomes de campo e os modelos de evento exatos, consulte o arquivo siem_conversion_rules.xml. Os parâmetros de evento estão disponíveis somente em inglês.

Campo do evento	Tipo de dados	Descrição
`eventType`	string	Tipo do evento. Permite criar regras de correlação para esse tipo específico de evento. Valores possíveis: "Política criada", "Política modificada", "Política excluída".
`srvName`	string	Nome do Servidor de Administração.
`eventTime`	datetime	Data e hora do evento (em UTC).
`eventGroupID`	int	ID do grupo de eventos de uma modificação.
`objectID`	int	ID interno de um objeto.
`objectName`	string	Nome de exibição da política.
`objectGroup`	string	Caminho e nome completos do grupo de administração que contém a política.
`user`	string	Nome do usuário que criou a modificação.
`operation`	string	Tipo de modificação do parâmetro. Valores possíveis: "Added", "Removed", "Changed".
`path`	string	Caminho do parâmetro. Contém o caminho para o nó principal do parâmetro final. O caminho é criado com base nos nomes das seções e subseções da política. A estrutura do caminho é idêntica àquelas descritas em Configurações da política do Agente de Rede, Configurações gerais da política e Comparação de revisões da política.
`parameter`	string	O nome da configuração de política modificada.
`oldValue`	string	Valor antigo do parâmetro final.
`newValue`	string	Novo valor do parâmetro final.

Exportando eventos diretamente do banco de dados

Você pode recuperar eventos diretamente do banco de dados do Kaspersky Security Center Linux sem ter necessidade de usar a interface Kaspersky Security Center Linux. Você pode consultar as vistas públicas diretamente e recuperar os dados de evento, ou ainda criar as suas próprias vistas com base em vistas públicas existentes e endereçá-las para receber os dados de que precisa.

Vistas públicas

Para a sua conveniência, um conjunto de vistas públicas é fornecido no banco de dados do Kaspersky Security Center Linux. Você pode encontrar a descrição dessas visualizações públicas no documento klakdb.chm.

A vista pública v_akpub_ev_event contém um conjunto de campos que representa os parâmetros de evento no banco de dados. No documento klakdb.chm você também pode encontrar informações sobre vistas públicas que correspondem a outras entidades do Kaspersky Security Center Linux, por exemplo, dispositivos, aplicativos ou usuários. Você pode usar estas informações nas suas consultas.

Esta seção contém instruções para executar uma consulta SQL por meio do utilitário klsql2 e um exemplo de consulta.

Para criar consultas SQL ou vistas do banco de dados, você também pode usar qualquer outro programa com bancos de dados. As informações sobre como exibir os parâmetros para conectar-se ao banco de dados do Kaspersky Security Center Linux, como o nome da instância e o nome do banco de dados, são fornecidas na seção correspondente.

Executar uma consulta SQL usando o utilitário klsql2

Este artigo descreve como usar o utilitário klsql2 e executar uma consulta SQL usando esse utilitário. Use a versão do utilitário klsql2 incluída na versão do Kaspersky Security Center Linux instalada.

Para usar o utilitário klsql2:

1. Vá para o diretório onde o Servidor de Administração está instalado. O caminho de instalação padrão é /opt/kaspersky/ksc64/sbin.

2. Neste diretório, crie um arquivo em branco com a extensão .sql.

3. Abra o arquivo .sql em qualquer editor de texto.

4. No arquivo .sql, digite a consulta SQL desejada e salve o arquivo.

5. No dispositivo com o Servidor de Administração instalado, na linha de comando, digite o seguinte comando para executar a consulta SQL do arquivo .sql e salvar os resultados no arquivo result.xml:

   ```
   sudo ./klsql2 -i src.sql -u <nome de usuário> -p <senha> -o result.xml
   ```

   onde `<nome de usuário>` e `<senha>` são as credenciais da conta de usuário que tem acesso ao banco de dados.

6. Caso seja necessário, digite o login e a senha da conta de usuário que tem acesso ao banco de dados.

7. Abra os arquivos result.xml criados recentemente para exibir os resultados da consulta SQL.

É possível editar o arquivo .sql e criar qualquer consulta SQL para as visualizações públicas. Então, da linha de comando, execute a sua consulta e salve os resultados em um arquivo.

Exemplo de uma consulta SQL no utilitário klsql2

Esta seção mostra um exemplo de uma consulta SQL, executada por meio do utilitário klsql2.

Os exemplos a seguir ilustram a recuperação dos eventos que ocorreram em dispositivos durante os últimos sete dias e exibe os eventos ordenados por horário de sua ocorrência. Os eventos mais recentes são exibidos primeiro.

Exemplo para PostgreSQL:

```
SELECT
  /* identificador do evento */
  "e"."nId",

  /* hora em que o evento ocorreu */
  "e"."tmRiseTime",

  /* nome interno do tipo de evento */
  "e"."strEventType",

  /* nome exibido do evento */
  "e"."wstrEventTypeDisplayName",

  /* descrição do evento exibida */
  "e"."wstrDescription",

  /* descrição do evento exibida */
  "e"."wstrGroupName",

  /* nome exibido do dispositivo no qual o evento ocorreu */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* endereço IP do dispositivo no qual o evento ocorreu */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Exemplo para MySQL ou MariaDB:

```
SELECT

  /* identificador do evento */
  `e`.`nId`,

  /* hora em que o evento ocorreu */
  `e`.`tmRiseTime`,

  /* nome interno do tipo de evento */
  `e`.`strEventType`,

  /* nome exibido do evento */
  `e`.`wstrEventTypeDisplayName`,

  /* descrição do evento exibida */
  `e`.`wstrDescription`,

  /* nome do grupo de dispositivos */
  `e`.`wstrGroupName`,

  /* nome exibido do dispositivo no qual o evento ocorreu */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* endereço IP do dispositivo no qual o evento ocorreu */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Exibir o nome de banco de dados do Kaspersky Security Center Linux

Caso queira acessar o banco de dados do Kaspersky Security Center Linux por meio das ferramentas de gerenciamento de banco de dados do MySQL ou MariaDB, será necessário conhecer o nome do banco de dados para poder se conectar a ele usando seu editor de script SQL.

Para exibir o nome do banco de dados do Kaspersky Security Center Linux:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Detalhes do banco de dados atual**.

O nome do banco de dados é especificado no campo **Nome do banco de dados**. Use o nome do banco de dados para endereçar o banco de dados nas suas consultas SQL.

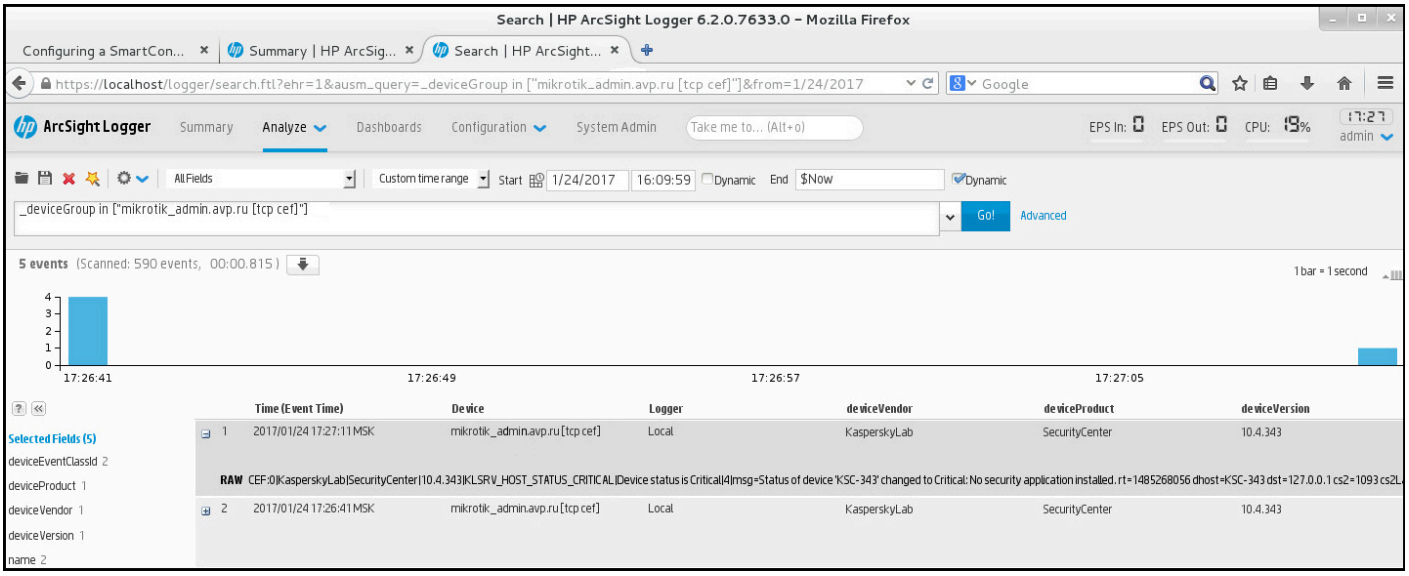
Exibir os resultados da exportação

Você pode controlar para a conclusão bem-sucedida do procedimento de exportação de eventos. Para fazer isto, verifique se as mensagens com eventos exportados são recebidas pelo seu sistema SIEM.

Se os eventos enviados do Kaspersky Security Center Linux forem recebidos e apropriadamente analisados pelo seu sistema SIEM, a configuração nos dois lados foi feita apropriadamente. De outra forma, verifique as configurações que você especificou no Kaspersky Security Center Linux contra a configuração no seu sistema SIEM.

A figura abaixo mostra os eventos exportados ao ArcSight. Por exemplo, o primeiro evento é crítico do Servidor de Administração: "*Status do dispositivo é crítico*".

A representação da exportação de eventos no sistema SIEM varia de acordo com o sistema SIEM que você usa.



Exemplo de eventos

Gerenciar revisões de objeto

Esta seção contém informações sobre o gerenciamento de revisão de objeto.

A *revisão* é o estado de um objeto em um determinado momento. Sempre que você cria ou modifica um objeto, uma nova revisão desse objeto é criada. Cada revisão contém todas as configurações do objeto como estavam no momento em que a revisão foi criada ou salva.

Os objetos suportam o gerenciamento de revisão incluem:

- Propriedades do Servidor de Administração
- Políticas
- Tarefas
- Grupos de administração
- Contas de usuário
- Pacotes de instalação

Você pode executar as seguintes ações nas revisões do objeto:

- Exibir uma revisão selecionada (disponível somente para políticas)
- Reverter as modificações feitas em um objeto para uma revisão selecionada
- Salvar as revisões como um arquivo JSON (disponível somente para políticas)

Na janela de propriedades de qualquer objeto que suporta o gerenciamento de revisão, a seção **Histórico de revisões** exibe uma lista de revisões de objeto com os seguintes detalhes:

- **Revisão** – Número de revisão do objeto.
- **Hora** – Data e hora em que o objeto foi modificado.
- **Usuário** - Nome do usuário que modificou o objeto.
- **Endereço IP do dispositivo do usuário** – Endereço IP do dispositivo a partir do qual o objeto foi modificado.
- **Endereço IP do Web Console** – Endereço IP do Kaspersky Security Center Web Console com o qual o objeto foi modificado.
- **Ação** - A ação executada no objeto.
- **Descrição** - A descrição da revisão em relação à modificação feita nas configurações do objeto.

  Por padrão, a descrição da revisão do objeto está em branco. Para adicionar uma descrição a uma revisão, selecione a revisão relevante e clique no botão **Editar descrição**. Na janela aberta, insira algum texto para a descrição da revisão.

Exibir e salvar uma revisão da política

Uma revisão de política é um estado salvo de uma política, criado automaticamente sempre que ela é alterada ou salva. Uma revisão contém as configurações da política, os perfis e as regras para sua ativação, além de metadados sobre a data de criação da revisão, o usuário que a criou e o endereço IP usado. O Kaspersky Security Center Linux permite exibir revisões de políticas para acompanhar as alterações nas configurações. Você também pode salvar uma revisão em um arquivo JSON.

A exibição e o salvamento de uma revisão de política estão disponíveis se o plug-in da web de gerenciamento correspondente for compatível com essa funcionalidade.
As opções estão disponíveis para as políticas do Servidor de Administração, do Agente de Rede, do Kaspersky Endpoint Security for Windows (a partir da versão 14.0 do plug-in da web), do Kaspersky Endpoint Security for Linux (a partir da versão 12.4 do plug-in da web) e do Kaspersky Endpoint Security for Mac (a partir da versão 12.2.1 patch A do plug-in da web).

Para visualizar uma revisão da política:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.
2. Clique na política da revisão que deseja visualizar e vá para a seção **Histórico de revisões**.
3. Na lista de revisões de política, clique no número da revisão que deseja visualizar.

O relatório exibido fornece informações sobre as configurações da política, seus perfis e as regras de ativação desses perfis.

Se o tamanho da revisão for superior a 10 MB, não poderá visualizá-la usando o Kaspersky Security Center Web Console. Você será solicitado a salvar a revisão selecionada em um arquivo JSON.

Se o tamanho da revisão não exceder 10 MB, um relatório no formato HTML com as configurações da revisão de política selecionada será exibido. Como o relatório é exibido em uma janela pop-up, assegure-se de que os pop-ups sejam permitidos em seu navegador.

Para as políticas do Kaspersky Endpoint Security for Windows e do Kaspersky Endpoint Security for Mac, o relatório não conterá informações sobre os perfis da política.

Para salvar uma revisão de política em um arquivo JSON,

Na lista de revisões de política, selecione a revisão que deseja salvar e clique em **Salvar no arquivo**.

A revisão é salva em um arquivo JSON.

Se necessário, você pode comparar as revisões da política.

Comparar as revisões de uma política

Você pode comparar revisões anteriores de uma política com a atual, comparar diferentes revisões selecionadas na lista ou comparar uma revisão de uma política com a revisão de outra. As opções estão disponíveis para as políticas do Servidor de Administração, Agente de Rede, Kaspersky Endpoint Security for Windows (a partir da versão 14.0 do plug-in da web) e Kaspersky Endpoint Security for Mac (a partir da versão 12.2.1 Patch A do plug-in da web).

A comparação de revisões de políticas está disponível se os plug-ins da web de gerenciamento correspondentes oferecerem suporte a essa funcionalidade.

Para comparar revisões de uma política:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.
2. Clique na política cujas revisões você deseja comparar.

   A janela Propriedades da política será aberta.
3. Vá para a guia **Histórico de revisões** e marque as caixas de seleção ao lado das revisões a serem comparadas.

4. Na barra de ferramentas, clique no botão **Comparar** e, na lista suspensa, selecione uma das seguintes opções:

   - **Com a revisão atual**, se desejar comparar a revisão selecionada na etapa 3 com a última revisão salva da mesma política.
   - **Revisões selecionadas**, se você quiser comparar as duas revisões cujas caixas de seleção você marcou na etapa 3.

     A ordem de seleção das caixas de seleção não afeta os resultados da comparação. Por padrão, a revisão anterior da que foi selecionada é comparada com a revisão mais recente. Por exemplo, se você marcar as caixas de seleção ao lado das revisões 5 e 1, a revisão 1 será comparada à revisão 5. O relatório conterá informações sobre as configurações na revisão 1 que foram adicionadas, removidas ou alteradas em comparação com a revisão 5.

   - **Com outra revisão da política**, se você quiser comparar as revisões de duas políticas diferentes.

     No painel esquerdo que é exibido, execute uma das seguintes ações:

     a. No campo **Nome do aplicativo**, selecione a política que deseja comparar: Agente de Rede ou Servidor de Administração.

     b. No campo **Nome da política**, informe o nome da política cuja revisão você deseja comparar com aquela selecionada na etapa 3.

        A lista de revisões da política é exibida.

     c. Selecione a revisão desejada e clique no botão **Comparar**.

Um relatório sobre a comparação das revisões é exibido no formato HTML em uma nova guia do navegador.

Se o resultado da comparação exceder 10 MB, a caixa de diálogo correspondente será exibida. Você pode clicar no botão **Salvar como arquivo** para salvar o relatório como um arquivo, ou cancelar a operação.

O relatório é exibido no idioma da interface do Kaspersky Security Center Web Console. Você pode expandir algumas seções do relatório clicando no ícone de seta para baixo (▾) ao lado da seção, ou recolher a seção clicando no ícone de seta para cima (▴).

O relatório contém as seguintes informações:

- Logotipo da Kaspersky.
- O nome do relatório.
- Data e hora da criação do relatório.
- O nome da política, o Servidor de Administração e o grupo de administração que inclui a política (políticas) cujas revisões foram comparadas.
- O botão **Salvar como HTML**. Se você clicar no botão, o relatório será salvo no seu computador.

- A seção **Resumo** que exibe informações gerais sobre as revisões comparadas: nome da política (políticas), número, data e hora em que a revisão foi salva, além do usuário que salvou a revisão e a descrição da revisão.

  Para políticas herdadas, o usuário não é exibido.

- Diferenças entre as revisões comparadas. As diferenças são exibidas nas seguintes seções:

  - **Configurações adicionadas**
  - **Configurações removidas**
  - **Configurações alteradas**
  - **Configurações disponíveis somente para o objeto 1** (se você comparou as revisões de duas políticas diferentes)
  - **Configurações disponíveis somente para o objeto 2** (se você comparou as revisões de duas políticas diferentes)

  Uma seção não é exibida se não tiver dados.

Reverter um objeto para uma revisão anterior

Você poderá reverter as alterações feitas à um objeto, se necessário. Por exemplo, você poderá ter que reverter as configurações de uma política ao seu estado em uma data específica.

Para reverter as alterações feitas à um objeto:

1. Na janela de propriedades do objeto, abra a guia **Histórico de revisões**.
2. Na lista de revisões do objeto, selecione a revisão para a qual você precisa reverter as modificações.
3. Clique no botão **Reverter**.
4. Clique em **OK** para confirmar a operação.

   O objeto é agora revertido à revisão selecionada. A lista de revisões de objeto exibe um registro da ação que foi executada. A descrição da revisão exibe as informações sobre o número da revisão à qual você reverteu o objeto.

A operação de reversão está disponível apenas para objetos de política e tarefa.

Ameaças ativas

As informações sobre arquivos não processados encontrados em dispositivos cliente são armazenadas na seção **Repositórios**, subseção **Ameaças ativas**.

O processamento e a desinfeção adiados são executados pelo aplicativo de segurança quando da solicitação ou após que um evento especificado ocorra. Você pode configurar o processamento adiado.

Desinfeção de um arquivo não processado

Para iniciar a desinfeção de um arquivo não processado:

1. No menu principal, vá para **Repositórios** → **Ameaças ativas**.
2. Execute uma das seguintes ações:
   - Marque a caixa de seleção ao lado do arquivo que deve ser desinfectado.
   - Clique no nome do arquivo que deve ser desinfectado.
3. Inicie a desinfecção do arquivo clicando no botão **Desinfectar**.

   A tentativa de desinfectar o arquivo selecionado é então realizada.

Se o arquivo estiver desinfectado, o aplicativo de segurança instalado no dispositivo cliente o restaura para sua pasta original. O registro do arquivo é removido da lista na seção **Ameaças ativas**. Se o arquivo não puder ser desinfectado, o aplicativo de segurança instalado no dispositivo o exclui daquele dispositivo. O registro do arquivo é removido da lista na seção **Ameaças ativas**.

O recurso de desinfecção e exclusão de arquivos pode variar dependendo de qual aplicativo de segurança está instalado, sua versão e configurações.

Baixando um arquivo não processado

O Kaspersky Security Center Linux permite baixar cópias de arquivos não processados encontrados em dispositivos cliente. Isso se refere a arquivos tratados ou excluídos pelo aplicativo. Os arquivos são baixados para a pasta especificada no dispositivo com o Kaspersky Security Center Linux instalado.

É possível baixar as cópias dos arquivos caso eles tenham sido excluídos ou modificados durante a desinfecção e suas cópias estejam armazenadas no armazenamento do Kaspersky Endpoint Security for Linux no dispositivo gerenciado.

Para baixar uma cópia de um arquivo não processado:

1. No menu principal, vá para **Repositórios** → **Ameaças ativas**.
2. Execute uma das seguintes ações:
   - Marque a caixa de seleção ao lado do arquivo que deseja baixar.
   - Clique no nome do arquivo que deve ser baixado.
3. Inicie o download clicando no botão **Baixar**.

O aplicativo de segurança instalado no dispositivo cliente no qual o arquivo não processado foi encontrado baixa uma cópia do arquivo na pasta especificada.

Exclusão de arquivos da seção Ameaças ativas

*Para excluir um arquivo da seção **Ameaças ativas**:*

1. No menu principal, vá para **Repositórios** → **Ameaças ativas**.
2. Execute uma das seguintes ações:
   - Marque a caixa de seleção ao lado do arquivo que deseja excluir.
   - Clique no nome do arquivo que deve ser excluído.
3. Exclua os arquivos clicando no botão **Excluir**.
4. Na janela exibida, clique em **Excluir**.

Os aplicativos de segurança que colocaram arquivos nos repositórios em dispositivos clientes excluirão esses arquivos desses repositórios. Os registros dos arquivos são removidos da lista na seção **Ameaças ativas**.

Exclusão de objetos

Esta seção fornece informações sobre como excluir objetos.

Você pode excluir objetos, como os seguintes:

- Políticas
- Tarefas
- Pacotes de instalação
- Servidores de Administração virtual
- Usuários

- Grupos de segurança
- Grupos de administração

Para excluir um objeto:

1. Abra a seção necessária do Kaspersky Security Center Web Console e selecione o objeto.
2. Na barra de ferramentas, clique no botão **Excluir**.
3. Na janela que se abre, clique em **OK** para confirmar a sua seleção.

O objeto selecionado será excluído.

Quando você exclui um objeto, as informações sobre ele permanecem no banco de dados. O período de armazenamento das informações sobre os objetos excluídos é igual ao período de armazenamento das revisões de objetos (o período recomendado é de 90 dias). Você pode alterar o prazo de armazenamento somente se tiver a permissão **Modificar** na área de direitos **Objetos excluídos**.

Sobre a exclusão de dispositivos clientes

Quando um dispositivo gerenciado é excluído de um grupo de administração, o aplicativo move o dispositivo para o grupo dispositivos não atribuídos. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados, o Agente de Rede e qualquer aplicativo de segurança, por exemplo, o Kaspersky Endpoint Security, permanecem no dispositivo.

O Kaspersky Security Center Linux gerencia os dispositivos no grupo Dispositivos não atribuídos de acordo com as seguintes regras:

- Caso tenha configurado as regras de movimentação de dispositivo e um dispositivo atenda aos critérios de uma regra de movimentação, o dispositivo é automaticamente movido para um grupo de administração de acordo com a regra.
- O dispositivo é armazenado no grupo Dispositivos não atribuídos e é automaticamente removido do grupo de acordo com as regras de retenção de dispositivos.

  As regras de retenção de dispositivo não afetam os dispositivos que têm uma ou mais unidades criptografadas com criptografia completa do disco. Esses dispositivos não são excluídos automaticamente. Somente é possível excluí-los manualmente. Caso necessite excluir um dispositivo com uma unidade criptografada, primeiro descriptografe a unidade e, em seguida, exclua o dispositivo.

  Ao excluir um dispositivo com unidade criptografada, os dados necessários para descriptografar a unidade também são excluídos. Se você marcar a caixa de seleção **Eu entendo o risco e desejo excluir os dispositivos selecionados** na janela de confirmação que é aberta quando você exclui esses dispositivos (do grupo **Dispositivos não atribuídos** ou **Dispositivos gerenciados**), significa que você está ciente da exclusão de dados.

Para descriptografar o dispositivo, as seguintes condições devem ser atendidas:

- O dispositivo é reconectado ao Servidor de Administração para restaurar os dados necessários para descriptografar a unidade.
- O usuário do dispositivo lembra a senha de descriptografia.
- O aplicativo de segurança usado para criptografar o dispositivo, por exemplo, o Kaspersky Endpoint Security for Windows, ainda está instalado nele.

Caso o dispositivo seja criptografado pela tecnologia Kaspersky Disk Encryption, também é possível tentar recuperar os dados usando o utilitário de restauração FDERT.

Na VDI, se você tiver um equipamento com unidades criptografadas, as informações na unidade criptografada serão excluídas após a exclusão do equipamento.

Quando um dispositivo é excluído manualmente do grupo dispositivos não atribuídos, o aplicativo remove o dispositivo da lista. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados (se houver) permanecem no dispositivo. Assim, caso o dispositivo ainda esteja visível para o Servidor de Administração e a sondagem regular de rede tenha sido configurada, o Kaspersky Security Center Linux descobre o dispositivo durante a sondagem de rede e o adiciona de volta ao grupo Dispositivos não atribuídos. Portanto, é razoável excluir um dispositivo manualmente somente se o dispositivo estiver invisível para o Servidor de Administração.

Baixar e excluir arquivos da Quarentena e do Backups de arquivo

Esta seção fornece informações sobre como baixar e excluir arquivos da Quarentena e do Backups de arquivo no Kaspersky Security Center Web Console.

Baixar arquivos da Quarentena e dos backups de arquivos

Você só pode baixar arquivos da Quarentena e dos backups de arquivos se uma das duas condições for atendida: ou a opção **Não desconectar do Servidor de Administração** estiver habilitada nas configurações do dispositivo, ou um gateway de conexão estiver em uso. Caso contrário, o download não será possível.

Para salvar uma cópia do arquivo da Quarentena ou do Backups de arquivo em um disco rígido:

1. Execute uma das seguintes ações:

   - Caso queira salvar uma cópia do arquivo da Quarentena, No menu principal, vá para **Operações** → **Repositórios** → **Quarentena**.

   - Caso queira salvar uma cópia do arquivo a partir do Backup, No menu principal, vá para **Operações** → **Repositórios** → **Backups de arquivo**.

2. Na janela que se abre, selecione um arquivo que deseja baixar e clique em **Baixar**.

   O download é iniciado. Uma cópia do arquivo que foi colocado em Quarentena no dispositivo cliente é salva na pasta especificada.

Sobre a remoção de objetos dos repositórios da Quarentena, do Backup de arquivos ou das Ameaças ativas

Quando os aplicativos de segurança da Kaspersky instalados em dispositivos cliente colocam objetos nos repositórios de Quarentena, Backup ou Ameaças ativas, eles enviam as informações sobre os objetos adicionados às seções **Quarentena**, **Backups de arquivo** ou **Ameaças ativas** no Kaspersky Security Center Linux. Ao abrir uma dessas seções, será possível remover o objeto desejado.

Para a seção **Backups de arquivo** ou **Ameaças ativas**, selecione um objeto na lista e clique no botão **Remover**.

Para a seção de **Quarentena**, é possível fazer o seguinte:

- Marque a caixa de seleção ao lado do nome de um objeto a ser removido e, na barra de ferramentas, clique no botão **Excluir**.

- Clique no nome do objeto a ser removido e, na janela de informações exibida, clique no botão **Excluir** na barra de ferramentas.

  Nesse caso, o objeto é excluído, uma notificação correspondente é exibida na tela e a janela de detalhes é fechada.

O Kaspersky Security Center Linux remove o objeto selecionado da lista ou o exclui do repositório. A ação a ser executada é definida pelo aplicativo da Kaspersky que colocou o objeto selecionado no repositório. O aplicativo da Kaspersky é especificado no campo **Entrada adicionada por**.

Para obter informações sobre qual ação deve ser executada, consulte a documentação do aplicativo da Kaspersky.

Gerenciamento do aplicativo pelo SNMP

Esta seção descreve como obter informações do Servidor de Administração usando SNMP (Protocolo de Gerenciamento de Rede Simples) no Linux.

SNMP é um protocolo para gerenciar dispositivos de rede.

Para funcionar via SNMP, o Kaspersky Security Center Linux usa o serviço snmpd incluído no sistema operacional e um agente SNMP para monitorar o desempenho do Servidor de Administração e enviar dados para aplicativos auxiliares usando OIDs. A Kaspersky Security Center Linux pode enviar essas informações na forma de estatísticas ou interceptações SNMP, que são notificações sobre eventos do aplicativo.

O SNMP permite acessar as seguintes informações sobre o aplicativo:

- Informações gerais
- Estatísticas da Kaspersky Security Center Linux desde a instalação do aplicativo
- Informações sobre eventos da Kaspersky Security Center Linux

O acesso somente leitura é concedido.

As informações sobre interceptações SNMP e estatísticas enviadas por SNMP são armazenadas no arquivo adminkit.mib. Por padrão, o arquivo adminkit.mib está localizado na pasta /opt/kaspersky/ksc64/share/snmp/.

O serviço snmpd local em cada nó do cluster serve como o servidor SNMP que recebe as estatísticas. A interação com um servidor SNMP externo não é permitida. As interceptações SNMP podem ser recebidas usando o serviço snmptrapd localmente em cada nó de cluster ou podem ser redirecionadas para um servidor externo.

Para operações via SNMP, pré-configure o serviço snmpd no sistema operacional em cada nó de cluster.

Configuração do serviço snmpd no sistema operacional

Antes de configurar, certifique-se de que o serviço snmpd esteja instalado em seu sistema operacional.

Criação de uma conta de usuário para acessar os dados

Antes de criar a conta, pare o serviço snmpd executando o seguinte comando:

```
bash
sudo systemctl stop snmpd
```

Para garantir a segurança do acesso aos dados por meio de SNMPv3 com autenticação e criptografia, você precisa criar uma conta de usuário no serviço snmpd com as seguintes informações:

- Nome de usuário (diferencia maiúsculas de minúsculas)
- Algoritmo de autenticação (MD5 ou SHA. SHA é recomendado)
- Senha de autenticação
- Algoritmo de criptografia (compatível somente com AES)
- Senha de criptografia

Você pode criar uma conta de usuário das seguintes formas:

- Usando o utilitário net-snmp-create-v3-user, se disponível no sistema operacional.
- Manualmente, adicionando a diretiva apropriada ao arquivo de configuração do serviço snmpd.

Para criar uma conta de usuário usando o utilitário net-snmp-create-v3-user, execute o seguinte comando:

```
net-snmp-create-v3-user -ro -a <algoritmo de autenticação> -x <algoritmo de criptografia> <nome de usuário>
```

As senhas de autenticação e criptografia são solicitadas interativamente.

Por exemplo:

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

Para criar uma conta de usuário manualmente:

1. Crie o arquivo de configuração /var/lib/snmp/snmpd.conf executando o seguinte comando:

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. Adicione as seguintes linhas ao arquivo de configuração:

   ```
   createUser <nome de usuário> <algoritmo de autenticação> "<senha de autenticação>" <algoritmo de criptografia>
   "<senha de criptografia>"
   ```

   Por exemplo:

   ```
   createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
   ```

Criação de uma conta de usuário para receber interceptações SNMP

Para receber interceptações SNMP sobre SNMPv3 com autenticação e criptografia, você precisa criar uma conta no sistema de monitoramento no contexto do serviço correspondente (geralmente o serviço snmptrapd).

A conta deve conter as seguintes informações:

- Nome de usuário
- Algoritmo de autenticação
- Senha de autenticação

- Encryption algorithm
- Senha de criptografia

Para fins de segurança, use contas de usuário separadas para acessar os dados e receber as interceptações SNMP.

Para obter instruções sobre como criar uma conta de usuário para receber interceptações SNMP, consulte a documentação do seu sistema de monitoramento.

Configuração do serviço snmpd

A configuração do serviço snmpd é armazenada no arquivo /etc/snmp/snmpd.conf. É possível adicionar as informações necessárias a um arquivo de configuração existente ou criar um novo arquivo de configuração e adicionar as linhas listadas abaixo na ordem especificada.

Se você optar por criar um novo arquivo de configuração, certifique-se de que somente o superusuário tenha acesso a ele. Se as permissões de acesso necessárias não estiverem definidas, configure-as executando os seguintes comandos na ordem especificada:

```
chown root:root /etc/snmp/snmpd.conf
chmod 600 /etc/snmp/snmpd.conf
```

Para configurar o serviço snmpd:

1. No arquivo de configuração, informe o protocolo, o endereço da interface de rede e o número da porta em que o serviço snmpd deve escutar as solicitações recebidas.

   - Se você quiser ouvir solicitações em todas as interfaces de rede, adicione as seguintes linhas ao arquivo de configuração:

     ```
     agentAddress udp:161
     ```

   - Se você quiser ouvir solicitações somente na interface de rede local, por exemplo, se o sistema de monitoramento estiver instalado na mesma máquina, adicione as seguintes linhas ao arquivo de configuração:

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. Configure a interação entre o Kaspersky Security Center Linux e o serviço snmpd. Você pode usar um soquete UNIX ou um soquete TCP.

   - Se você usar um soquete UNIX:

     a. Especifique o caminho e as permissões para o soquete UNIX. Para fazer isso, adicione as seguintes linhas ao arquivo de configuração:

     ```
     master agentx
     agentXSocket unix:/var/run/agentx-master.socket
     agentXPerms 770 770 kluser klusers
     ```

     b. Adicione o grupo klusers como um grupo suplementar para a conta {'KLSRV_UNATT_KLSVCUSER'}.

   - Se você usar um soquete TCP, especifique a porta e o endereço dele. Para fazer isso, adicione as seguintes linhas ao arquivo de configuração:

     ```
     master agentx
     agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
     ```

3. Defina o tempo limite de resposta mínimo para pelo menos 30 segundos. Para fazer isso, adicione as seguintes linhas ao arquivo de configuração:

   ```
   agentxTimeout 30
   ```

4. Se necessário, você pode fornecer uma descrição do servidor onde o SNMP está configurado, a localização do sistema e o endereço de contato do administrador. Para fazer isso, adicione as seguintes linhas ao arquivo de configuração:

   ```
   sysDescr <descrição do servidor>
   sysLocation <localização do servidor>
   sysContact <endereço de contato do administrador>
   sysServices 72
   ```

5. Especifique o escopo da árvore OID que você deseja que esteja disponível para seu sistema de monitoramento por meio do protocolo SNMP. Para fazer isso, adicione as seguintes linhas ao arquivo de configuração:

   ```
   view monitoring included .1.3.6.1.4.1.23668.1093.1

   view systemonly included .1.3.6.1.4.1.23668.1093.1
   ```

6. Se necessário, você também pode especificar o escopo da árvore OID que contém informações sobre o sistema operacional armazenado pelo serviço snmpd. Este escopo estará disponível no seu sistema de monitoramento.

As informações sobre o sistema operacional incluem, por exemplo, informações sobre o uso da CPU e da RAM, espaço livre nas partições do disco, carga das interfaces de rede, além de uma lista de softwares instalados, uma lista de conexões de rede abertas e uma lista de processos em execução. Parte dessas informações pode ser confidencial.

- Se você quiser permitir o acesso somente a informações gerais do sistema e informações sobre o uso da RAM, CPU e dispositivos de disco, adicione as seguintes linhas ao arquivo de configuração:

```
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

- Se você quiser permitir o acesso a todas as informações do sistema, adicione as seguintes linhas ao arquivo de configuração:

```
view monitoring included .1
```

7. Especifique o modo de acesso e o escopo das informações para a conta de usuário criada. Para fazer isso, adicione as seguintes linhas ao arquivo de configuração:

```
rouser <user name> priv -V monitoring
```

8. Para enviar interceptações SNMP, informe o endereço IP do sistema de monitoramento e as credenciais de usuário para receber interceptações. Para fazer isso, adicione as seguintes linhas ao arquivo de configuração:

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <nome de usuário para o recebimento de interceptações> -a <algoritmo
de autenticação> -A "<senha do usuário para o recebimento de interceptações>" -x <algoritmo de criptografia> -X
"<senha de criptografia>" udp:<endereço IP>:162
```

O serviço snmpd está configurado.

Para fazer a integração com vários sistemas de monitoramento, crie uma conta de usuário separada para cada sistema, informe o escopo das informações disponíveis para cada conta de usuário (as diretivas 'view' e 'rouser') e configure o envio de interceptações SNMP (a diretiva 'trapsess').

Iniciar o serviço snmpd com a nova configuração

Para aplicar a nova configuração:

1. Reinicie o serviço snmpd:

   ```
   systemctl restart snmpd
   ```

2. Verifique o status do serviço snmpd:

   ```
   systemctl status snmpd
   ```

   O status deve ser `running`.

3. Permitir que o serviço seja iniciado automaticamente na inicialização do sistema operacional:

   ```
   systemctl enable snmpd
   ```

4. Se você estiver usando um firewall no seu sistema operacional ou equipamento de rede, adicione regras para permitir o envio de pacotes SNMP.

O serviço snmpd está em execução.

Se o serviço klcssnmp estava em execução no momento em que o serviço snmpd foi configurado, reinicie o serviço klcssnmp também.

Verificação da integridade do serviço snmpd

Para testar o serviço snmpd, configure o uso do SNMP no Kaspersky Security Center Linux e solicite dados SNMP por meio do utilitário snmpwalk.

Para obter os escopos dos dados SNMP fornecidos pela Kaspersky Security Center Linux,

execute o seguinte comando:

```
snmpwalk -v3 -l authPriv -u <nome de usuário> -a <algoritmo de autenticação> -A "<senha de autenticação>" -x
<algoritmo de criptografia> -X "<senha de criptografia>" <endereço IP> .1.3.6.1.4.1.23668.1093.1
```

Por exemplo:

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

Ativar e desativar as notificações por SNMP

O Kaspersky Security Center Linux envia notificações sobre eventos do Servidor de Administração na forma de interceptações SNMP.

Por padrão, as notificações SNMP para eventos da Kaspersky Security Center Linux são desativadas.

Para ativar ou desativar as notificações por SNMP para eventos da Kaspersky Security Center Linux:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela **Propriedades do Servidor de Administração** é aberta.

2. Na guia **Configuração de eventos** da janela de propriedades, clique no tipo de evento para o qual você deseja receber notificações SNMP.

3. No painel que se abre, ative ou desative o botão de alternância **Notificar via SNMP**.

   Esta opção está disponível somente se a opção **Enviar estatísticas via SNMP** estiver ativada.

As notificações SNMP para eventos da Kaspersky Security Center Linux são ativadas ou desativadas de acordo com sua seleção.

Ativar e desativar o SNMP na Kaspersky Security Center Linux

Por padrão, o envio de estatísticas por SNMP está ativado. Para enviar interceptações SNMP, configure o serviço snmpd.

Para ativar ou desativar o envio de estatísticas por SNMP:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela **Propriedades do Servidor de Administração** é aberta.

2. Na guia **Geral**, selecione a seção **SNMP**.

3. Ative ou desative o botão de alternância **Enviar estatísticas via SNMP**.

4. Clique no botão **Salvar**.

O envio de estatísticas por SNMP é ativado ou desativado de acordo com sua seleção.

Valores de identificadores de objetos para SNMP

A tabela abaixo mostra os valores e descrições dos identificadores de objetos (também chamados de OIDs), usados para transferir informações sobre o desempenho do Servidor de Administração para aplicativos de terceiros.

Valor do identificador de objeto	Tipo de dados numérico	OID	Descrição
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	Status de implementação. O status pode ser um dos seguintes: • **Informação**. A licença não é mais válida para N dispositivos. • **Advertência**. Um dos seguintes: Há M dispositivos com aplicativos Kaspersky instalados em um total de N dispositivos nos grupos do Servidor de Administração (N > M). A licença L irá expirar em N dispositivos em M dias. A tarefa T de instalação de aplicativos foi concluída com êxito em N dispositivos. É necessário reiniciar para M dispositivos. • **Crítico** Licença expirada para N dispositivos. • **OK**. Nenhuma das opções acima.
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	`deploymentStatus` mostra que o grupo do Servidor de Administração contém muitos dispositivos sem aplicativos gerenciados. O valor é igual a 1 se houver dispositivos sem aplicativos gerenciados e 0, caso contrário.
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	`deploymentStatus` mostra que a tarefa de instalação remota falhou em alguns dispositivos. O número desses dispositivos pode ser obtido via `hostsRemoteInstallFailed`.
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	`deploymentStatus` mostra que há alguns dispositivos com uma licença que expira nos próximos 7 dias. O número desses dispositivos pode ser obtido via `hostsLicenseExpiring`.
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	`deploymentStatus` mostra que há alguns dispositivos com uma licença expirada. Você pode obter a quantidade desses dispositivos via `hostsLicenseExpired`.
`hostsInGroups`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.3	Número de dispositivos nos grupos do Servidor de Administração.
`hostsWithAntivirus`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.4	Número de dispositivos nos grupos do Servidor de Administração com aplicativos gerenciados instalados.
`hostsRemoteInstallFailed`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.5	Número de dispositivos nos quais a tarefa de instalação remota falhou.
`licenceExpiringSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.6	ID de uma chave de licença que expira em menos de 7 dias.
`licenceExpiredSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.7	ID da chave de licença expirada.
`licenceExpiringDays`	`Unsigned32`	.1.3.6.1.4.1.23668.1093.1.1.8	Número de dias antes do término de uma licença. Para esse parâmetro, o período da licença é considerado expirado caso haja menos de 7 dias restantes até a data de término. Caso haja mais de 7 dias restantes até a data de término, o valor será 0.
`hostsLicenceExpiring`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.9	Número de dispositivos com uma licença que expira em menos de 7 dias.
`hostsLicenceExpired`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.10	Número de dispositivos com uma licença expirada.

Valor do identificador de objeto	Tipo de dados numérico	OID	Descrição
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Status atual da atualização das bases de antivírus. O status pode ser um dos seguintes: • **Informação**. As bases de antivírus no Servidor de Administração ou nos dispositivos não foram atualizadas por mais de um dia, e menos de um dia se passou desde a instalação do aplicativo. • **Advertência**. As bases de antivírus no Servidor de Administração ou nos dispositivos não foram atualizadas por mais de 3 dias. Esse valor pode ser alterado nas configurações do grupo. • **Crítico** As bases de antivírus no Servidor de Administração ou nos dispositivos não foram atualizadas por mais de 7 dias. Esse valor pode ser alterado nas configurações do grupo. • **OK**. Nenhuma das opções acima.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	O Servidor de Administração não é atualizado há muito tempo. A quantidade de tempo considerada longa é especificada em `updatesStatus`.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Alguns dispositivos não foram atualizados há bastante tempo (por padrão, 7 dias ou mais para **Crítico** e 3 dias para **Advertência**). Você pode obter a quantidade desses dispositivos via `hostsNotUpdated`.
lastServerUpdateTime	Hex-STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Última vez que os bancos de antivírus foram atualizados no Servidor de Administração.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Número de dispositivos que contêm bancos de antivírus que não são atualizados há bastante tempo (por padrão, 7 dias ou mais para **Crítico** e 3 dias para **Advertência**). Se houver dispositivos com o status de atualização **Crítico**, somente esses dispositivos serão contabilizados. Você pode obter o status de atualização via `updatesStatus`.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Status da proteção em tempo real. Um dos seguintes: • **Advertência**. Um dos seguintes: Uma violação de segurança é detectada em um dispositivo que pertence ao grupo do Servidor de Administração. Erros de criptografia provocaram a alteração de status de proteção de alguns dispositivos. Verificação completa não foi executada há muito tempo. • **Crítico** A proteção antivírus não está funcionando em alguns dispositivos nos grupos do Servidor de Administração. • **OK**. Nenhuma das opções acima.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Um aplicativo de segurança não está sendo executado em alguns dispositivos. Você pode obter o número desses dispositivos via `hostsAntivirusNotRunning`.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	A proteção em tempo real não está sendo executada em alguns dispositivos. Você pode obter o número desses dispositivos via `hostsRealtimeNotRunning`.
psRealtimeLevelChanged	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.3	O nível de proteção durante o tempo de execução é diferente do nível definido pelo administrador em N computadores em grupos de administração.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Há dispositivos que contêm objetos não desinfectados. Você pode obter a quantidade desses dispositivos via `hostsNotCuredObject`.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Foram encontradas ameaças em alguns dispositivos. Você pode obter a quantidade desses dispositivos via `hostsTooManyThreats`.

Valor do identificador de objeto	Tipo de dados numérico	OID	Descrição
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Status de infecção por vírus do sistema. O valor é igual a 1 se uma determinada quantidade de vírus foi encontrada durante um determinado período de tempo e 0, caso contrário. A quantidade de vírus e o tempo são especificados no Servidor de Administração, usando as configurações de `Virus attack`.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	Foram detectadas vulnerabilidades.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	Foram detectados erros de criptografia que alteraram o status de proteção do dispositivo.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	Foram detectadas vulnerabilidades em alguns dispositivos.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	Foram detectados dispositivos que não passaram por uma verificação completa por um longo período.
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	Foram detectados dispositivos nos quais o Agente de Rede é iniciado apenas após uma reinicialização.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Quantidade de dispositivos sem aplicativos de segurança sendo executados.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Quantidade de dispositivos sem proteção em tempo real sendo executados.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Quantidade de dispositivos com proteção em tempo real inaceitável.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Quantidade de dispositivos contendo objetos não desinfectados.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Quantidade de dispositivos contendo ameaças.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	O status da verificação completa do antivírus é um dos seguintes: • **Informação**. Menos 7 dias se passaram desde a instalação do aplicativo. • **Advertência**. A verificação completa do Antivírus não foi realizada por mais de 7 dias desde a instalação do aplicativo. • **Crítico** A verificação completa do Antivírus não foi realizada por mais de 14 dias desde a instalação do aplicativo. • **OK**. Nenhuma das opções acima.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Alguns dispositivos não foram verificados por um determinado período. Você pode obter a quantidade desses dispositivos via `hostsNotScannedLately`. A quantidade de tempo é especificada em `fullScanStatus`.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Quantidade de dispositivos que não foram verificados por um determinado período. A quantidade de tempo é especificada em `fullScanStatus`.

Valor do identificador de objeto	Tipo de dados numérico	OID	Descrição
`logicalNetworkStatus`	`INTEGER { ok(0), warning(1), critical(2) }`	.1.3.6.1.4.1.23668.1093.1.5.1	Status da rede lógica do Servidor de Administração. Um dos seguintes: • **Advertência**. Se houver dispositivos com status de aviso que não podem ser acessados ou se houver dispositivos que não pertençam a nenhum grupo do Servidor de Administração. • **Crítico** Se houver dispositivos cujo controle foi perdido pelo Servidor de Administração ou se houver dispositivos com um status crítico e que não podem ser acessados. • **OK**. Nenhuma das opções acima.
`notConnectedLongTime`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.1	Alguns dispositivos não foram conectados ao Servidor de Administração há bastante tempo (7 dias ou mais para um dispositivo com status de **Advertência** e 4 dias para um dispositivo com status **Crítico**). Você pode obter a quantidade desses dispositivos via `hostsNotConnectedLongTime`.
`controlLost`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.2	Há dispositivos cujo controle foi perdido pelo Servidor de Administração. Você pode obter a quantidade desses dispositivos via `hostsControlLost`.
`hostsFound`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.3	Quantidade de dispositivos encontrados pelo Servidor de Administração que não pertencem a nenhum grupo do Servidor de Administração.
`groupsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.4	Quantidade de grupos no Servidor de Administração.
`hostsNotConnectedLongTime`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.5	Quantidade de dispositivos que não estão conectados ao Servidor de Administração há muito tempo. A quantidade de tempo considerada longa é especificada em `notConnectedLongTime`.
`hostsControlLost`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.6	Quantidade de dispositivos que não controlados pelo Servidor de Administração.
`eventsStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.6.1	O status do subsistema de eventos é um dos seguintes: • **Advertência**. Um dos seguintes: Dispositivos do grupo do Servidor de Administração não procuraram por atualizações do Windows há muito tempo. Há dispositivos com problemas de status. • **Crítico** Um dos seguintes: Há um evento "Crítico" em pelo menos um dispositivo. Há um evento de "Erro" em pelo menos um dispositivo. Há um evento de conclusão de tarefa sem sucesso em pelo menos um dispositivo. Dispositivos do grupo do Servidor de Administração não procuraram por atualizações do Windows há muito tempo. Há dispositivos com problemas de status. • **Informações** Um dos seguintes: Menos de uma semana se passou desde a última verificação completa de vírus em todos os dispositivos. As tarefas de instalação remota foram concluídas e nenhum dispositivo precisa ser reiniciado. Menos de uma semana se passou desde a última atualização do Servidor de Administração. O Servidor de Administração não é atualizado há muito tempo, mas uma atualização está em andamento. • **OK**. Nenhuma das opções acima.

Valor do identificador de objeto	Tipo de dados numérico	OID	Descrição
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	`eventsStatus` mostra que existem alguns eventos críticos no Servidor de Administração. Você pode obter a quantidade desses eventos via `criticalEventsCount`. O valor é igual a 1 se houver pelo menos um evento crítico em qualquer dispositivo e 0, caso contrário.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Número de eventos críticos no Servidor de Administração.

Trabalhando com o Kaspersky Security Center Linux sob o licenciamento Kaspersky Next XDR Optimum

Se você adquiriu uma licença do Kaspersky Next XDR Optimum como parte de uma licença do aplicativo EPP e uma licença do Kaspersky Security Center Linux, poderá usar a funcionalidade do Kaspersky Next XDR Optimum depois de executar a configuração inicial.

Se você adquiriu uma licença separada do Kaspersky Next XDR Optimum como extensão de uma licença adquirida anteriormente, após instalar e ativar os aplicativos da Kaspersky nos dispositivos, será necessário reativar o Kaspersky Security Center Linux neles usando o novo código de ativação ou arquivo de chave, dependendo da forma como a licença do Kaspersky Next XDR Optimum foi adquirida. Depois disso, execute a configuração inicial.

Além disso, é possível utilizar a funcionalidade do Kaspersky Next XDR Optimum no modo de teste. Para fazer isso, você deve primeiro adicionar um Servidor de Administração físico secundário e, depois, ativar esse Servidor com uma licença de avaliação do Kaspersky Next XDR Optimum. A funcionalidade Kaspersky Next XDR Optimum estará disponível no Servidor secundário durante o período de validade da sua licença de avaliação.

Depois de ativar o Servidor de Administração com sua licença do Kaspersky Next XDR Optimum e implementar a chave de licença nos dispositivos gerenciados pelo Servidor de Administração correspondente, você pode fazer o seguinte:

- Responda a ameaças usando integrações com a Kaspersky Automated Security Awareness Platform, o Kaspersky Threat Intelligence Portal Sandbox e o Active Directory.
- Agrupe alertas por atributos.

Para obter mais informações sobre os recursos ativados pelo Licenciamento do Kaspersky Next XDR Optimum, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum.

Integrações para responder a alertas

Se tiver o licenciamento do Kaspersky Next XDR Optimum, poderá configurar integrações com as seguintes soluções para responder a ameaças:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Essas integrações estarão disponíveis se você tiver ativado o Servidor de Administração com uma licença do Kaspersky Next XDR Optimum.
Para executar ações de resposta, você deve implantar a chave de licença do Kaspersky Next XDR Optimum nos aplicativos gerenciados.
Ao usar a funcionalidade Kaspersky Next XDR Optimum com uma licença de avaliação, você deve primeiro adicionar um Servidor de Administração físico secundário, ativá-lo com a licença de avaliação e, depois, implantar a chave de licença nos dispositivos gerenciados por esse Servidor de Administração.

Se estiver usando o licenciamento do Kaspersky Next EDR Optimum, não é necessário ativar os aplicativos instalados nos dispositivos gerenciados sob o licenciamento do Kaspersky Next XDR Optimum. Isso deve ser feito apenas para novos dispositivos, se houver.

Como a licença do Kaspersky Next XDR Optimum permite a multilocação, você pode distribuir centralmente a chave de licença para aplicativos gerenciados. A distribuição automática da licença para Servidores de Administração secundários e virtuais não é compatível.

Para configurar as integrações, você deve ter os direitos **Ler** e **Gravar** para os **recursos Gerais: Área funcional Integração de aplicativos**.

Configurar a integração com o Active Directory para executar ações de resposta

A integração com o Active Directory permite executar ações de resposta para usuários do Active Directory afetados ou envolvidos no alerta.

Para configurar a integração com o Active Directory para responder a alertas, você deve usar o Servidor de Administração Kaspersky Security Center Linux versão 15.4 ou posterior.

A integração com o Active Directory para responder a alertas e as configurações para verificar o controlador de domínio do Active Directory (o endereço e as credenciais do usuário do controlador de domínio) especificadas ao configurar uma sondagem do controlador de domínio são duas configurações diferentes. Você deve garantir que o usuário para o qual uma ação de resposta deve ser executada tenha uma conta do Active Directory. Para isso, deve configurar ambas as integrações: para verificação e para responder. A ordem não é relevante.

As configurações de integração não são herdadas e são aplicadas somente ao Servidor de Administração (servidor físico ou virtual) no qual você define essas configurações.

Para configurar a integração com o Active Directory para responder a alertas:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Execute uma das seguintes ações:

   - Selecione a seção **Pontos de distribuição**, clique no nome do ponto de distribuição desejado e, na janela de propriedades exibida, selecione a seção **Active Directory**.

   - Selecione a seção **Resposta do Active Directory**.

3. No painel direito, ative o botão de alternância **Integração do Active Directory**.

   Posteriormente, se você quiser desativar a integração, só poderá fazê-lo para todas as conexões desativando o botão de alternância **Integração do Active Directory**. Você não pode desativar a integração para uma conexão separada. Em vez disso, pode excluir a conexão.

   > Ao ativar ou desativar o botão de alternância **Integração do Active Directory**, a configuração é aplicada tanto à seção **Resposta do Active Directory** quanto à seção **Pontos de distribuição**.

4. Crie uma conexão com o controlador de domínio do Active Directory, clicando no botão **Adicionar**.

5. Na janela aberta, especifique os seguintes parâmetros para a conexão:

   - **Endereço do controlador de domínio**

     Nome do computador, por exemplo: `server.mycompany.com`.

     Você pode especificar vários endereços. Todos os controladores de domínio cujos endereços você especificar devem pertencer ao mesmo domínio.

   - **Nome de domínio do Active Directory**

     Nome de domínio DNS totalmente qualificado, por exemplo: `mycompany.com`

     Além disso, você pode especificar um nome SAM ou NetBIOS, por exemplo: `mycompany`

     Use letras minúsculas. Se você criar várias conexões para o Servidor de Administração ou um ponto de distribuição, especifique nomes diferentes para cada conexão.

     > Para executar ações de resposta, o nome de domínio do Active Directory especificado neste campo deve corresponder ao nome de domínio do Active Directory especificado no alerta.

   - **Login**

     Login da conta do Active Directory com direitos de administrador sob os quais as ações de resposta devem ser executadas.

   - **Senha**

     Senha da conta do Active Directory com direitos de administrador sob a qual as ações de resposta devem ser executadas.

6. Se quiser verificar o status da conexão, clique no botão **Verificar conexão**.

   Se a conexão for estabelecida com êxito, o status **Conectado** é exibido. Caso contrário, o status será **Falhou** e uma mensagem de erro será exibida com os controladores de domínio aos quais você não conseguiu se conectar.

Você deve considerar como a conexão com o Active Directory é feita: **de um dispositivo Linux ou de um dispositivo Windows**.

Conectando via dispositivo Linux

Por padrão, ao conectar e autenticar em um controlador de domínio via um dispositivo Linux, a lógica é a seguinte:

1. O Servidor de Administração ou um ponto de distribuição tenta se conectar ao controlador de domínio através do LDAPS.

   A verificação rigorosa do certificado do servidor LDAP é executada.

2. Você deve colocar a parte pública do certificado do controlador de domínio no repositório de certificados do sistema para validar o certificado válido.

   O caminho dependente do SO para a autorização de certificação (CA) do sistema é usado para acessar a cadeia de certificados.

   Por exemplo:

   - /etc/ssl/certs/ca-certificates.crt — Caminho para sistemas operacionais baseados em Debian (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem — Caminho para CentOS ou Red Hat.

3. Se a conexão LDAPS falhar, ocorrerá um erro e nenhum outro protocolo de conexão será usado.

   Em caso de problemas com o LDAP, você pode entrar em contato com o Suporte Técnico da Kaspersky.

Se não quiser instalar o certificado no repositório de certificados do sistema, poderá usar o sinalizador KLNAG_LDAP_SSL_CACERT para definir o caminho para o certificado do controlador de domínio. Para isso, execute o comando:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

onde `</path/to/domain-controller/cert>` é o caminho para a parte pública do certificado do controlador de domínio.

Por exemplo, se o caminho for `"/var/opt/kaspersky/ldap_cert.crt"`, o comando será `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Conectando via dispositivo Windows

Ao conectar e autenticar em um controlador de domínio via um dispositivo Windows, as configurações de conexão são definidas pelo domínio.

Você deve garantir que:

- O LDAP está ativado e a porta 636 está disponível no dispositivo.
- Você permite conexões com o controlador de domínio através de um firewall ou de um servidor proxy.

7. Clique no botão **Salvar**.

A janela é fechada e a conexão é exibida na tabela de conexões.

Na barra de conexões, você pode fazer o seguinte:

- Edite os parâmetros de conexão.

  Para fazer isso, clique no link com o parâmetro **Endereço do controlador de domínio** para a conexão necessária. Na janela exibida, adicione as fontes necessárias e clique no botão **Salvar**.

  Você pode editar somente os parâmetros **Login** e **Senha**.

- Exclua as conexões.

  Para fazer isso, marque a caixa de seleção ao lado da conexão que deseja excluir, clique no botão **Remover** na barra de ferramentas e confirme a exclusão da conexão.

Configurando a integração com a Kaspersky Automated Security Awareness Platform

Integração com a Kaspersky Automated Security Awareness Platform (aqui também referida como KASAP) permite atribuir cursos de aprendizagem KASAP para usuários associados a alertas.

As configurações de integração não são herdadas e são aplicadas somente ao Servidor de Administração (servidor físico ou virtual) no qual você define essas configurações.

Antes de configurar uma integração no Kaspersky Security Center Web Console, você deve criar um token de autorização e obter um URL para solicitações de API no KASAP.

Para configurar a integração com a Kaspersky Automated Security Awareness Platform:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Selecione a seção **KASAP**.

3. No painel direito, ative o seletor de **Integração KASAP**.

4. Especifique as configurações a serem usadas para as Conexões com a KASAP:

   - **Token API** — Token que você criou para acessar a Open API da KASAP.
   - **URL** — URL para solicitações da API que você obteve ao criar o token da API.

- **Usar um servidor proxy** — Defina o alternante para permitir o uso de um servidor proxy ao conectar-se ao KASAP.

  O seletor fica desativado por padrão.

5. Se necessário, verifique as configurações especificadas clicando no botão **Verificar conexão**.

   O status da conexão é exibido.

6. Clique no botão **Salvar**.

A integração com a Kaspersky Automated Security Awareness Platform está configurada.

Depois que as configurações de integração KASAP forem salvas, você poderá visualizar a lista de grupos de aprendizado KASAP clicando no botão **Exibir grupos**.

Se necessário, quando a lista de grupos for exibida, você poderá atualizá-la clicando no botão **Atualizar grupos**.

Você não pode ocultar a lista depois de abri-la. Se você desativar o botão de alternância **Integração KASAP**, a lista de grupos KASAP não será exibida.

Configurando a integração com o Kaspersky Threat Intelligence Portal Sandbox

Integração com o Kaspersky Threat Intelligence Portal (aqui também referido como Kaspersky TIP) permite executar os arquivos movidos para a seção **Quarentena** usando o Kaspersky Sandbox —um ambiente seguro isolado de sua rede corporativa.

As configurações de integração não são herdadas e são aplicadas somente ao Servidor de Administração (servidor físico ou virtual) no qual você define essas configurações.

Antes de configurar a integração, você deve obter um token de autorização para solicitações de API no Kaspersky TIP.

Para configurar a integração com o Kaspersky TIP Sandbox:

1. No menu principal, clique no nome do Servidor de Administração.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Selecione **Kaspersky TIP**.

3. No painel direito, ative o alternante **Integração**.

   As configurações para a conexão com o Kaspersky TIP são exibidas.

   Se, depois de configurar e salvar as configurações de integração, você desativar o botão de alternância **Integração**, as configurações não serão excluídas, mas a resposta não poderá ser executada.

4. Clique no botão **Adicionar token** e, na janela exibida, especifique o token obtido anteriormente no Kaspersky TIP. Em seguida, clique no botão **Adicionar**.

   A janela é fechada e o token da API é adicionado.

5. Se quiser usar um servidor proxy ao se conectar ao Kaspersky TIP, ative o alternante **Usar um servidor proxy**.

   O seletor fica desativado por padrão.

6. Clique no botão **Salvar**.

A integração com o Kaspersky TIP Sandbox está configurada.

Agora, você pode enviar arquivos do **Quarentena** seção para o Kaspersky TIP Sandbox para análise de ameaças. O tamanho máximo de um arquivo é de 100 MB.

Como a licença do Kaspersky Next XDR Optimum suporta multilocação, os arquivos colocados em **Quarentena** são divididos por locações. Essa separação em nível de tenant também se aplica ao enviar arquivos para o Kaspersky TIP Sandbox e exibir os resultados se o administrador usar uma conta TIP dedicada e um token de API relacionado a cada tenant. No entanto, o gerenciamento centralizado da seção **Quarentena** para todos os tenants não é possível, pois a lista de quarentena não exibe objetos de acordo com a hierarquia do servidor.

Agrupando alertas por atributos

A agregação de alertas ajuda a identificar alertas que podem estar relacionados ao mesmo incidente, simplificando o processo de investigação.

Para ativar a funcionalidade de agregação de alertas, você deve fazer o seguinte:

- Ative a subseção **Alertas** no menu principal.
- Ative o Servidor de Administração com uma licença do Kaspersky Next XDR Optimum e, em seguida, implemente a chave de Licenciamento do Kaspersky Next XDR Optimum nos aplicativos gerenciados.

  Ao usar a funcionalidade Kaspersky Next XDR Optimum com uma licença de avaliação no modo de teste, você deve primeiro adicionar um Servidor de Administração físico secundário e, depois, ativar esse servidor com esta licença.

Se estiver usando o licenciamento do Kaspersky Next EDR Optimum, não é necessário ativar os aplicativos instalados nos dispositivos gerenciados sob o licenciamento do Kaspersky Next XDR Optimum. Isso deve ser feito apenas para novos dispositivos, se houver.
Como a licença do Kaspersky Next XDR Optimum permite a multilocação, você pode distribuir centralmente a chave de licença para aplicativos gerenciados. A distribuição automática da licença para Servidores de Administração secundários e virtuais não é compatível.

Você pode agregar alertas por nome de dispositivo, conta ou nome de hash (SHA256).

> Os alertas são agregados por um atributo somente se esse atributo não estiver vazio.

Os alertas são agregados se compartilharem pelo menos um atributo e ocorrerem dentro de 24 horas após qualquer outro alerta no grupo.

Para agregar alertas por atributos:

1. No menu principal, vá para **Monitoramento** → **Alertas**.
2. Execute uma das seguintes ações:

   - Ative o alternante **Agrupamento de alertas** e selecione um ou mais atributos para agregar alertas por:

     - **Nome do dispositivo**
     - **Conta**
     - **Hash de arquivo (SHA256)**

     Os atributos **Nome do dispositivo** e **Conta** são selecionados por padrão.

   - Clique no ícone de configurações (⚙). No painel aberto **Configurações da tabela**, vá para a guia **Agrupamento**. Selecione o **ID do grupo de agregação** e clique em **Aplicar**.

   Quando a agregação estiver ativada, os alertas são classificados por **Hora do evento** do mais novo ao mais antigo. As opções de classificação adicionais não são compatíveis. Selecione um grupo de opções diferente desativará a agregação.

A tabela exibe alertas agregados por atributos. Os alertas não agregados são exibidos na parte inferior da tabela.

Cada alerta é atribuído a apenas um grupo após a agregação.

Integração entre o Kaspersky Security Center Web Console e outras soluções

Esta seção descreve como configurar o acesso a partir do Kaspersky Security Center Web Console a outro aplicativo Kaspersky, como o Kaspersky Managed Detection and Response. Esta seção também descreve como configurar a exportação para sistemas SIEM.

Estabelecendo uma conexão em segundo plano

Para configurar a interação entre o Kaspersky Security Center Linux e outro aplicativo ou solução da Kaspersky, por exemplo, o Kaspersky Managed Detection and Response (também conhecido como MDR), é preciso estabelecer uma conexão de segundo plano entre o Kaspersky Security Center Web Console e o Servidor de Administração. Você pode estabelecer essa conexão somente se sua conta tiver o direito de Modificar ACLs de objetos da área funcional **Recursos gerais: Permissões do usuário**.

É possível configurar a interação apenas entre o Kaspersky Managed Detection and Response e a versão baseada no Windows do Kaspersky Security Center.

Para estabelecer uma conexão em segundo plano:

1. No menu principal, vá para **Configurações** → **Integração**.
2. Selecione a guia **Configurações do servidor proxy do Web Console**.
3. Na seção **Integração**, defina a chave da conexão em segundo plano como **Conexão em segundo plano para integração Ativado**.
4. Na seção aberta **Ativar uma conexão em segundo plano**, clique no botão **OK**.

A conexão de segundo plano entre o Kaspersky Security Center Web Console e o Servidor de Administração é estabelecida. O Servidor de Administração cria uma conta para a conexão em segundo plano e essa conta é usada como uma conta de serviço para manter a interação entre o Kaspersky Security Center Linux e outro aplicativo ou solução da Kaspersky. O nome desta conta de serviço contém o prefixo NWCSvcUser. Por motivos de segurança, o Servidor de Administração muda automaticamente a senha da conta de serviço a cada 30 dias. Você não pode excluir a conta de serviço manualmente. O Servidor de Administração exclui esta conta automaticamente se você desativar uma conexão entre serviços. O Servidor de Administração cria uma única conta de serviço para cada Kaspersky Security Center Web Console e Console de Administração e atribui todas as contas de serviço ao grupo de segurança com o nome ServiceNwcGroup. O Servidor de Administração cria este grupo de segurança automaticamente durante o processo de instalação do Kaspersky Security Center Linux. Você não pode excluir este grupo de segurança manualmente.

Configuração da conexão do servidor proxy

Para configurar uma conexão do servidor proxy para o Kaspersky Security Center Web Console e plug-ins da web:

1. No menu principal, vá para **Configurações** → **Integração**.
2. Selecione a aba **Configurações do servidor proxy do Web Console**.
3. Ative a opção **Usar servidor proxy**.
4. Especifique as configurações de conexão do servidor proxy:
   - **Endereço do servidor proxy**
   - **Número da porta**
   - **Autenticação do servidor proxy**
   - **Nome de usuário** (obrigatório se a opção **Autenticação no servidor proxy** estiver ativada)
   - **Senha** (obrigatória se a opção **Autenticação no servidor proxy** estiver ativada)
5. Clicar em **Salvar** para salvar as configurações de conexão do servidor proxy

Se houver uma hierarquia de Servidores de Administração, as configurações de proxy não são propagadas para os Web Consoles dos Servidores de Administração secundários. Você deve configurar a conexão do servidor proxy separadamente para cada Kaspersky Security Center Web Console.

Diagnóstico remoto de dispositivos cliente

É possível usar o diagnóstico remoto para execução remota das seguintes operações nos dispositivos clientes baseados em Windows e Linux:

- Ativar e desativar o rastreamento, alterar o nível de rastreamento e baixar o arquivo de rastreamento
- Download de informações do sistema e de configurações do aplicativo
- Download de registros de eventos
- Gerar um arquivo de dump para um aplicativo
- Início do diagnóstico e download de seus relatórios
- Início, interrupção e reinício de aplicativos

Você pode usar registros de eventos e relatórios de diagnóstico baixados de um dispositivo cliente para resolver problemas. Além disso, ao entrar em contato com o Suporte Técnico da Kaspersky, um especialista de Suporte Técnico pode pedir que você faça download de arquivos de rastreamento, arquivos de despejo, logs de eventos e relatórios de diagnóstico de um dispositivo cliente para análise adicional na Kaspersky.

Abertura da janela de diagnóstico remoto

Para executar diagnóstico remoto em dispositivos clientes baseados em Windows e Linux, é necessário abrir a janela de diagnóstico remoto.

Para abrir a janela de diagnóstico remoto:

1. Para selecionar o dispositivo para o qual você deseja abrir a janela de diagnóstico remoto, execute um dos seguintes procedimentos:
   - Caso o dispositivo pertença a um grupo de administração, no menu principal, acesse **Gerenciamento de ativos → Dispositivos gerenciados**.
   - Caso o dispositivo pertença ao grupo de Dispositivos não atribuídos, no menu principal, vá para **Gerenciamento de ativos → Dispositivos não atribuídos**.
2. Clique no nome do dispositivo necessário.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Avançado**.
4. Na guia **Avançado**, clique em **Diagnóstico remoto**.

   Isso abre a janela de **Diagnóstico remoto** do dispositivo cliente. Caso a conexão entre o Servidor de Administração e o dispositivo cliente não seja estabelecida, a mensagem de erro será exibida.

Como alternativa, caso precise obter todas as informações de diagnóstico sobre um dispositivo cliente baseado em Linux de uma só vez, é possível executar o script collect.sh nesse dispositivo.

Ativação e desativação do rastreamento para aplicativos

É possível ativar e desativar o rastreamento para aplicativos, incluindo o rastreamento do Xperf.

Ativação e desativação do rastreamento

Para ativar ou desativar o rastreamento em um dispositivo remoto:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos da Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione o aplicativo para o qual deseja ativar ou desativar o rastreamento.

   A lista de opções de diagnóstico remoto é aberta.
4. Se desejar ativar o rastreamento:

   a. Na seção **Rastreamento**, clique em **Ativar rastreamento**.

   b. Na janela **Modificar nível de rastreamento** que se abre, recomendamos que você mantenha os valores padrões das configurações. Quando necessário, um especialista de Suporte Técnico orientará você através do processo de configuração. As seguintes opções estão disponíveis:

   - **Nível de rastreamento**

     O nível de rastreamento define o volume de detalhes que o arquivo de rastreamento contém.

   - **Rastreamento baseado em rotação**

     O aplicativo sobrescreve as informações de rastreamento para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o número máximo de arquivos a serem usados para armazenar as informações de rastreamento e o tamanho máximo de cada arquivo. Se o número máximo de arquivos de rastreamento com o tamanho máximo estiver gravado, o arquivo de rastreamento mais antigo será excluído para que um novo arquivo possa ser gravado.

     Essa configuração está disponível apenas para o Kaspersky Endpoint Security.

   c. Clique no botão **Salvar**.

O rastreamento está ativado para o aplicativo selecionado. Em alguns casos, um aplicativo de segurança e sua tarefa devem ser reiniciados para que seja possível ativar o rastreamento.

Em dispositivos clientes baseados em Linux, o rastreamento do componente Atualizador do Agente de Rede é regulado pelas configurações do Agente de Rede. Portanto, as opções **Ativar rastreamento** e **Modificar nível de rastreamento** estão desativadas para este componente em dispositivos clientes que executam o Linux.

5. Caso deseje desativar o rastreamento para o aplicativo selecionado, clique no botão **Desabilitar rastreamento**.

   O rastreamento está desativado para o aplicativo selecionado.

Ativação do rastreamento do Xperf

Para o Kaspersky Endpoint Security, um especialista de Suporte Técnico pode solicitar que você ative o rastreamento do Xperf para obter informações sobre o desempenho do sistema.

Para ativar e configurar o rastreamento do Xperf ou desativá-lo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos da Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione Kaspersky Endpoint Security for Windows.

   A lista de opções de diagnóstico remoto do Kaspersky Endpoint Security for Windows é exibida.
4. Na seção **Rastreamento do Xpref** da lista, clique em **Ativar rastreamento Xperf**.

   Se o rastreamento do Xperf já estiver ativado, o botão **Desativar rastreamento Xperf** é exibido. Clique neste botão caso queira desativar o rastreamento do Xperf para o Kaspersky Endpoint Security for Windows.
5. Na janela **Alterar nível de rastreamento Xperf** que se abre, dependendo da solicitação do especialista de Suporte Técnico, faça o seguinte:

   a. Selecione um dos seguintes níveis de rastreamento:

   - **Nível leve**

     Um arquivo de rastreamento deste tipo contém a quantidade mínima de informações sobre o sistema.

     Por padrão, esta opção está selecionada.

   - **Nível profundo**

     Um arquivo de rastreamento deste tipo contém informações mais detalhadas do que as dos arquivos de rastreamento do tipo *Superficial*, podendo ser solicitados pelos especialistas do Suporte Técnico quando um arquivo de rastreamento do tipo *Superficial* não for suficiente para a avaliação de desempenho. Um arquivo de rastreamento *Profundo* contém informações técnicas sobre o sistema, como as informações sobre hardware, sistema operacional, lista de processos e aplicativos iniciados e concluídos, eventos usados para avaliação de desempenho e eventos da Ferramenta de Avaliação de Sistema do Windows.

   b. Selecione um dos seguintes tipos de rastreamento do Xperf:

   - **Tipo básico**

     As informações de rastreamento são recebidas durante a operação do aplicativo Kaspersky Endpoint Security.

     Por padrão, esta opção está selecionada.

- **Tipo Ao reiniciar**

  As informações de rastreamento são recebidas quando o sistema operacional é iniciado no dispositivo gerenciado. Esse tipo de rastreamento é eficaz quando o problema que afeta o desempenho do sistema ocorre depois que o dispositivo é ligado e antes da inicialização do Kaspersky Endpoint Security.

Você também poderá ser solicitado a ativar a opção **Tamanho do arquivo de rotação, em MB** para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o tamanho máximo do arquivo de rastreamento. Quando o arquivo atingir o tamanho máximo, as informações de rastreamento mais antigas serão substituídas por novas informações.

c. Defina o tamanho do arquivo de rotação.

d. Clique no botão **Salvar**.

O rastreamento do Xperf está ativado e configurado.

6. Caso queira desativar o rastreamento do Xperf para o Kaspersky Endpoint Security for Windows, clique em **Desativar rastreamento Xperf** na seção **Rastreamento do Xpref**.

   O rastreamento do Xperf está desativado.

Download de arquivos de rastreamento de um aplicativo

Para fazer download do arquivo de rastreamento de um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos da Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione o aplicativo para o qual deseja baixar o arquivo de rastreamento.
4. Na seção **Rastreamento**, clique no botão **Arquivos de rastreamento**.

   Assim, a janela **Registros de rastreamento do dispositivo** é aberta, onde uma lista de arquivos de rastreamento é exibida.
5. Na lista de arquivos de rastreamento, selecione o arquivo que deseja baixar.
6. Execute uma das seguintes ações:

   - Faça o download do arquivo selecionado clicando em **Baixar**. É possível selecionar um ou vários arquivos para baixar.
   - Baixe uma parte do arquivo selecionado:

     a. Clique em **Baixar uma parte**.

     Não é possível baixar partes de vários arquivos ao mesmo tempo. Caso selecione mais de um arquivo de rastreamento, o botão **Baixar uma parte** será desativado.

b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada, de acordo com suas necessidades.

Para dispositivos baseados em Linux, a edição do nome da parte do arquivo não está disponível.

c. Clique em **Baixar**.

O arquivo selecionado, ou sua parte, é baixado no local especificado.

Exclusão de arquivos de rastreamento

É possível excluir arquivos de rastreamento que não sejam mais necessários.

Para excluir um arquivo de rastreamento:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto que é aberta, selecione a guia **Logs de eventos**.
3. Na seção **Arquivos de rastreamento**, clique em **Logs do Windows Update** ou **Logs de instalação remota**, dependendo de quais arquivos de rastreamento deseja excluir.

   O link **Logs do Windows Update** está disponível apenas para os dispositivos cliente baseados em Windows.

   Assim, a janela **Registros de rastreamento do dispositivo** é aberta, onde uma lista de arquivos de rastreamento é exibida.
4. Na lista de arquivos de rastreamento, selecione um ou vários arquivos que deseja excluir.
5. Clique no botão **Remover**.

Os arquivos de rastreamento selecionados são excluídos.

Download das configurações do aplicativo

Para baixar as configurações do aplicativo a partir de um dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos da Kaspersky**.
3. Na seção **Configurações do aplicativo**, clique no botão **Baixar** para baixar as informações sobre as configurações dos aplicativos instalados no dispositivo cliente.

O arquivo ZIP com as informações é baixado no local especificado.

Baixar as informações do sistema a partir de um dispositivo cliente

Para baixar as informações do sistema a partir de um dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Informações do sistema**.
3. Clique no botão **Baixar** para baixar as informações do sistema sobre o dispositivo cliente.

   Caso obtenha as informações do sistema sobre um dispositivo baseado em Linux, um arquivo de despejo para aplicativos finalizados por emergência será adicionado ao arquivo resultante.

   O arquivo pode conter dados confidenciais (por exemplo, chaves e senhas) em texto simples. Recomendamos revisar os arquivos no arquivo compactado e remover esses dados antes de enviá-los ao Suporte Técnico da Kaspersky.

O arquivo com as informações é baixado para o local especificado.

Download de registros de eventos

Para baixar um log de eventos a partir de um dispositivo remoto:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, na guia **Logs de eventos**, clique em **Todos os logs do dispositivo**.
3. Na janela **Todos os logs do dispositivo**, selecione os logs relevantes.
4. Execute uma das seguintes ações:

   - Baixe o log selecionado clicando em **Baixar todo o arquivo**.
   - Baixe uma parte do log selecionado:

     a. Clique em **Baixar uma parte**.

     Não é possível baixar partes de vários logs ao mesmo tempo. Caso mais de uma política seja selecionada, o botão **Baixar uma parte** será desabilitado.

     b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada de acordo com suas necessidades.

     Para dispositivos baseados em Linux, a edição do nome da parte do log não está disponível.

     c. Clique em **Baixar**.

O log de eventos selecionado, ou uma parte dele, é baixado no local especificado.

Início, interrupção e reinício do aplicativo

É possível iniciar, parar e reiniciar aplicativos em um dispositivo cliente.

Para iniciar, interromper ou reiniciar um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos da Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione o aplicativo que deseja iniciar, parar ou reiniciar.
4. Selecione uma ação clicando em um dos seguintes botões:

   - **Parar aplicativo**

     Esse botão está disponível apenas se o aplicativo estiver em execução no momento.
   - **Reiniciar aplicativo**

     Esse botão está disponível apenas se o aplicativo estiver em execução no momento.
   - **Iniciar aplicativo**

     Esse botão está disponível apenas se o aplicativo não estiver em execução no momento.

   Dependendo da ação selecionada, o aplicativo necessário é iniciado, parado ou reiniciado no dispositivo cliente.

Se o Agente de Rede for reiniciado, será exibida uma mensagem informando que a conexão atual do dispositivo com o Servidor de Administração será perdida.

Execução do diagnóstico remoto do Agente de Rede do Kaspersky Security Center Linux e download dos resultados

Para iniciar o diagnóstico do Agente de Rede do Kaspersky Security Center Linux em um dispositivo remoto e baixar os resultados:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, selecione a guia **Aplicativos da Kaspersky**.

   Na seção **Gerenciamento de aplicativos**, a lista de aplicativos da Kaspersky instalados no dispositivo é exibida.
3. Na lista de aplicativos, selecione **Agente de Rede do Kaspersky Security Center Linux**.

   A lista de opções de diagnóstico remoto é aberta.

4. Na seção **Relatório de diagnóstico**, clique no botão **Executar diagnósticos**.

   Isso inicia o processo de diagnóstico remoto e gera um relatório de diagnóstico. Quando o processo de diagnóstico estiver concluído, o botão **Baixar o relatório de diagnóstico** ficará disponível.

5. Clique no botão **Baixar o relatório de diagnóstico** para baixar o relatório.

O relatório é baixado no local especificado.

Execução de um aplicativo em um dispositivo cliente

Você pode ter que executar um aplicativo no dispositivo cliente se um especialista de suporte da Kaspersky solicitar. Não será necessário instalar o aplicativo no dispositivo.

Se você quiser executar um script personalizado no dispositivo cliente, será possível usar a variável de ambiente `KLACDT_SAVE_SETTING` para determinar o caminho onde os resultados da execução serão salvos. Por exemplo:

- Para um dispositivo baseado em Windows:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Para um dispositivo baseado em Linux:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

Para executar um aplicativo no dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto, selecione a guia **Executando um aplicativo remoto**.

3. No campo **Tipo de objeto**, selecione o tipo de objeto que deseja carregar:

   - Selecione **Arquivo** para carregar o arquivo executável.

   - Selecione **Pasta** para carregar a pasta que contém o aplicativo que deseja executar no dispositivo cliente.

     Caso selecione esse tipo de objeto, o campo **Nome do arquivo a ser executado** será exibido. Neste campo, especifique o nome do arquivo executável na pasta. Também é possível especificar o caminho relativo para o arquivo.

   - Selecione **Arquivo** para carregar o arquivo ZIP contendo o aplicativo que deseja executar no dispositivo cliente.

     Caso selecione esse tipo de objeto, o campo **Nome do arquivo a ser executado** será exibido. Neste campo, especifique o nome do arquivo executável na pasta. Também é possível especificar o caminho relativo para o arquivo.

     > O arquivo comprimido deve incluir a pasta do utilitário. Essa pasta contém o arquivo executável a ser executado em um dispositivo remoto.

4. Carregue o objeto ao selecioná-lo na janela do sistema ou arraste para o campo de upload.

5. Caso necessário, no campo **Argumentos da linha de comando**, especifique os argumentos a fornecidos à linha de comando ao executar o arquivo executável.

6. Clique no botão **Carregar e executar** para executar o aplicativo selecionado em um dispositivo cliente.

7. Após a execução do aplicativo ser concluída com sucesso, baixe os resultados da execução ao clicar no botão **Baixar resultados de execução do aplicativo**.

   Os resultados da execução do aplicativo são armazenados até que um novo diagnóstico seja executado ou a janela seja fechada.

O diagnóstico remoto do dispositivo cliente com o uso do aplicativo é concluído.

Execução do diagnóstico remoto em um dispositivo cliente baseado em Linux

O Kaspersky Security Center Linux permite baixar as informações básicas de diagnóstico de um dispositivo cliente. Como alternativa, é possível obter as informações de diagnóstico sobre um dispositivo baseado em Linux com o uso do script collect.sh da Kaspersky. Esse script deve ser executado no dispositivo cliente baseado em Linux que precisa ser diagnosticado. Em seguida, é criado um arquivo com informações de diagnóstico, informações do sistema do dispositivo, arquivos de rastreamento do aplicativo, logs de eventos do dispositivo e um arquivo de dump para falhas e processos encerrados.

Recomendamos usar o script collect.sh para obter todas as informações de diagnóstico sobre o dispositivo cliente baseado em Linux de uma só vez. Caso as informações de diagnóstico sejam baixadas remotamente pelo Kaspersky Security Center Linux, será necessário passar por todas as seções da interface de diagnóstico remoto. Além disso, as informações de diagnóstico para um dispositivo baseado em Linux provavelmente não serão obtidas completamente.

Se você precisar enviar o arquivo gerado com as informações de diagnóstico ao Suporte técnico da Kaspersky, exclua todas as informações confidenciais antes de enviar o arquivo.

Para baixar as informações de diagnóstico de um dispositivo cliente baseado em Linux usando o script collect.sh:

1. Baixe o script collect.sh compactado no arquivo collect.tar.gz.

2. Copie o arquivo baixado para o dispositivo cliente baseado em Linux que precisa ser diagnosticado.

3. Execute o seguinte comando para descompactar o arquivo collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Execute o seguinte o comando para especificar os direitos de execução do script:

   ```
   # chmod +x collect.sh
   ```

5. Execute o script collect.sh usando uma conta com direitos de administrador:

   ```
   # ./collect.sh
   ```

Um arquivo com as informações de diagnóstico é gerado e salvo na pasta /tmp/$HOST_NAME-collect.tar.gz.

Gerenciar aplicativos e arquivos executáveis de terceiros em dispositivos clientes

Esta seção descreve os recursos do Kaspersky Security Center Linux relacionados ao gerenciamento de aplicativos e arquivos executáveis de terceiros nos dispositivos clientes.

Usar o Controle de Aplicativos para gerenciar arquivos executáveis

Você pode usar o componente Controle de Aplicativos para permitir ou bloquear a inicialização de arquivos executáveis nos dispositivos de usuário. O componente Controle de Aplicativos é compatível com sistemas operacionais baseados em Windows e Linux.

Para sistemas operacionais baseados em Linux, o componente Controle de Aplicativos está disponível a partir do Kaspersky Endpoint Security 11.2 for Linux.

Pré-requisitos

- O Kaspersky Security Center Linux está implementado em sua organização.
- A política do Kaspersky Endpoint Security for Linux ou do Kaspersky Endpoint Security for Windows está criada e ativa. O componente Controle de Aplicativos está ativado na política.

Fases

O cenário de uso do Controle de Aplicativos prossegue em fases:

1. **Formar e visualizar a lista de arquivos executáveis em dispositivos clientes**

   Esta etapa ajuda a descobrir quais arquivos executáveis são encontrados nos dispositivos gerenciados. Exiba a lista de arquivos executáveis e compare-a com a lista de arquivos executáveis permitidos e proibidos. As restrições sobre a utilização de arquivos executáveis podem estar relacionadas às políticas de segurança da informação em sua organização.

   Instruções de como proceder: Obter e visualizar uma lista de arquivos executáveis armazenados em dispositivos clientes

2. **Criar categorias para arquivos executáveis usados em sua organização**

   Analise a lista de arquivos executáveis armazenados nos dispositivos gerenciados. Com base na análise, crie categorias para arquivos executáveis. É recomendável criar uma categoria "Aplicativos de trabalho" que cubra o conjunto padrão de arquivos executáveis usados na sua organização. Se diferentes grupos de segurança usarem seus próprios conjuntos de arquivos executáveis em seu trabalho, uma categoria poderá ser criada para cada grupo de segurança.

A inicialização de arquivos executáveis cujas configurações não correspondem a nenhuma das regras do Controle de Aplicativos é regulada pelo modo de operação selecionado do componente:

- *Lista de bloqueio*. O modo é usado se você deseja permitir a inicialização de todos os arquivos executáveis, exceto aqueles especificados nas regras de bloqueio. Este modo é selecionado por padrão.
- *Lista de permissão*. O modo é usado se você deseja bloquear a inicialização de todos os arquivos executáveis, exceto aqueles especificados nas regras de permissão.

As regras de Controle de Aplicativos são implementadas por meio de categorias para arquivos executáveis. No Kaspersky Security Center Linux, existem três tipos de categorias de arquivos executáveis:

- Categoria com conteúdo adicionado manualmente. O usuário define as condições, por exemplo, metadados, código de hash, certificado e caminho do arquivo para incluir os arquivos executáveis na categoria.
- Categoria que inclui os arquivos executáveis dos dispositivos selecionados. Você especifica um dispositivo cujos arquivos executáveis são incluídos automaticamente na categoria.
- Categoria que inclui os arquivos executáveis da pasta selecionada. Você especifica uma pasta da qual os arquivos executáveis são incluídos automaticamente na categoria.

3. **Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security**

   Configure o componente Controle de Aplicativos na política do Kaspersky Endpoint Security for Linux usando as categorias criadas na fase anterior.

   Instruções: Configurar o Controle de Aplicativos na política do Kaspersky Endpoint Security for Windows

4. **Ativar o componente Controle de Aplicativos no modo de teste**

   Para garantir que as regras do Controle de Aplicativos não bloqueiem os arquivos executáveis necessários para o trabalho do usuário, é recomendável ativar o teste das regras do Controle de Aplicativos e analisar a sua operação após a criação de novas regras. Quando o teste está ativado, o Kaspersky Endpoint Security for Windows não bloqueia os arquivos executáveis cuja inicialização é proibida pelas regras do Controle de Aplicativos, mas envia notificações sobre a inicialização ao Servidor de Administração.

   Ao testar as regras do Controle de Aplicativos, é recomendável realizar as seguintes ações:

   - Determine o período de teste. O período de teste pode variar de vários dias a dois meses.
   - Examine os eventos resultantes do teste da operação do Controle de Aplicativos.

   Instruções para o Kaspersky Security Center Web Console: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e ative a opção **Modo de teste** no processo de configuração.

5. **Alterar as configurações do componente Controle de Aplicativos**

   Se necessário, faça alterações nas configurações do Controle de Aplicativos. Com base nos resultados do teste, você pode adicionar arquivos executáveis relativos a eventos do componente Controle de Aplicativos a uma categoria com conteúdo adicionado manualmente.

   Instruções: Kaspersky Security Center Web Console: Adicionar arquivos executáveis relacionados com eventos na categoria de aplicativo

6. **Aplicar as regras do Controle de Aplicativos no modo de operação**

   Após as regras de Controle de Aplicativos terem sido testadas e a configuração das categorias estar concluída, você pode aplicar as regras do Controle de Aplicativos no modo de operação.

   Instruções para o Kaspersky Security Center Web Console: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e desative a opção **Modo de teste** no processo de configuração.

7. **Verificar a configuração do Controle de Aplicativos**

   Certifique-se de ter feito o seguinte:

   - Categorias criadas para arquivos executáveis.
   - Configurado o Controle de Aplicativos usando as categorias.
   - Aplicado as regras do Controle de Aplicativos no modo de operação.

Resultados

Quando o cenário estiver concluído, a inicialização dos arquivos executáveis nos dispositivos gerenciados será controlada. Os usuários podem executar apenas aqueles arquivos executáveis permitidos na sua organização e não podem executar arquivos executáveis proibidos na sua organização.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte a Ajuda do Kaspersky Endpoint Security for Linux e a Ajuda do Kaspersky Endpoint Security for Windows.

Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos clientes

É possível obter a lista de arquivos executáveis armazenados em dispositivos clientes de uma das seguintes maneiras:

- Habilitar notificações sobre inicialização de aplicativos na política do Kaspersky Endpoint Security.
- Criar uma tarefa de inventário.

Ativar notificações sobre inicialização de aplicativos na política do Kaspersky Endpoint Security

Para habilitar notificações sobre a inicialização de aplicativos:

1. Abra as configurações da política do Kaspersky Endpoint Security e vá para **Configurações gerais** → **Relatórios e armazenamento**.
2. No grupo de configurações **Transferência de dados para o Servidor de Administração**, marque a caixa de seleção **Sobre aplicativos iniciados** e salve as alterações.

Quando um usuário tenta iniciar arquivos executáveis, informações sobre esses arquivos são adicionadas à lista de arquivos executáveis em um dispositivo cliente. O Kaspersky Endpoint Security envia essas informações ao Agente de Rede e, em seguida, o Agente de Rede as envia ao Servidor de Administração.

Criar uma tarefa de inventário

Para o Kaspersky Endpoint Security for Linux, o recurso de inventário de arquivos executáveis está disponível a partir da versão 11.2.

É possível reduzir a carga no banco de dados enquanto as informações sobre os aplicativos instalados são obtidas. Para economizar espaço em um banco de dados, execute uma tarefa de inventário em dispositivos de referência nos quais um conjunto padrão de software está instalado. O número desejável de dispositivos é entre 1 e 3.

Para criar uma tarefa de inventário para arquivos executáveis em dispositivos clientes:

1. No menu principal, vá para **Tarefas**.

   A lista de tarefas é exibida.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Na página **Novas configurações de tarefa**, na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Linux ou Kaspersky Endpoint Security for Windows, dependendo do sistema operacional dos dispositivos clientes.
4. Na lista suspensa **Tipo de tarefa**, selecione **Inventário**.
5. Na página **Concluir a criação da tarefa**, clique no botão **Concluir**.

Após a conclusão do Assistente para novas tarefas, a tarefa **Inventário** será criada e configurada. Se desejar, você pode alterar as configurações da tarefa criada. A tarefa recém-criada é exibida na lista de tarefas.

Para obter uma descrição detalhada da tarefa de inventário, consulte a Ajuda do Kaspersky Endpoint Security for Linux e a Ajuda do Kaspersky Endpoint Security for Windows.

Após a tarefa **Inventário** ser executada, a lista de arquivos executáveis armazenados nos dispositivos gerenciados é formada e você pode visualizá-la.

Durante o inventário, arquivos executáveis nos seguintes formatos podem ser detectados (dependendo da opção selecionada nas propriedades da tarefa de inventário): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Visualizar a lista de arquivos executáveis armazenados nos dispositivos gerenciados

Para exibir a lista dos arquivos executáveis armazenados nos dispositivos clientes:

No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Arquivos executáveis**.

A página exibe a lista de arquivos executáveis armazenados nos dispositivos clientes.

Se necessário, é possível enviar o arquivo executável do dispositivo gerenciado para o dispositivo em que o Kaspersky Security Center Web Console está aberto.

Para enviar um arquivo executável:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Arquivos executáveis**.
2. Clique no link do arquivo executável que deseja enviar.
3. Na janela que é aberta, vá para a seção **Dispositivos** e marque a caixa de seleção do dispositivo gerenciado do qual você deseja enviar o arquivo executável.

   Antes de enviar o arquivo executável, certifique-se de que o dispositivo gerenciado tenha uma conexão direta com o Servidor de Administração marcando a caixa de seleção **Não desconectar do Servidor de Administração**.

4. Clique no botão **Enviar**.

   O arquivo executável selecionado é baixado para envio posterior ao dispositivo onde o Kaspersky Security Center Web Console está aberto.

Criar uma categoria de aplicativos com conteúdo adicionado manualmente

Você pode especificar um conjunto de critérios como um modelo de arquivos executáveis cuja inicialização deseja permitir ou bloquear na sua organização. Com base nos arquivos executáveis correspondentes aos critérios, você poderá criar uma categoria de aplicativos e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria de aplicativos com conteúdo adicionado manualmente:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Categorias de aplicativos**.

   A página com uma lista de categorias de aplicativos é exibida.

2. Clique em **Adicionar**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na etapa **Selecionar método de criação de categoria**, especifique o nome da categoria de aplicativo e selecione a opção **Categoria com conteúdo adicionado manualmente. Os dados dos arquivos executáveis são adicionados manualmente à categoria**.

4. Na etapa **Condições**, clique no botão **Adicionar** para adicionar um critério de condição para incluir arquivos na criação da categoria.

5. Na etapa **Critérios da condição**, faça o seguinte:

   a. Selecione um tipo de regra para a criação da categoria:

   - **Da categoria KL**

     Se esta opção estiver selecionada, você poderá especificar uma categoria de aplicativos da Kaspersky como a condição para adicionar aplicativos da categoria do usuário. Os aplicativos da categoria da Kaspersky especificada serão adicionados à categoria de aplicativos do usuário.

   - **Selecionar certificado do repositório**

     Se essa opção for selecionada, será possível especificar certificados a partir do repositório. A condição de categoria só se relaciona com os arquivos executáveis assinados pelo certificado definido.

     Os certificados serão adicionados ao repositório se você tiver criado e iniciado uma tarefa de inventário ou marcado a caixa de seleção **Sobre os aplicativos iniciados** na política do Kaspersky Endpoint Security. É possível executar ambas as ações.

     > As informações sobre certificados podem ser extraídas somente de arquivos executáveis no formato PE (.exe, .dll, .sys).

   - **Especificar caminho para o aplicativo (máscaras aceitas)**

     Se esta opção estiver selecionada, você poderá especificar o caminho para a pasta no dispositivo cliente contendo os arquivos executáveis a serem adicionados à categoria de aplicativos do usuário.

   - **Unidade removível**

     Se esta opção estiver selecionada, você pode especificar o tipo de mídia (qualquer unidade ou unidade removível) no qual o aplicativo será executado. Os aplicativos que foram executados no tipo de unidade selecionado são adicionados à categoria de aplicativo do usuário.

   - **Hash, metadados ou certificado**:

     - **Selecionar na lista de arquivos executáveis**

       Se esta opção estiver selecionada, você poderá utilizar a lista de arquivos executáveis no dispositivo cliente para selecionar e adicionar aplicativos deles à categoria.

- **Selecionar do registro de aplicativos**

  Se esta opção for selecionada, o registro dos aplicativos será exibido. Após selecionar um aplicativo no registro, uma janela se abrirá com os parâmetros já preenchidos com metadados do aplicativo selecionado:

  - Nome do arquivo.
  - Versão do arquivo. Você pode especificar um valor preciso da versão ou descrever uma condição, por exemplo "posterior a 5.0".
  - Nome do aplicativo.
  - Versão do aplicativo. Você pode especificar um valor preciso da versão ou descrever uma condição, por exemplo "posterior a 5.0".
  - Fornecedor.

  Observe que só será bloqueada a inicialização de arquivos executáveis que atendam aos parâmetros especificados, mas não a inicialização de aplicativos que você selecionou. Você poderá prosseguir para a próxima etapa se os metadados do aplicativo selecionado corresponderem ao do arquivo executável que é iniciado quando você inicia o aplicativo. Caso contrário, altere manualmente os valores para que correspondam aos metadados do arquivo executável.

- **Especificar manualmente**

  Se esta opção estiver selecionada, você deve especificar hash do arquivo, metadados ou certificado como a condição para adicionar aplicativos à categoria do usuário.

  Hash de arquivo

  Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é preciso selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center Linux de arquivos nessa categoria. As informações de valores de hash calculados por funções de hash são armazenadas no banco de dados do Servidor de Administração.

  SHA256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security for Linux oferece suporte ao cálculo SHA256.

  Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center Linux de arquivos na categoria:

  - Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem Kaspersky Endpoint Security for Linux, marque a caixa de seleção **SHA256**.
  - Marque a caixa de seleção **Hash MD5** somente se você usar o Kaspersky Endpoint Security for Windows. O Kaspersky Endpoint Security for Linux não oferece suporte a uma função de hash MD5.

  Metadados

  Se esta opção for selecionada, você poderá especificar os metadados do arquivo como nome, versão e fornecedor. A condição de categoria só se relaciona aos arquivos executáveis com os mesmos metadados.

  Certificado

  Se essa opção for selecionada, será possível especificar certificados a partir do repositório. A condição de categoria só se relaciona com os arquivos executáveis assinados pelo certificado definido.

Os certificados serão adicionados ao repositório se você tiver criado e iniciado uma tarefa de inventário ou marcado a caixa de seleção **Sobre os aplicativos iniciados** na política do Kaspersky Endpoint Security. É possível executar ambas as ações.

- **From archived folder**

  Se esta opção estiver selecionada, você pode especificar uma pasta de arquivamento e selecionar a condição desejada para usar para adicionar aplicativos à categoria de usuário. A pasta de arquivamento é desempacotada e as condições selecionadas são aplicadas aos arquivos na pasta. Como condição, você pode selecionar uma das seguintes categorias:

  - **Hash de arquivo**

    Você seleciona qual função hash (MD5 ou SHA256) deseja usar para calcular valores hash. Os aplicativos que têm o mesmo valor de hash que os arquivos na pasta de arquivamento são adicionados à categoria de aplicativos do usuário.

    Selecione a função de hash MD5 somente se você usar o Kaspersky Endpoint Security for Windows. O Kaspersky Endpoint Security for Linux não oferece suporte a uma função de hash MD5.

  - **Metadados**

    Você seleciona que metadados deseja usar como critérios. Os arquivos executáveis que contenham os mesmos metadados serão adicionados à categoria de aplicativos do usuário.

  - **Certificado**

    Você seleciona quais propriedades de certificado (assunto do certificado, impressão digital ou emissor) deseja usar como critérios. Arquivos executáveis que tenham sido assinados com os certificados contendo as mesmas propriedades serão adicionados à categoria de usuário.

  Os critérios **Metadados** e **Certificado** devem ser definidos manualmente após carregar um arquivo ou pasta arquivada, caso queira usá-los.

  Se esta opção estiver selecionada, você pode especificar uma pasta de arquivamento e selecionar a condição desejada para usar para adicionar aplicativos à categoria de usuário. A pasta de arquivamento é desempacotada e as condições selecionadas são aplicadas aos arquivos na pasta. Como condição, você pode selecionar uma das seguintes categorias:

  - **Hash de arquivo**

    Você seleciona qual função hash (MD5 ou SHA256) deseja usar para calcular valores hash. Os aplicativos que têm o mesmo valor de hash que os arquivos na pasta de arquivamento são adicionados à categoria de aplicativos do usuário.

    Selecione a função de hash MD5 somente se você usar o Kaspersky Endpoint Security for Windows. O Kaspersky Endpoint Security for Linux não oferece suporte a uma função de hash MD5.

  - **Metadados**

    Você seleciona que metadados deseja usar como critérios. Os arquivos executáveis que contenham os mesmos metadados serão adicionados à categoria de aplicativos do usuário.

- **Certificado**

  Você seleciona quais propriedades de certificado (assunto do certificado, impressão digital ou emissor) deseja usar como critérios. Arquivos executáveis que tenham sido assinados com os certificados contendo as mesmas propriedades serão adicionados à categoria de usuário.

> Os critérios **Metadados** e **Certificado** devem ser definidos manualmente após carregar um arquivo ou pasta arquivada, caso queira usá-los.

b. Se necessário, adicione um comentário no campo **Descrição**. O número de símbolos não pode exceder 1.000.

Posteriormente, você poderá editar ou excluir o comentário. Para fazer isso, nas propriedades da categoria de aplicativos, abra a guia **Condições** e, na coluna **Critério da condição**, clique no link da condição cujo comentário você deseja editar ou excluir.

> Ao selecionar o tipo de regra **Da categoria KL**, é possível adicionar um comentário para todas as condições a serem criadas com base nesse tipo de regra. É possível editar ou excluir o comentário para cada condição separadamente.

O critério selecionado é adicionado à lista de condições.

Você pode adicionar quantos critérios forem necessários para a categoria de aplicativo que está sendo criada.

6. Na etapa **Exclusões**, clique no botão **Adicionar** para adicionar um critério de condição exclusivo para excluir arquivos da categoria que está sendo criada.

   Se necessário, é possível adicionar um comentário no campo **Descrição**. O número de símbolos não pode exceder 1.000.

   Posteriormente, você poderá editar ou excluir o comentário. Para fazer isso, nas propriedades da categoria de aplicativos, abra a guia **Exclusões** e, na coluna **Critério da condição**, clique no link da condição cujo comentário você deseja editar ou excluir.

7. Na etapa **Critérios da condição**, selecione um tipo de regra na lista tal como você selecionou um tipo de regra para a criação da categoria.

Quando o assistente for concluído, a categoria de aplicativos será criada e exibida na lista de categorias de aplicativos. Você pode usar a categoria de aplicativos criada ao configurar o Controle de Aplicativos.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte a Ajuda do Kaspersky Endpoint Security for Linux e a Ajuda do Kaspersky Endpoint Security for Windows.

Criar uma categoria de aplicativo que inclua arquivos executáveis dos dispositivos selecionados

Você pode usar arquivos executáveis de dispositivos selecionados como um modelo de arquivos executáveis que deseja permitir ou bloquear. Com base nos arquivos executáveis dos dispositivos selecionados, você pode criar uma categoria de aplicativo e usá-la na configuração do componente Controle de Aplicativos.

Verifique se os seguintes pré-requisitos foram atendidos:

- O componente Controle de aplicativos é ativado na política do Kaspersky Endpoint Security.
- Uma lista de arquivos executáveis armazenados em dispositivos gerenciados foi obtida.

Para criar uma categoria de aplicativo que inclui arquivos executáveis de dispositivos selecionados:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Categorias de aplicativos**.

   A página com uma lista de categorias de arquivos executáveis é exibida.

2. Clique em **Adicionar**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na etapa **Selecionar método de criação de categoria**, especifique o nome da categoria e selecione a opção **Categoria que inclui arquivos executáveis dos dispositivos selecionados. Esses arquivos executáveis são processados automaticamente e suas métricas são adicionadas à categoria**.

4. Clique em **Adicionar**.

5. Na janela que se abre, selecione um ou mais dispositivos cujos arquivos executáveis serão usados para criar a categoria de aplicativos.

6. Especificar as seguintes configurações:

   - **Algoritmo de cálculo do valor hash**

     Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é preciso selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center Linux de arquivos nessa categoria. As informações de valores de hash calculados por funções de hash são armazenadas no banco de dados do Servidor de Administração.

     SHA256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security for Linux oferece suporte ao cálculo SHA256.

     Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center Linux de arquivos na categoria:

     - Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem Kaspersky Endpoint Security for Linux, marque a caixa de seleção **SHA256**.

     Marque a caixa de seleção **Hash MD5** somente se você usar o Kaspersky Endpoint Security for Windows. O Kaspersky Endpoint Security for Linux não oferece suporte a uma função de hash MD5.

     A caixa de seleção **Calcular SHA256 para arquivos nesta categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e quaisquer versões posteriores)** está marcada por padrão.

     A caixa de seleção **Calcular o MD5 para os arquivos nesta categoria (suportado pelas versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** é selecionado por padrão.

   - **Sincronizar dados com o repositório do Servidor de Administração**

     Selecione esta opção se você desejar que o Servidor de Administração verifique periodicamente as alterações na pasta (ou pastas) especificada.

     Por padrão, esta opção está desativada.

Se você ativar esta opção, especifique o período (em horas) para verificar as alterações nas pastas especificadas. Por padrão, o intervalo de verificação é de 24 horas.

- **Tipo de arquivo**

  Nesta seção, você pode especificar o tipo de arquivo usado para criar a categoria de aplicativo.

  Todos os arquivos. Todos os arquivos são levados em consideração durante a criação da categoria. Por padrão, esta opção está selecionada.

  Somente arquivos fora das categorias de aplicativos. Somente arquivos fora das categorias de aplicativos são levados em consideração durante a criação da categoria.

- **Pastas**

  Nesta seção, você pode especificar quais pastas dos dispositivos selecionados contendo arquivos usados para criar a categoria de aplicativos.

  Todas as pastas. Todas as pastas são levadas em consideração para a categoria de criação. Por padrão, esta opção está selecionada.

  Pasta especificada. Somente a pasta especificada é levada em consideração para a categoria de criação. Se você selecionar esta opção, deverá especificar o caminho para a pasta.

Quando o assistente for concluído, a categoria de arquivos executáveis será criada. Ela é exibida na lista de categorias. Você pode usar a categoria criada ao configurar o Controle de Aplicativos.

Criar uma categoria de aplicativo que inclua arquivos executáveis da pasta selecionada

Você pode usar arquivos executáveis da pasta selecionada como um padrão de arquivos executáveis que deseja permitir ou bloquear. Com base nos arquivos executáveis da pasta selecionada, você poderá criar uma categoria de aplicativos e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria que inclui arquivos executáveis da pasta selecionada:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Categorias de aplicativos**.

   A página com uma lista de categorias é exibida.

2. Clique em **Adicionar**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na etapa **Selecionar método de criação de categoria**, especifique o nome da categoria e selecione a opção **Categoria que inclui arquivos executáveis de uma pasta específica. Os arquivos executáveis de aplicativos copiados para a pasta especificada são processados automaticamente e suas métricas são adicionadas à categoria**.

4. Especifique a pasta cujos arquivos executáveis serão usados para criar a categoria.

5. Defina as seguintes configurações:

- **Incluir bibliotecas de link dinâmico (DLL) nessa categoria**

  A categoria de aplicativo inclui bibliotecas de link dinâmico (arquivos no formato de DLL), e o componente Controle de Aplicativos registra as ações de tais bibliotecas que ocorrem no sistema. A inclusão de arquivos DLL na categoria pode diminuir o desempenho do Kaspersky Security Center Linux.

  Por padrão, esta caixa de seleção está desmarcada.

- **Incluir dados de script nesta categoria**

  A categoria do aplicativo inclui dados sobre scripts, e os scripts não são bloqueados pelo Proteção Contra Ameaças da Web. Incluir os dados de script na categoria pode diminuir o desempenho do Kaspersky Security Center Linux.

  Por padrão, esta caixa de seleção está desmarcada.

- **Algoritmo de cálculo de valor hash**: **Calcular SHA256 para arquivos nesta categoria/Calcular hashes MD5 para arquivos nesta categoria**

  Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é preciso selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center Linux de arquivos nessa categoria. As informações de valores de hash calculados por funções de hash são armazenadas no banco de dados do Servidor de Administração.

  SHA256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security for Linux oferece suporte ao cálculo SHA256.

  Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center Linux de arquivos na categoria:

  - Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem Kaspersky Endpoint Security for Linux, marque a caixa de seleção **SHA256**.

  Marque a caixa de seleção **Hash MD5** somente se você usar o Kaspersky Endpoint Security for Windows. O Kaspersky Endpoint Security for Linux não oferece suporte a uma função de hash MD5.

  A caixa de seleção **Calcular SHA256 para arquivos nesta categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e quaisquer versões posteriores)** está marcada por padrão.

  A caixa de seleção **Calcular o MD5 para os arquivos nesta categoria (suportado pelas versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** é selecionado por padrão.

- **Forçar verificação da pasta para procurar alterações**

  Se esta opção estiver ativada, o aplicativo verifica regularmente a pasta de inclusão de conteúdo à categoria, buscando por alterações. Você pode especificar a frequência de verificações (em horas) no campo de entrada próximo da caixa de seleção. Por padrão, o tempo de intervalo entre verificações forçadas é de 24 horas.

  Se esta opção estiver ativada, o aplicativo não força nenhuma verificação da pasta. O Servidor tenta acessar arquivos se eles tiverem sido modificados, adicionados ou excluídos.

  Por padrão, esta opção está desativada.

Quando o assistente for concluído, a categoria de arquivos executáveis será criada. Ela é exibida na lista de categorias. Você pode usar a categoria na configuração do Controle de Aplicativos.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte a Ajuda do Kaspersky Endpoint Security for Linux e a Ajuda do Kaspersky Endpoint Security for Windows.

Visualizando a lista de categorias de aplicativo

Você pode visualizar a lista de categorias de arquivos executáveis configuradas, bem como as configurações de cada uma delas.

Para visualizar a lista de categorias de aplicativos,

No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Categorias de aplicativos**.

A página com uma lista de categorias é exibida.

Para visualizar propriedades de uma categoria de aplicativos,

Clique no nome da categoria.

A janela de propriedades da categoria é exibida. As propriedades estão agrupadas em várias guias.

Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos

Após configurar o Controle de Aplicativos nas políticas do Kaspersky Endpoint Security, os seguintes eventos serão exibidos na lista de eventos:

- **Inicialização do aplicativo proibida** (evento *Crítico*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para aplicar regras.
- **Proibida a inicialização do aplicativo em modo de teste** (evento *Informativo*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para testar regras.
- **Mensagem ao administrador sobre a proibição de inicialização do aplicativo** (evento de *Advertência*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para aplicar regras e um usuário tiver solicitado acesso ao aplicativo bloqueado para inicialização.

É recomendável criar seleções de eventos para visualizar eventos relacionados à operação do Controle de Aplicativos.

Você pode adicionar arquivos executáveis relacionados aos eventos do Controle de Aplicativos à uma categoria de aplicativos existente ou a uma nova categoria de aplicativos. Você pode adicionar arquivos executáveis apenas à categoria de aplicativos com conteúdo adicionado manualmente.

Para adicionar arquivos executáveis relativos aos eventos de Controle de Aplicativos para uma categoria de aplicativos:

1. No menu principal, vá para **Monitoramento → Seleções de eventos**.

   A lista de seleção de eventos é exibida.

2. Selecione a seleção de eventos para visualizar os eventos relacionados ao Controle de Aplicativos e iniciar essa seleção de eventos.

   Se você não criou uma seleção de eventos relacionada ao Controle de Aplicativos, poderá selecionar e iniciar uma seleção predefinida, por exemplo, **Eventos recentes**.

   A lista de eventos é exibida.

3. Selecione os eventos cujos arquivos executáveis associados você deseja adicionar à categoria de aplicativos e clique no botão **Atribuir à categoria**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

4. Na página do assistente, especifique as configurações relevantes:

   - Na seção **Ação em arquivo executável relacionado ao evento**, selecione uma das seguintes opções:

     - **Adicionar a uma nova categoria de aplicativos**

       Selecione esta opção se desejar criar uma nova categoria de aplicativo com base nos arquivos executáveis relacionados ao evento.

       Por padrão, esta opção está selecionada.

       Se você selecionou esta opção, especifique um novo nome de categoria.

     - **Adicionar a uma categoria de aplicativos existente**

       Selecione esta opção se você quiser adicionar arquivos executáveis relativos ao evento a uma categoria de aplicativo existente.

       Por padrão, esta opção não está selecionada.

       Se você selecionou essa opção, selecione a categoria de aplicativo com conteúdo adicionado manualmente ao qual você deseja adicionar arquivos executáveis.

   - Na seção **Tipo de regra**, selecione uma das seguintes opções:

     - **Regras para adicionar às inclusões**

     - **Regras para adicionar às exclusões**

   - Na seção **Parâmetro usado como condição**, selecione uma das seguintes opções:

     - **Detalhes do certificado (ou hashes SHA256 para arquivos sem certificado)**

       Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

       Cada arquivo tem a sua própria função SHA256 hash única. Quando você seleciona uma função SHA256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

       Selecione esta opção se você quiser adicionar às regras de categoria os detalhes do certificado de um arquivo executável (ou a função SHA256 hash de arquivos sem um certificado).

       Por padrão, esta opção está selecionada.

- **Detalhes do certificado (arquivos sem um certificado serão ignorados)**

  Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

  Selecione esta opção se você quiser adicionar os detalhes do certificado de um arquivo executável às regras de categoria. Se o arquivo executável não tiver um certificado, este arquivo será ignorado. Nenhuma informação sobre este arquivo será adicionada à categoria.

- **Somente SHA256 (arquivos sem hash serão ignorados)**

  Cada arquivo tem a sua própria função SHA256 hash única. Quando você seleciona uma função SHA256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

  Selecione esta opção se você quiser adicionar somente os detalhes da função SHA256 hash do arquivo executável.

- **Somente hashes MD5**

  Selecione esta opção somente se você usar o Kaspersky Endpoint Security for Windows. O Kaspersky Endpoint Security for Linux não oferece suporte a uma função de hash MD5.

  Cada arquivo tem a sua própria função MD5 hash única. Quando você seleciona uma função MD5 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

5. Clique em **OK**.

   Quando o assistente for concluído, os arquivos executáveis relacionados aos eventos do Controle de Aplicativos serão adicionados à categoria de aplicativos existente ou a uma nova categoria de aplicativos. Você pode visualizar as configurações da categoria de aplicativos que modificou ou criou.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte a Ajuda do Kaspersky Endpoint Security for Linux e a Ajuda do Kaspersky Endpoint Security for Windows.

Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows

Após você criar as categorias do Controle de Aplicativos, poderá usá-las para configurar o Controle de Aplicativos nas políticas do Kaspersky Endpoint Security for Windows.

Para configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows:

1. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.

   Uma página com uma lista de políticas é exibida.

2. Clique na política do **Kaspersky Endpoint Security for Windows**.

   A janela Propriedades da política será aberta.

3. Acesse **Configurações do aplicativo → Controles de Segurança → Controle de Aplicativos**.

   A janela **Controle de Aplicativos** com as configurações de Controle de Aplicativos é exibida.

4. A opção **Controle de Aplicativos** está ativada por padrão. Alterne o botão **Controle de aplicativos DESATIVADO** para desativar a opção.

5. No configurações de bloqueio **Configurações de Controle de Aplicativos**, ative o modo de operação para aplicar as Regras de Controle de Aplicativos e permita que o Kaspersky Endpoint Security for Windows bloqueie a inicialização de aplicativos.

   Se quiser testar as regras de Controle de Aplicativos, na seção **Configurações de Controle de Aplicativos**, ative o modo de teste. No modo de teste, o Kaspersky Endpoint Security for Windows não bloqueia a inicialização de aplicativos, mas registra no relatório as informações sobre as regras acionadas. Clique no link **Ver relatório** para visualizar esta informação.

6. Ative a opção **Controlar carregamento dos módulos DLL** caso desejar que o Kaspersky Endpoint Security for Windows monitore o carregamento dos módulos DLL quando os aplicativos forem iniciados pelos usuários.

   As informações sobre o módulo e o aplicativo que carregou o módulo serão salvas em um relatório.

   O Kaspersky Endpoint Security for Windows monitora apenas os módulos DLL e drivers carregados após a opção **Controlar carregamento dos módulos DLL** tiver sido selecionada. Reinicie o dispositivo após selecionar a opção **Controlar carregamento dos módulos DLL** se quiser que o Kaspersky Endpoint Security for Windows monitore todos os módulos DLL e drivers, incluindo aqueles carregados antes do Kaspersky Endpoint Security for Windows ter sido iniciado.

7. (Opcional) No bloco **Modelos de mensagem**, altere o modelo da mensagem exibida quando um aplicativo é impedido de iniciar e o modelo da mensagem de e-mail enviada para você.

8. Nas configurações de bloqueio **Modo de Controle de Aplicativos**, selecione o modo **Lista de bloqueio** ou **Lista de permissão**.

   Por padrão, o modo **Lista de bloqueio** é selecionado.

9. Clique no link **Configurações das listas de regras**.

   A janela **Listas de bloqueio e permissão** é aberta para permitir a adição de uma categoria de aplicativo. Por padrão, a guia **Lista de bloqueio** é selecionada se o modo **Lista de bloqueio** estiver selecionado ou a guia **Lista de aprovação** é selecionada se o modo **Lista de aprovação** estiver selecionado.

10. Na janela **Listas de bloqueio e de aprovação**, clique no botão **Adicionar**.

    A janela **Regra de Controle de Aplicativos** abre.

11. Clique no link **Escolha uma categoria**.

    A janela **Categoria de Aplicativo** é aberta.

12. Adicione a categoria de aplicativo (ou categorias) que você criou anteriormente.

    Você pode editar as configurações de uma categoria criada clicando no botão **Editar**.

    Você pode criar uma nova categoria clicando no botão **Adicionar**.

    Você pode excluir uma categoria da lista clicando no botão **Excluir**.

13. Após lista de categorias de aplicativos estiver completa, clique no botão **OK**.

    A janela **Categoria de Aplicativos** é fechada.

14. Na janela Regra de **Controle de Aplicativos**, na seção **Pessoas e seus direitos**, crie uma lista de usuários e grupos de usuários para aplicar a regra de Controle de Aplicativos.

15. Clique no botão **OK** para salvar as configurações e fechar a janela **Regra de Controle de Aplicativos**.

16. Clique no botão **OK** para salvar as configurações e fechar a janela **Listas de bloqueio e de aprovação**.

17. Clique no botão **OK** para salvar as configurações e fechar a janela **Controle de Aplicativos**.

18. Feche a janela com as configurações da política do Kaspersky Endpoint Security for Windows.

    O Controle de Aplicativos está configurado. Após a política ter sido propagada para os dispositivos cliente, a inicialização dos arquivos executáveis é gerenciada.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte a Ajuda do Kaspersky Endpoint Security for Linux e a Ajuda do Kaspersky Endpoint Security for Windows.

Obter e visualizar uma lista de aplicativos instalados nos dispositivos cliente

O Kaspersky Security Center Linux executa um inventário de todos os softwares instalados nos dispositivos clientes gerenciados que executam Linux e Windows.

O Agente de Rede compila uma lista de aplicativos instalados em um dispositivo cliente e, a seguir, transmite esta lista para o Servidor de Administração. São necessários cerca de 10 a 15 minutos para o Agente de Rede atualizar a lista de aplicativos.

Para dispositivos clientes baseados no Windows, o Agente de Rede recebe a maioria das informações sobre os aplicativos instalados do registro do Windows. Para dispositivos clientes baseados em Linux, os gerenciadores de pacotes fornecem ao Agente de Rede informações sobre os aplicativos instalados.

Para exibir a lista de aplicativos instalados nos dispositivos gerenciados:

1. No menu principal, vá para **Gerenciamento de software → Aplicativos de terceiros → Registro de aplicativos**.

   A página exibe uma tabela com os aplicativos instalados nos dispositivos gerenciados. Selecione o aplicativo para visualizar suas propriedades, por exemplo, nome do fornecedor, número da versão, lista de arquivos executáveis e lista de dispositivos nos quais o aplicativo está instalado.

2. É possível agrupar e filtrar os dados da tabela com os aplicativos instalados da seguinte forma:

   - Clique no ícone de configurações ( ) no canto superior direito da tabela.

     No menu **Configurações de colunas** resultante, selecione as colunas a serem exibidas na tabela. Para visualizar o tipo de sistema operacional dos dispositivos clientes nos quais o aplicativo está instalado, selecione a coluna **Tipo do SO**.

   - Clique no ícone de filtro ( ) no canto superior direito da tabela e depois, especifique e aplique o critério de filtro no menu resultante.

     A tabela filtrada de aplicativos instalados é exibida.

Para visualizar a lista de aplicativos instalados em um dispositivo gerenciado específico,

No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados** → **nome do dispositivo** → **Avançado** → **Registro de aplicativos**. Neste menu, é possível exportar a lista de aplicativos para um arquivo CSV ou TXT.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte a Ajuda do Kaspersky Endpoint Security for Linux e a Ajuda do Kaspersky Endpoint Security for Windows.

Sobre aplicativos de terceiros

O Kaspersky Security Center Linux pode ajudar na atualização de software de terceiros instalado em dispositivos clientes, além de corrigir as vulnerabilidades do software de terceiros. O Kaspersky Security Center Linux pode atualizar o software de terceiros apenas da versão atual para a versão mais recente.

A lista de softwares de terceiros pode ser alterada, sendo atualizada dinamicamente. É possível verificar se é possível atualizar o software de terceiros (instalado nos dispositivos dos usuários) com o Kaspersky Security Center Linux ao visualizar a lista de atualizações disponíveis no Kaspersky Security Center Web Console.

O procedimento exposto abaixo tem o único propósito de exibir a lista de softwares de terceiros que podem ser atualizados com o Kaspersky Security Center Linux. As etapas são seguidas para acessar as informações relevantes sem ter de iniciar nenhuma tarefa.

Para visualizar a lista de softwares de terceiros que podem ser atualizados com o Kaspersky Security Center Linux:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na etapa **Novas configurações de tarefa** do assistente, especifique as seguintes configurações:
   a. Na lista suspensa **Aplicativo**, selecione **Kaspersky Security Center Linux**.
   b. No campo **Tipo de tarefa**, selecione **Instalar as atualizações necessárias e corrigir vulnerabilidades**.
4. Na etapa **Escopo da tarefa** do assistente, selecione a opção **Dispositivos gerenciados**.
5. Na etapa **Especifique regras para a instalação de atualizações** do assistente, clique no botão **Adicionar**.

   O Assistente de criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
6. Na etapa **Selecione o tipo de regra** do assistente, selecione a opção **Regra para atualizações de terceiros**.
7. Na etapa **Critérios gerais** do assistente, selecione a opção **Instalar todas as atualizações (exceto as recusadas)** e clique em **Avançar**.

A lista de softwares de terceiros será exibida.

Instalar atualizações de software de terceiros

O Kaspersky Security Center Linux permite gerenciar as atualizações de softwares de terceiros instalados em dispositivos gerenciados e a corrigir vulnerabilidades em tais softwares por meio da instalação das atualizações necessárias.

O Kaspersky Security Center Linux procura atualizações por meio da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Servidor de Administração recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa. Após visualizar as informações sobre as atualizações disponíveis, você pode instalar essas atualizações seus dispositivos.

O Kaspersky Security Center Linux atualiza alguns aplicativos ao remover a versão anterior do aplicativo e ao instalar uma nova versão.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Por motivos de segurança, todas as atualizações de softwares de terceiros instaladas usando o recurso Gerenciamento de patches e vulnerabilidades são verificadas automaticamente pelas tecnologias da Kaspersky em busca de malwares. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

Quando os metadados das atualizações de software de terceiros são baixados para o repositório, você pode instalar as atualizações nos dispositivos clientes usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

> A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades.

Quando essa tarefa é concluída, as atualizações são instaladas nos dispositivos gerenciados automaticamente. Quando os metadados das novas atualizações são baixados no repositório do Servidor de Administração, o Kaspersky Security Center Linux verifica se as atualizações atendem aos critérios especificados nas regras de atualização. Todas as novas atualizações que atendem aos critérios serão baixadas e instaladas automaticamente na próxima tarefa executada.

Cenário: Atualizando software de terceiros

Esta seção fornece um cenário para a atualização software de terceiros instalados nos dispositivos clientes. Software de terceiros incluem aplicativos de outros fornecedores de software.

Pré-requisitos

O Servidor de Administração deve estar conectado à Internet para instalar atualizações de software de terceiros.

Fases

A atualização de software de terceiros prossegue em fases:

1. **Procurar atualizações necessárias**

   Para encontrar as atualizações de softwares de terceiros necessárias para os dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa é concluída, o Kaspersky Security Center Linux recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

   A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo Assistente de início rápido do Servidor de Administração. Caso não tenha executado o assistente, crie a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou execute o assistente de início rápido agora.

   > Você pode criar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* somente para dispositivos Windows. Você não pode criar esta tarefa para dispositivos em execução em outros sistemas operacionais.

2. **Visualizar a lista de atualizações encontradas**

   Visualize informações sobre as atualizações de software de terceiros disponíveis e decida quais atualizações você deseja instalar. Para visualizar informações detalhadas sobre cada atualização, clique no nome da atualização na lista. Para cada atualização na lista, você também pode visualizar as estatísticas sobre a instalação da atualização nos dispositivos cliente.

3. **Configurar instalação de atualizações**

   Quando o Kaspersky Security Center Linux recebe a lista de atualizações de software de terceiros, será possível instalá-las em dispositivos clientes criando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

   > Você pode criar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* somente para dispositivos Windows. Você não pode criar esta tarefa para dispositivos em execução em outros sistemas operacionais.

   A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para instalar atualizações para aplicativos da Microsoft, incluindo as atualizações fornecidas pelo serviço Windows Update e atualizações de software de outros fornecedores. Observe que a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades.

   Para instalar algumas atualizações de software, você deve aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software. Se você recusar o EULA, a atualização do software não será instalada.

   Você pode iniciar uma tarefa de instalação de atualizações. Ao especificar o agendamento de tarefas, certifique-se de que a tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

4. **Agendar as tarefas**

   Para garantir que a lista de atualizações esteja sempre atualizada, agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para executá-la automaticamente de tempos em tempos. Por padrão, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é configurada para iniciar manualmente.

   Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência.

   Ao agendar as tarefas, certifique-se de que uma tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

5. **Aprovando e recusando atualizações de software de terceiros (opcional)**

   Se você tiver criado a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, poderá especificar regras para instalação da atualização na janela de propriedades da tarefa.

   Para cada regra, você pode definir as atualizações a serem instaladas, dependendo do status da atualização: *Indefinido*, *Aprovado* ou *Negado*. Por exemplo, convém criar uma tarefa específica para servidores e definir uma regra para essa tarefa para permitir a instalação apenas de aquelas atualizações com status *Aprovado*. Depois disso, você define manualmente o status *Aprovado* para as atualizações que deseja instalar. Nesse caso, as atualizações com status *Indefinido* ou *Negado* não serão instaladas nos servidores especificados para a tarefa.

   O uso do status *Aprovado* para gerenciar a instalação da atualização é eficiente para uma pequena quantidade de atualizações. Para instalar várias atualizações, use as regras que você pode configurar na tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Recomendamos que você defina o status *Aprovado* apenas para as atualizações específicas que não atendem aos critérios especificados nas regras. Se você aprovar manualmente um grande número de atualizações, o desempenho do Servidor de Administração diminui, o que pode levar a uma sobrecarga do Servidor de Administração.

   Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Você pode alterar o status para *Aprovado* ou *Negado* na lista **Atualizações de software** (**Gerenciamento de software** → **Gerenciamento de patches** → **Atualizações de software**).

   Para obter mais detalhes, consulte as instruções sobre como aprovar e recusar atualizações de software de terceiros.

6. **Executar uma tarefa de instalação de atualização**

   Iniciar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* Quando você inicia essa tarefa, as atualizações são baixadas e instaladas nos dispositivos gerenciados. Após a conclusão da tarefa, verifique se ela possui o status *Conclusão com êxito* na lista de tarefas.

7. **Crie um relatório sobre os resultados da instalação da atualização (opcional)**

   Para ver estatísticas detalhadas sobre a instalação de atualização, gere um Relatório de resultados da instalação de atualizações de software de terceiros.

Resultados

Se você tiver criado e configurado a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, as atualizações serão instaladas nos dispositivos gerenciados automaticamente. Quando novas atualizações são baixadas no repositório do Servidor de Administração, o Kaspersky Security Center Linux verifica se elas atendem aos critérios especificados nas regras de atualização. Todas as novas atualizações que atendem aos critérios serão instaladas automaticamente na próxima tarefa executada.

Opções de instalação de atualizações de software de terceiros

Você pode instalar atualizações de software de terceiros e atualizações do Windows Update em dispositivos gerenciados criando e executando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades. Você pode usar essa tarefa para instalar as atualizações de software de outros fornecedores.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Como opção, é possível criar uma tarefa para instalar as atualizações necessárias das seguintes maneiras:

- Abrindo a lista de atualizações e, então, especificando quais atualizações instalar.

  Como resultado, é criada uma nova tarefa para instalar as atualizações selecionadas. Como opção, você pode adicionar as atualizações selecionadas a uma tarefa existente.

- Executando o assistente de instalação de atualização.

  O Assistente de instalação das Atualizações só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

  O assistente simplifica a criação e configuração de uma tarefa de instalação de atualizações e permite eliminar a criação de tarefas redundantes que contenham as mesmas atualizações a serem instaladas.

Instalar atualizações de softwares de terceiros usando a lista de atualizações

Para instalar atualizações de software de terceiros usando a lista de atualizações:

1. Abra a lista de atualizações usando um dos seguintes caminhos:

   - **Gerenciamento de software** → **Gerenciamento de patches** → **Atualizações de software**.
   - **Gerenciamento de ativos** → **Dispositivos gerenciados** → <nome do dispositivo> → **Avançado** → **Atualizações disponíveis**.
   - **Gerenciamento de software** → **Aplicativos de terceiros** → **Registro de aplicativos** → <nome do aplicativo> → **Atualizações disponíveis**.

   Aparece uma lista das atualizações disponíveis.

2. Marque as caixas de seleção ao lado das atualizações que deseja baixar.

3. Clique no botão **Instalar as atualizações**. Se esse botão não estiver visível, clique no botão de reticências e selecione **Instalar as atualizações** na lista suspensa.

   Para instalar algumas atualizações de software, você deve aceitar o Contrato de Licença do Usuário Final (EULA). Se você recusar o EULA, a atualização do software não é instalada.

4. Escolha uma das seguintes opções:

   - **Nova tarefa**

     O Assistente para novas tarefas inicia. Se você tiver a licença do Gerenciamento de patches e vulnerabilidades, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será pré-selecionada. Seguem abaixo as etapas do assistente para concluir a criação da tarefa.

   - **Instalar a atualização (adicionar a regra à tarefa especificada)**

     Selecione uma tarefa à qual deseja adicionar as atualizações selecionadas. Se você tiver a licença de Gerenciamento de patches e vulnerabilidades, selecione a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Uma nova regra para instalar as atualizações selecionadas é adicionada automaticamente à tarefa escolhida. As atualizações selecionadas são adicionadas às propriedades da tarefa.

     A janela de propriedades da tarefa é aberta. Clique em **Salvar** para salvar as alterações.

   Se você escolheu criar uma nova tarefa, ela será criada e exibida na lista de tarefas em **Tarefas**. Se você optou por adicionar as atualizações a uma tarefa existente, as atualizações serão salvas nas propriedades da tarefa.

Para instalar atualizações de software de terceiros, você deve iniciar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Você pode iniciar esta tarefa clicando no botão **Iniciar** na lista de tarefas ou especificando as configurações de agendamento nas propriedades da tarefa iniciada. Ao especificar o agendamento de tarefas, certifique-se de que a tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

Instalar atualizações de softwares de terceiros usando o assistente de instalação de atualização

O Assistente de instalação das Atualizações só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

Para criar uma tarefa para instalar atualizações de softwares de terceiros usando o assistente de instalação de atualização:

1. No menu principal, vá para **Gerenciamento de software → Gerenciamento de patches → Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.

2. Marque a caixa de seleção ao lado da atualização que deseja instalar.

3. Clique no botão **Executar o Assistente de Instalação de Atualização**.

   O Assistente de instalação de atualização inicia. A página **Selecionar tarefa de instalação de atualização** exibe a lista de todas as tarefas existentes dos seguintes tipos:

   - *Instalar as atualizações necessárias e corrigir vulnerabilidades*
   - *Corrigir vulnerabilidades*

4. Caso deseje que o assistente exiba apenas as tarefas que instalam a atualização selecionada, ative a opção **Mostrar apenas tarefas que instalam esta atualização**.

5. Selecione o que deseja fazer:

- Para iniciar uma tarefa existente, marque a caixa de seleção ao lado da tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* e clique no botão **Iniciar**.

  A tarefa será concluída no modo de segundo plano. Nenhuma outra ação será necessária.

- Para adicionar uma nova regra a uma tarefa existente:

  a. Marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Adicionar regra**.

  > O botão **Adicionar regra** é desativado se você selecionar mais de uma tarefa.

  Você não pode adicionar uma regra para uma tarefa *Corrigir vulnerabilidades*. Se você selecionar uma tarefa *Corrigir vulnerabilidades*, a seguinte notificação será exibida: "*Para instalar atualizações, use a tarefa "Instalar as atualizações necessárias e corrigir vulnerabilidades*".

  b. Na etapa **Criar regra de instalação da atualização** do assistente, configure a nova regra:

  - **Regra de instalação de atualizações deste nível de importância**

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

    Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

    Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

    Por padrão, esta opção está desativada.

    Esta regra não é exibida se o nível de importância da atualização selecionada for *Desconhecido*.

  - **Regra de instalação de atualizações deste nível de importância de acordo com o MSRC**

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

    Se esta opção estiver ativada (disponível apenas para atualizações do Windows Update), as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

    Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

    Por padrão, esta opção está desativada.

    Esta regra é exibida somente para atualizações de software da Microsoft. Ela não será exibida se o nível de importância da atualização selecionada for *Desconhecido*.

  - **Regra de instalação para atualizações deste fornecedor**

Esta opção está disponível apenas para atualizações de aplicativos de terceiros. O Kaspersky Security Center Linux instala apenas as atualizações relacionadas aos aplicativos feitos pelo mesmo fornecedor que a atualização selecionada. As atualizações recusadas e as atualizações dos aplicativos feitos por outros fornecedores não são instaladas.

Por padrão, esta opção está desativada.

Esta regra é exibida somente para atualizações de software de terceiros.

- **Regra de instalação para atualizações do tipo**
- **Regra de instalação para atualizações do aplicativo selecionado**

  Esta regra é exibida somente para atualizações de software de terceiros.

- **Regra de instalação para a atualização selecionada**
- **Aprovar atualizações selecionadas**

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

- **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

  Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

  Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

  Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

  Por padrão, esta opção está ativada.

c. Clique em **Adicionar**.

A janela de propriedades da tarefa é aberta. A nova regra já foi adicionada às propriedades da tarefa. Você pode visualizar ou modificar a regra ou outras configurações de tarefa. Clique em **Salvar** para salvar as alterações.

- Para criar uma tarefa:

  a. Clique no botão **Nova tarefa**.

  b. Na etapa **Criar regra de instalação da atualização** do assistente, configure a nova regra:

  - **Regra de instalação de atualizações deste nível de importância**

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

Por padrão, esta opção está desativada.

Esta regra não é exibida se o nível de importância da atualização selecionada for *Desconhecido*.

- **Regra de instalação de atualizações deste nível de importância de acordo com o MSRC**

  Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

  Se esta opção estiver ativada (disponível apenas para atualizações do Windows Update), as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

  Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

  Por padrão, esta opção está desativada.

  Esta regra é exibida somente para atualizações de software da Microsoft. Ela não será exibida se o nível de importância da atualização selecionada for *Desconhecido*.

- **Regra de instalação para atualizações deste fornecedor**

  Esta opção está disponível apenas para atualizações de aplicativos de terceiros. O Kaspersky Security Center Linux instala apenas as atualizações relacionadas aos aplicativos feitos pelo mesmo fornecedor que a atualização selecionada. As atualizações recusadas e as atualizações dos aplicativos feitos por outros fornecedores não são instaladas.

  Por padrão, esta opção está desativada.

  Esta regra é exibida somente para atualizações de software de terceiros.

- **Regra de instalação para atualizações do tipo**

- **Regra de instalação para atualizações do aplicativo selecionado**

  Esta regra é exibida somente para atualizações de software de terceiros.

- **Regra de instalação para a atualização selecionada**

- **Aprovar atualizações selecionadas**

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

- **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

  Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

Por padrão, esta opção está ativada.

c. Clique em **Adicionar**.

Continue a criar a tarefa no Assistente para novas tarefas. A nova regra adicionada no assistente de instalação de atualização é exibida no Assistente para Novas Tarefas. Ao concluir o assistente, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será adicionada na lista de tarefas.

As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias

A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente quando o Assistente de Início Rápido é executado. Se você não tiver executado o Assistente, poderá criar a tarefa manualmente.

Além das configurações gerais da tarefa, é possível especificar as seguintes configurações ao criar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou mais recentes, ao configurar as propriedades da tarefa criada:

- **Buscar por vulnerabilidades e atualizações listadas pela Microsoft**

  Ao procurar por vulnerabilidades e atualizações, o Kaspersky Security Center Linux usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft, que estão disponíveis no momento.

  Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

  As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

- **Conectar com o servidor de atualizações para atualizar dados**

  O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

  - Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
  - Servidores de atualizações da Microsoft

  Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

Caso esta opção esteja desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows recebidas da fonte de atualizações da Microsoft antes.

A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

Por padrão, esta opção está ativada.

A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

- O Windows Update Agent em um dispositivo gerenciado se conecta ao servidor de atualização para receber atualizações somente se a configuração **Conectar com o servidor de atualizações para atualizar dados** estiver ativada nas propriedades da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* e o **Modo de pesquisa do Windows Update** estiver definido como **Ativo** nas configurações da política do Agente de Rede.

- Caso não precise do Agente de Rede para iniciar uma conexão com a fonte de atualização do Microsoft Windows e as atualizações sejam baixadas durante a execução da tarefa de *Verificação de vulnerabilidades*, será possível definir a opção **Modo de pesquisa do Windows Update** como **Passivo**, enquanto a opção **Conectar com o servidor de atualizações para atualizar dados** deve permanecer ativada. Isso permite economizar recursos e usar atualizações do Windows recebidas anteriormente para verificar vulnerabilidades. É possível usar o modo passivo se o recebimento de atualizações do Microsoft Windows for configurado de uma forma diferente. Caso o recebimento de atualizações do Microsoft Windows não seja configurado de outra forma, não defina a opção **Modo de pesquisa do Windows Update** como **Passivo**, pois, nesse caso, as informações sobre as atualizações nunca serão recebidas.

- Independentemente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativada ou desativada), caso a opção **Modo de pesquisa do Windows Update** esteja definida como **Desativado**, o Kaspersky Security Center Linux não solicitará nenhuma informação sobre as atualizações.

Se na rede da sua organização o servidor WSUS for utilizado (servidor WSUS local) e você quiser utilizá-lo junto com o Servidor de Administração do Kaspersky Security Center, você deve primeiro assegurar-se de que o Servidor de Administração do Kaspersky Security Center não seja utilizado como um servidor WSUS, e, em seguida, faça o seguinte:

1. Nos dispositivos gerenciados que executam o Windows, especifique o servidor WSUS local para o serviço Windows Update. É possível fazer isso manualmente no Registro do Windows ou utilizando uma política de grupo do Windows.

2. No servidor WSUS local, especifique as classificações necessárias para as atualizações e os aplicativos nos quais as atualizações devem ser distribuídas.

3. Sincronize o servidor WSUS com o servidor upstream (que pode ser um servidor Microsoft WSUS ou outro servidor WSUS upstream local).

Após a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ser executada no dispositivo, o Agente de Rede utilizará o serviço Windows Update para iniciar uma solicitação de atualizações do Windows aplicáveis ao dispositivo. O serviço Windows Update obtém o endereço do servidor WSUS externo do registro e busca atualizações diretamente desse servidor WSUS externo. Em seguida, o serviço Windows Update encaminha esta lista para o Servidor de Administração por meio do Agente de Rede. Assim, o Servidor de Administração terá uma base atualizada.

- **Buscar vulnerabilidades e atualizações de terceiros listadas pela Kaspersky**

  Se esta opção estiver ativada, o Kaspersky Security Center Linux pesquisará vulnerabilidades e as atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

  Se esta opção estiver desativada, o Kaspersky Security Center Linux não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

- **Especifique caminhos para a pesquisa avançada de aplicativos no sistema de arquivos**

  As pastas nas quais o Kaspersky Security Center Linux pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

  Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista contém pastas do sistema nas quais a maioria dos aplicativos está instalada.

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento ainda que esta opção esteja desativada para ele no Utilitário de Diagnóstico Remoto do Kaspersky Security Center Linux. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede grava rastreamentos de acordo com as configurações do Utilitário de Diagnóstico Remoto do Kaspersky Security Center Linux. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

Recomendações sobre o agendamento de tarefas

Ao agendar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*, certifique-se de que as duas opções **Executar tarefas ignoradas** e **Usar atraso aleatório automaticamente para início da tarefa** estejam desativadas.

Por padrão, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é configurada para iniciar manualmente. Se as regras do local de trabalho da organização proverem o desligamento de todos os dispositivos nessa hora, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* será executada após os dispositivos serem novamente ligados, ou seja, na manhã seguinte. Tal atividade pode ser indesejável porque uma verificação de vulnerabilidades pode aumentar a carga de subsistemas de disco e da CPU. Você deve definir o agendamento mais conveniente para a tarefa com base nas regras do local de trabalho adotadas na organização.

Criar a tarefa Encontrar vulnerabilidades e atualizações necessárias

Por meio da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*, o Kaspersky Security Center Linux recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para o software de terceiro instalado nos dispositivos gerenciados.

Você pode criar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* somente para dispositivos Windows. Você não pode criar esta tarefa para dispositivos em execução em outros sistemas operacionais.

A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente quando o Assistente de Início Rápido é executado. Caso não tenha executado o assistente, é possível criar a tarefa manualmente.

Para criar uma tarefa Encontrar as vulnerabilidades e as atualizações necessárias:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Encontrar as vulnerabilidades e as atualizações necessárias**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Selecione os dispositivos aos quais a tarefa será atribuída.
6. Especifique os métodos para verificar vulnerabilidades e aplicativos que requerem atualização:

   - **Buscar por vulnerabilidades e atualizações listadas pela Microsoft**

     Ao procurar por vulnerabilidades e atualizações, o Kaspersky Security Center Linux usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft, que estão disponíveis no momento.

     Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

     Por padrão, esta opção está ativada.

As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

- **Conectar com o servidor de atualizações para atualizar dados**

  O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

  - Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
  - Servidores de atualizações da Microsoft

  Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

  Caso esta opção esteja desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows recebidas da fonte de atualizações da Microsoft antes.

  A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

  Por padrão, esta opção está ativada.

  A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

  - O Windows Update Agent em um dispositivo gerenciado se conecta ao servidor de atualização para receber atualizações somente se a configuração **Conectar com o servidor de atualizações para atualizar dados** estiver ativada nas propriedades da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* e o **Modo de pesquisa do Windows Update** estiver definido como **Ativo** nas configurações da política do Agente de Rede.
  - Caso não precise do Agente de Rede para iniciar uma conexão com a fonte de atualização do Microsoft Windows e as atualizações sejam baixadas durante a execução da tarefa de *Verificação de vulnerabilidades*, será possível definir a opção **Modo de pesquisa do Windows Update** como **Passivo**, enquanto a opção **Conectar com o servidor de atualizações para atualizar dados** deve permanecer ativada. Isso permite economizar recursos e usar atualizações do Windows recebidas anteriormente para verificar vulnerabilidades. É possível usar o modo passivo se o recebimento de atualizações do Microsoft Windows for configurado de uma forma diferente. Caso o recebimento de atualizações do Microsoft Windows não seja configurado de outra forma, não defina a opção **Modo de pesquisa do Windows Update** como **Passivo**, pois, nesse caso, as informações sobre as atualizações nunca serão recebidas.
  - Independentemente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativada ou desativada), caso a opção **Modo de pesquisa do Windows Update** esteja definida como **Desativado**, o Kaspersky Security Center Linux não solicitará nenhuma informação sobre as atualizações.

Se na rede da sua organização o servidor WSUS for utilizado (servidor WSUS local) e você quiser utilizá-lo junto com o Servidor de Administração do Kaspersky Security Center, você deve primeiro assegurar-se de que o Servidor de Administração do Kaspersky Security Center não seja utilizado como um servidor WSUS, e, em seguida, faça o seguinte:

1. Nos dispositivos gerenciados que executam o Windows, especifique o servidor WSUS local para o serviço Windows Update. É possível fazer isso manualmente no Registro do Windows ou utilizando uma política de grupo do Windows.

2. No servidor WSUS local, especifique as classificações necessárias para as atualizações e os aplicativos nos quais as atualizações devem ser distribuídas.

3. Sincronize o servidor WSUS com o servidor upstream (que pode ser um servidor Microsoft WSUS ou outro servidor WSUS upstream local).

Após a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ser executada no dispositivo, o Agente de Rede utilizará o serviço Windows Update para iniciar uma solicitação de atualizações do Windows aplicáveis ao dispositivo. O serviço Windows Update obtém o endereço do servidor WSUS externo do registro e busca atualizações diretamente desse servidor WSUS externo. Em seguida, o serviço Windows Update encaminha esta lista para o Servidor de Administração por meio do Agente de Rede. Assim, o Servidor de Administração terá uma base atualizada.

- **Buscar vulnerabilidades e atualizações de terceiros listadas pela Kaspersky**

  Se esta opção estiver ativada, o Kaspersky Security Center Linux pesquisará vulnerabilidades e as atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

  Se esta opção estiver desativada, o Kaspersky Security Center Linux não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

Você pode desativar essas opções após a criação da tarefa na guia **Configurações do aplicativo** da janela de propriedades da tarefa.

7. **Especifique caminhos para a pesquisa avançada de aplicativos no sistema de arquivos**

   As pastas nas quais o Kaspersky Security Center Linux pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

   Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista contém pastas do sistema nas quais a maioria dos aplicativos está instalada.

   Você pode alterar os caminhos especificados após a criação da tarefa na guia **Configurações do aplicativo** da janela de propriedades da tarefa.

8. Se necessário, **Ativar diagnóstico avançado**

   Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento ainda que esta opção esteja desativada para ele no Utilitário de Diagnóstico Remoto do Kaspersky Security Center Linux. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

   Se esse recurso estiver desativado, o Agente de Rede grava rastreamentos de acordo com as configurações do Utilitário de Diagnóstico Remoto do Kaspersky Security Center Linux. Nenhum rastreamento adicional é gravado.

   Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

   Por padrão, esta opção está desativada.

   Você pode desativar esta opção após a criação da tarefa na guia **Configurações do aplicativo** da janela de propriedades da tarefa.

9. Especifique o **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

   O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

   Você deve especificar esse valor se tiver ativado o diagnóstico avançado na etapa anterior. Você pode alterar esse valor após a criação da tarefa na guia **Configurações do aplicativo** da janela de propriedades da tarefa.

10. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode alterar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    O assistente cria a tarefa. Caso a opção **Abrir detalhes da tarefa quando a criação for concluída** tenha sido ativada, a janela de propriedades da tarefa abrirá automaticamente. Nesta janela, você pode especificar as configurações gerais da tarefa e, se necessário, alterar as configurações especificadas durante a criação da tarefa.

    > Você também pode abrir a respectiva janela de propriedades clicando no nome da tarefa criada na lista de tarefas.

A tarefa é criada e configurada. Para executar a tarefa, selecione-a na lista de tarefas e, então, clique no botão **Iniciar**.

Recomendações sobre o agendamento de tarefas

Ao agendar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*, certifique-se de que as duas opções **Executar tarefas ignoradas** e **Usar atraso aleatório automaticamente para início da tarefa** estejam desativadas.

Por padrão, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é configurada para iniciar manualmente.

Você também pode agendar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para iniciar em um horário específico. Por exemplo, você pode selecionar o início agendado **A cada N horas** na lista suspensa **Iniciar tarefa**, na guia **Agendamento** na janela de propriedades da tarefa. Nesse caso, observe que se as regras do local de trabalho da organização preveem o desligamento de todos os dispositivos nessa hora, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* será executada após os dispositivos serem novamente ligados. Tal atividade pode ser indesejável porque uma verificação de vulnerabilidades pode aumentar a carga de subsistemas de disco e da CPU. Você deve definir o agendamento mais conveniente para a tarefa com base nas regras do local de trabalho adotadas na organização.

Para obter uma descrição detalhada das configurações de início agendado, consulte as configurações gerais da tarefa.

Exibir informações sobre atualizações disponíveis para software de terceiros

Você pode visualizar a lista de atualizações disponíveis para software de terceiros, incluindo software da Microsoft, instalado em dispositivos cliente.

Para exibir uma lista de atualizações disponíveis para aplicativos de terceiros instalados em dispositivos clientes:

No menu principal, vá para **Gerenciamento de software → Gerenciamento de patches → Atualizações de software**.

Aparece uma lista das atualizações disponíveis.

Você pode especificar um filtro para visualizar a lista de atualizações de software. Clique no ícone de **Filtro** ( ) da lista de atualizações de software para gerenciar o filtro. Você também pode selecionar um dos filtros predefinidos na lista suspensa **Filtros predefinidos**, acima da lista de vulnerabilidades de software.

Para visualizar as propriedades de uma atualização:

1. Clique no nome da atualização de software necessária.
2. A janela de propriedades da atualização é aberta, exibindo informações agrupadas nas seguintes guias:
   - **Geral**

     Esta guia exibe detalhes gerais da atualização selecionada:

     - Status de aprovação da atualização (pode ser alterado manualmente, selecionando um novo status na lista suspensa)
     - Data e hora em que a atualização foi registrada
     - Data e hora em que a atualização foi criada
     - Nível de importância da atualização
     - Requisitos de instalação impostos pela atualização

- Família de aplicativos à qual a atualização pertence
- Aplicativo ao qual a atualização se aplica
- Número da revisão de atualização

- **Atributos**

  Esta guia exibe um conjunto de atributos que você pode usar para obter mais informações sobre a atualização selecionada. Este conjunto difere, dependendo se a atualização é publicada pela Microsoft ou por um fornecedor terceiro.

  A guia exibe as seguintes informações para uma atualização da Microsoft:

  - O nível de importância da atualização, conforme definido pelo Microsoft Security Response Center (MSRC)
  - Link para o artigo na Base de Dados de Conhecimento Microsoft que descreve a atualização
  - Link para o artigo no Boletim de Segurança da Microsoft que descreve a atualização
  - Identificador da atualização (ID)

  A guia exibe as seguintes informações para uma atualização de terceiros:

  - Se a atualização é um patch ou um pacote de distribuição completo
  - Idioma de localização da atualização
  - Se a atualização é instalada automática ou manualmente
  - Se a atualização foi revogada após ser aplicada
  - Link para baixar a atualização

- **Dispositivos**

  Esta guia exibe uma lista de dispositivos nos quais a atualização selecionada foi instalada.

- **Vulnerabilidades corrigidas**

  Esta guia exibe uma lista de vulnerabilidades que a atualização selecionada pode corrigir.

- **Cruzamento de atualizações**

  Esta guia exibe possíveis redundâncias entre várias atualizações publicadas para o mesmo aplicativo, ou seja, se a atualização selecionada pode substituir outras atualizações ou, vice-versa (disponíveis apenas para atualizações Windows).

- **Tarefas para instalar esta atualização**

  Esta guia exibe uma lista de tarefas cujo escopo inclui a instalação da atualização selecionada. A guia também permite que você crie uma nova tarefa de instalação remota para a atualização.

Para exibir as estatísticas de uma instalação de atualização:

1. Selecione a caixa de seleção ao lado da atualização de software necessária.

2. Clique no botão **Estatísticas de status da instalação de atualizações**.

O diagrama dos status de instalação da atualização é exibido. Clicar em um status abre uma lista de dispositivos que têm o status selecionado.

Você pode visualizar informações sobre atualizações de software disponíveis para software de terceiros, incluindo software da Microsoft, instalado no dispositivo gerenciado selecionado que executa o Windows.

Para visualizar a lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo para o qual você deseja visualizar atualizações de software de terceiros.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Na janela de propriedades do dispositivo selecionado, selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Atualizações disponíveis**. Caso deseje visualizar apenas as atualizações instaladas, ative a opção **Mostrar atualizações instaladas**.

A lista de atualizações de software de terceiros disponíveis para o dispositivo selecionado é exibida.

Exportando a lista de vulnerabilidades de software para um arquivo

Você pode exportar a lista de atualizações para software de terceiros, incluindo o software Microsoft, para um arquivo CSV e TXT. Você pode usar esses arquivos, por exemplo, para enviá-los ao seu gerente de segurança de informações ou para armazená-los para fins de estatística.

Para exportar como arquivo de texto a lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.

   Se você deseja exportar a lista completa de atualizações de software, apenas as atualizações exibidas na página atual serão exportadas.

Se você quiser exportar apenas atualizações específicas, marque as caixas de seleção ao lado das atualizações necessárias na lista.

2. Clique no botão **Exportar para TXT** ou **Exportar para CSV**, dependendo do formato preferido. Se algum desses botões não estiver visível, clique no botão de reticências e selecione a opção necessária na lista suspensa.

O arquivo que contém a lista de atualizações disponíveis para software de terceiros, incluindo software da Microsoft, é baixado para o dispositivo atual.

Para exportar como arquivo de texto uma lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:

1. Abra a lista de atualizações de software de terceiros disponíveis no dispositivo gerenciado selecionado.

   Aparece uma lista das atualizações disponíveis.

   Se você deseja exportar a lista completa de atualizações de software, apenas as atualizações exibidas na página atual serão exportadas.

   Se você quiser exportar apenas atualizações específicas, marque as caixas de seleção ao lado das atualizações necessárias na lista.

   Se deseja exportar apenas as atualizações instaladas, marque a caixa **Mostrar atualizações instaladas**.

2. Clique no botão **Exportar para TXT** ou **Exportar para CSV**, dependendo do formato preferido. Se algum desses botões não estiver visível, clique no botão de reticências e selecione a opção necessária na lista suspensa.

O arquivo contendo a lista de atualizações para software de terceiros, incluindo software da Microsoft, instalado no dispositivo gerenciado selecionado, é baixado para o dispositivo usado no momento.

Aprovando e recusando atualizações de software de terceiros

Ao configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é possível criar uma regra que exija um status específico das atualizações a serem instaladas. Por exemplo, uma regra de atualização pode permitir a instalação do seguinte:

- Somente atualizações aprovadas
- Somente atualizações aprovadas e indefinidas
- Todas as atualizações, independentemente dos status de atualização

Você pode aprovar atualizações que devem ser instaladas e recusar as atualizações que não devem ser instaladas.

O uso do status *Aprovado* para gerenciar a instalação da atualização é eficiente para uma pequena quantidade de atualizações. Para instalar várias atualizações, use as regras que você pode configurar nas propriedades da tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* Recomendamos que você defina o status *Aprovado* apenas para as atualizações específicas que não atendem aos critérios especificados nas regras. Quando você aprova manualmente um grande número de atualizações, o desempenho do Servidor de Administração diminui, o que pode levar a uma sobrecarga do Servidor de Administração.

Para aprovar ou recusar uma ou várias atualizações:

1. No menu principal, vá para **Gerenciamento de software → Gerenciamento de patches → Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.

2. Selecione as atualizações que deseja aprovar ou recusar.

3. Clique no botão **Aprovar** para aprovar as atualizações selecionadas ou no botão **Recusar** para recusar as atualizações selecionadas. Se algum desses botões não estiver visível, clique no botão de reticências e selecione a opção necessária na lista suspensa.

   O status padrão de uma atualização é *Indefinido*.

As atualizações selecionadas têm os status que você definiu.

Como opção, você pode alterar o status de aprovação nas propriedades de uma atualização específica.

Para aprovar ou recusar uma atualização em suas propriedades:

1. No menu principal, vá para **Gerenciamento de software → Gerenciamento de patches → Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.

2. Clique no nome da atualização que deseja aprovar ou recusar.

   A janela Propriedades da atualização é aberta.

3. Na seção **Geral**, selecione um status para a atualização na lista suspensa **Status de aprovação da atualização**. Você pode selecionar o status *Aprovado*, *Negado*, ou *Indefinido*.

4. Clique em **Salvar** para salvar as alterações.

A atualização selecionada tem o status que você definiu.

Caso o status *Negado* seja definido para as atualizações de software de terceiros, as atualizações não serão instaladas em dispositivos para os quais elas foram planejadas, mas que ainda não foram instaladas. As atualizações permanecerão nos dispositivos nos quais elas já foram instaladas. Se necessário, você pode excluí-los manualmente localmente.

Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros instalado nos dispositivos gerenciados. Essa tarefa permite instalar várias atualizações e corrigir várias vulnerabilidades de acordo com as regras especificadas nas configurações da tarefa.

Para instalar atualizações ou corrigir vulnerabilidades usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, execute uma das seguintes ações:

- Execute o assistente de instalação de atualização ou o assistente para correção de vulnerabilidades.
- Crie uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.
- Adicione uma regra para instalação da atualização a uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.

Para criar uma tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades:

1. No menu principal, vá para **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na lista suspensa **Aplicativo**, selecione Kaspersky Security Center Linux.
4. Na lista **Tipo de tarefa**, selecione o tipo de tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades**.

   Caso a tarefa não seja exibida, certifique-se de que sua conta tenha direitos de **Leitura**, **Gravação** e **Execução** para a área funcional **Gerenciamento de sistema**: **Gerenciamento de patches e vulnerabilidades**. Você não pode criar e configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* sem esses direitos de acesso.
5. No campo **Nome da tarefa**, especifique o nome da nova tarefa.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).
6. Selecione os dispositivos aos quais a tarefa será atribuída.
7. Adicione as regras de instalação de atualizações na etapa **Especifique regras para a instalação de atualizações** do assistente.

   Estas regras são aplicadas à instalação de atualizações nos dispositivos cliente. Se as regras não forem especificadas, a tarefa não terá nenhuma ação a ser executada. Para obter informações sobre operações com regras, consulte Regras para instalação da atualização.

   Estas regras são aplicadas à instalação de atualizações nos dispositivos cliente. Se você não especificar nenhuma regra, a tarefa não terá nada a executar.
8. Especificar as seguintes configurações:

   - **Iniciar a instalação ao reiniciar ou fechar o dispositivo**

     Se esta opção estiver ativada, as atualizações serão instaladas quando o dispositivo for reiniciado ou desligado. Caso contrário, as atualizações são instaladas segundo o agendamento.

     Use esta opção caso a instalação das atualizações afete o desempenho do dispositivo.

     Por padrão, esta opção está desativada.

   - **Instalar os componentes obrigatórios gerais do sistema**

     Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional.

Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

Por padrão, esta opção está desativada.

- **Permitir a instalação de novas versões dos aplicativos durante atualizações**

  Se esta opção estiver ativada, as atualizações serão permitidas quando resultarem na instalação de uma nova versão de um aplicativo de software.

  Se esta opção estiver desativada, o software não será atualizado. Você poderá então instalar novas versões do software manualmente ou através de outra tarefa. Por exemplo, você pode usar esta opção se a infraestrutura da sua empresa não tiver como base uma nova versão do software ou se você quiser verificar uma atualização usando uma infraestrutura de teste.

  Por padrão, esta opção está ativada.

  > A atualização de um aplicativo pode causar o funcionamento incorreto de aplicativos dependentes instalados em dispositivos cliente.

- **Baixar atualizações para o dispositivo sem instalá-las**

  Se esta opção estiver ativada, o aplicativo baixa as atualizações em um dispositivo cliente, mas não as instala automaticamente. Você então poderá instalar manualmente as atualizações baixadas.

  As atualizações da Microsoft são baixadas no armazenamento de sistema do Windows. Atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky e à Microsoft) são baixados na pasta especificada no campo **Baixar atualizações para**.

  Se esta opção estiver desativada, as atualizações serão instaladas no dispositivo automaticamente.

  Por padrão, esta opção está desativada.

  - **Baixar atualizações para**

    Esta pasta é usada para baixar atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft).

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento ainda que esta opção esteja desativada para ele no Utilitário de Diagnóstico Remoto do Kaspersky Security Center Linux. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede grava rastreamentos de acordo com as configurações do Utilitário de Diagnóstico Remoto do Kaspersky Security Center Linux. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

  - **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

    O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

Vá para a próxima etapa do assistente.

9. Especifique as configurações para reiniciar o sistema operacional:

   - **Não reiniciar o dispositivo**

     Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

   - **Reiniciar o dispositivo**

     Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

   - **Perguntar ao usuário o que fazer**

     O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

     Por padrão, esta opção está selecionada.

   - **Repetir aviso a cada (min)**

     Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

     Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

     Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

   - **Reiniciar após (min)**

     Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

     Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

   - **Tempo de espera antes do fechamento forçado de aplicativos nas sessões bloqueadas (min)**

     Os aplicativos são fechados no modo forçado quando o dispositivo for bloqueado (automaticamente, após um intervalo especificado de inatividade ou manualmente).

     Se esta opção estiver ativada, os aplicativos serão forçados a fechar no dispositivo bloqueado após a expiração do intervalo de tempo especificado no campo de entrada.

     Se essa opção estiver ativada, os aplicativos não serão fechados no dispositivo bloqueado.

     Por padrão, esta opção está desativada.

10. Na etapa **Concluir a criação da tarefa** do assistente, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** para modificar as configurações padrão da tarefa.

    Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois.

11. Clique no botão **Concluir**.

    O Assistente para novas tarefas cria a tarefa. Caso a opção **Abrir detalhes da tarefa quando a criação for concluída** tenha sido ativada, a janela de propriedades da tarefa abrirá automaticamente. Nesta janela, você pode especificar as configurações gerais da tarefa e, se necessário, alterar as configurações especificadas durante a criação da tarefa.

    > Você também pode abrir a respectiva janela de propriedades clicando no nome da tarefa criada na lista de tarefas.

    A tarefa é criada, configurada e exibida na lista de tarefas.

12. Para executar a tarefa, selecione-a na lista de tarefas e, então, clique no botão **Iniciar**.

    Você também pode definir um agendamento de início de tarefa na guia **Agendamento** da janela de propriedades da tarefa.

    Para obter uma descrição detalhada das configurações de início agendado, consulte as configurações gerais da tarefa.

Após a conclusão da tarefa, as atualizações necessárias são instaladas e as vulnerabilidades são corrigidas.

Se na rede da sua organização o servidor WSUS for utilizado (servidor WSUS local) e você quiser utilizá-lo junto com o Servidor de Administração, primeiro deverá assegurar-se de que o Servidor de Administração não seja utilizado como um servidor WSUS e, em seguida, fazer o seguinte:

a. Nos dispositivos gerenciados que executam o Windows, especifique o servidor WSUS local para o serviço Windows Update. É possível fazer isso manualmente no Registro do Windows ou utilizando uma política de grupo do Windows.

b. No servidor WSUS local, especifique as classificações necessárias para as atualizações e os aplicativos nos quais as atualizações devem ser distribuídas.

c. Sincronize o servidor WSUS com o servidor upstream (este pode ser um servidor Microsoft WSUS ou outro servidor WSUS upstream local).

Após a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ser executada no dispositivo, o Agente de Rede usará o serviço Windows Update para instalar as atualizações do Windows. O serviço Windows Update obtém o endereço do servidor WSUS externo do registro e baixa as atualizações diretamente desse servidor externo.

Adicionar regras para instalação da atualização

> Esse recurso está disponível apenas sob a licença do Gerenciamento de patches e vulnerabilidades.

Ao instalar atualizações de software ou corrigir vulnerabilidades de software usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é necessário especificar regras para a instalação da atualização. Essas regras determinam as atualizações a serem instaladas e as vulnerabilidades a serem corrigidas.

As configurações exatas dependem de você ter adicionado uma regra para todas as atualizações, para atualizações do Windows Update ou para atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software que não sejam a Kaspersky ou a Microsoft). Ao adicionar uma regra para atualizações do Windows Update ou atualizações de aplicativos de terceiros, é possível selecionar aplicativos e versões de aplicativo específicos para os quais deseja instalar atualizações. Ao adicionar uma regra para todas as atualizações, é possível selecionar atualizações específicas que deseja instalar e vulnerabilidades que deseja corrigir instalando as atualizações.

É possível adicionar uma regra para a instalação da atualização das seguintes maneiras:

- Adicionando uma regra ao criar uma nova tarefa do tipo *Instalar as atualizações necessárias e corrigir vulnerabilidades*.
- Adicionando uma regra na guia **Configurações do aplicativo** na janela de propriedades de uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.
- Por meio do assistente de instalação de atualização ou do assistente para correção de vulnerabilidades.

Adicionar regras para todas as atualizações

Para adicionar uma nova regra para todas as atualizações:

1. Clique em **Adicionar**.

   O Assistente de criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na etapa **Selecione o tipo de regra** do assistente, selecione **Regra para todas as atualizações**.

3. Na etapa **Critérios gerais** do assistente, especifique as seguintes configurações:

   - **Conjunto de atualizações a serem instaladas**

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - **Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que**

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

Por padrão, esta opção está desativada.

Vá para a próxima etapa do assistente.

4. Selecione as atualizações a serem instaladas:

- **Instalar todas as atualizações adequadas**

  Instale todas as atualizações de software que atendem aos critérios especificados na etapa **Critérios gerais** do assistente. Selecionado por padrão.

- **Instalar apenas as atualizações da lista**

  Instale somente as atualizações de software que você seleciona manualmente da lista. Essa lista contém todas as atualizações de software disponíveis.

  Por exemplo, pode ser necessário selecionar atualizações específicas nos seguintes casos: para verificar a instalação em um ambiente de teste, para atualizar somente aplicativos críticos ou para atualizar somente aplicativos específicos.

  - **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

    Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

    Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

    Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

    Por padrão, esta opção está ativada.

Vá para a próxima etapa do assistente.

5. Selecione as vulnerabilidades que serão corrigidas instalando as atualizações selecionadas:

- **Corrigir todas as vulnerabilidades que correspondem a outros critérios**

  Corrija todas as vulnerabilidades que atendem aos critérios especificados na etapa **Critérios gerais** do assistente. Selecionado por padrão.

- **Corrigir somente vulnerabilidades da lista**

  Corrija somente as vulnerabilidades que você seleciona manualmente da lista. Essa lista contém todas as vulnerabilidades detectadas.

  Por exemplo, pode ser necessário selecionar vulnerabilidades específicas nos seguintes casos: para verificar a correção em um ambiente de teste, para corrigir vulnerabilidades somente em aplicativos críticos ou para corrigir vulnerabilidades somente em aplicativos específicos.

Vá para a próxima etapa do assistente.

6. Especifique o nome da regra que você está adicionando. É possível mudar esse nome mais tarde na guia **Configurações do aplicativo** da janela de propriedades da tarefa criada.

A nova regra é criada, configurada e exibida na tabela de regras do Assistente para novas tarefas.

Adicionar regras para atualizações do Windows Update

Para adicionar uma nova regra para atualizações do Windows Update:

1. Clique em **Adicionar**.

   O Assistente de criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Selecione **Regra para o Windows Update**.

   Vá para a próxima etapa do assistente.

3. Na etapa **Critérios gerais** do assistente, especifique as seguintes configurações:

   - **Conjunto de atualizações a serem instaladas**

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - **Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que**

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

   - **Corrigir vulnerabilidades com um nível de gravidade do MSRC igual ou maior do que**

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Categorias de atualizações**, selecione as categorias das atualizações a serem instaladas. Essas categorias são iguais às no Catálogo do Microsoft Update. Por padrão, todas as categorias estão selecionadas.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Adicionar regras para atualizações de aplicativos de terceiros

Para adicionar uma nova regra para as atualizações de aplicativos de terceiros:

1. Clique em **Adicionar**.

   O Assistente de criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na etapa **Selecione o tipo de regra** do assistente, selecione **Regra para atualizações de terceiros**.

3. Na etapa **Critérios gerais** do assistente, especifique as seguintes configurações:

   - **Conjunto de atualizações a serem instaladas**

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - **Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que**

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

   Vá para a próxima etapa do assistente.

4. Selecione os aplicativos e as versões dos aplicativos para os quais você deseja instalar atualizações.

   Por padrão, todas os aplicativos estão selecionados.

Vá para a próxima etapa do assistente.

5. Especifique o nome da regra que você está adicionando. É possível mudar esse nome mais tarde na guia **Configurações do aplicativo** da janela de propriedades da tarefa criada.

A nova regra é criada, configurada e exibida na tabela de regras do Assistente para novas tarefas.

Configurações da tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades especificadas após a criação da tarefa

Após a criação da tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é possível especificar as seguintes configurações na guia **Configurações do aplicativo** da janela de propriedades da tarefa:

- Na seção **Testar instalação**:
  - **Não verificar**. Selecione esta opção se você não quiser efetuar uma instalação de teste de atualizações.
  - **Executar verificação nos dispositivos selecionados**. Selecione esta opção se você quiser testar a instalação de atualizações nos dispositivos selecionados. Clique no botão **Adicionar** e, em seguida, selecione os dispositivos nos quais deseja executar uma instalação de teste das atualizações.
  - **Executar verificação nos dispositivos no grupo especificado**. Selecione esta opção se você quiser testar a instalação de atualizações em um grupo de dispositivos. No campo **Especifique um grupo de teste**, especifique um grupo de dispositivos nos quais você deseja executar uma instalação de teste.
  - **Executar verificação no percentual de dispositivos especificado**. Selecione esta opção se você quiser testar a instalação de atualizações em uma porcentagem de dispositivos. No campo **Porcentagem de dispositivos de teste de todos os dispositivos de destino**, especifique a porcentagem de dispositivos nos quais você deseja executar uma instalação de teste de atualizações.

  Após selecionar qualquer outra opção além de **Não verificar**, no campo **Tempo para decidir se a instalação deve continuar, em horas**, especifique o número de horas que deve decorrer desde o teste da instalação das atualizações até o início da instalação das atualizações em todos os dispositivos.
- Na seção **Atualizações para instalar** você pode exibir a lista de atualizações instaladas pela tarefa. Somente as atualizações que correspondem com as configurações da tarefa aplicada são exibidas.

Para obter uma descrição completa das configurações de tarefa, consulte as configurações gerais da tarefa.

Atualizar aplicativos de terceiros automaticamente

Alguns aplicativos de terceiros podem ser atualizados automaticamente. O fornecedor do aplicativo define se o aplicativo é compatível com o recurso de atualização automática. Se um aplicativo de terceiros instalado em um dispositivo gerenciado for compatível com atualização automática, você poderá especificar a configuração de atualização automática nas propriedades do aplicativo. Depois de alterar a configuração de atualização automática, os Agentes de Rede aplicam a nova configuração a cada dispositivo gerenciado no qual o aplicativo está instalado.

A configuração de atualização automática é independente dos outros objetos e configurações do recurso Gerenciamento de patches e vulnerabilidades. Por exemplo, esta configuração não depende de um status de aprovação de atualização ou das tarefas de instalação da atualização, como *Instalar as atualizações necessárias e corrigir vulnerabilidades* e *Corrigir vulnerabilidades*.

Para definir a configuração de atualização automática para um aplicativo de terceiros:

1. Na janela principal do aplicativo, acesse a seção **Gerenciamento de software → Aplicativos de terceiros → Registro de aplicativos**.
2. Clique no nome do aplicativo para o qual deseja alterar a configuração de atualização automática.

   Para simplificar a pesquisa, você pode filtrar a lista pelas colunas **Status das atualizações automáticas** e **Gerenciar atualizações automáticas**.

   A janela Propriedades do aplicativo é aberta.
3. Na seção **Geral**, selecione um valor para o seguinte recurso:

   Status das atualizações automáticas

   Escolha uma das seguintes opções:

   - **Indefinido**

     O recurso de atualização automática será desativado. O Kaspersky Security Center Linux instala atualizações de aplicativos de terceiros usando as tarefas: *Instalar as atualizações necessárias e corrigir vulnerabilidades* e *Corrigir vulnerabilidades*.
   - **Permitido**

     Depois que o fornecedor lança uma atualização para o aplicativo, esta atualização é instalada nos dispositivos gerenciados automaticamente. Nenhuma outra ação é necessária.
   - **Bloqueado**

     As atualizações do aplicativo não são instaladas automaticamente. O Kaspersky Security Center Linux instala atualizações de aplicativos de terceiros usando as tarefas: *Instalar as atualizações necessárias e corrigir vulnerabilidades* e *Corrigir vulnerabilidades*.
4. Clique em **Salvar** para salvar as alterações.

A configuração de atualização automática é aplicada ao aplicativo selecionado.

Corrigindo vulnerabilidades de software de terceiros

Esta seção descreve os recursos do Kaspersky Security Center Linux relacionados à correção de vulnerabilidades no software instalado nos dispositivos gerenciados.

Sobre como encontrar e corrigir vulnerabilidades de software

O Kaspersky Security Center Linux detecta e corrige vulnerabilidades de software em dispositivos gerenciados que executam os sistemas operacionais Microsoft Windows. As vulnerabilidades são detectadas no sistema operacional e no software de terceiros, incluindo o software da Microsoft.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Localizar vulnerabilidades de software

Para encontrar vulnerabilidades de software, o Kaspersky Security Center Linux usa características do banco de dados de vulnerabilidades conhecidas. Esse banco de dados foi criado e é mantido atualizado por especialistas da Kaspersky. Ele contém informações sobre vulnerabilidades, como descrição da vulnerabilidade, data de detecção da vulnerabilidade e nível de gravidade da vulnerabilidade. Você pode encontrar os detalhes das vulnerabilidades de software no site da Kaspersky.

O Kaspersky Security Center Linux usa a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para encontrar vulnerabilidades de software.

Corrigir vulnerabilidades de software

Para corrigir vulnerabilidades de software, o Kaspersky Security Center Linux usa atualizações de software emitidas pelos fornecedores do software. Os metadados das atualizações de software são baixados para o repositório do Servidor de Administração como resultado da execução da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Essa tarefa tem como objetivo fazer o download de metadados para atualizações de software da Kaspersky e de terceiros. Essa tarefa é criada automaticamente pelo assistente de início rápido do Kaspersky Security Center Linux. Você pode criar a tarefa *Baixar atualizações no repositório do Servidor de Administração* manualmente.

As atualizações de software para corrigir vulnerabilidades podem ser representadas como pacotes ou patches de distribuição completos. As atualizações de software que corrigem vulnerabilidades de software são denominadas *correções*. As *correções recomendadas* são aquelas recomendadas para instalação pelos especialistas da Kaspersky. *Correções do usuário* são aquelas especificadas manualmente para instalação pelos usuários. Para instalar uma correção do usuário, você deve criar um pacote de instalação contendo essa correção.

Se você possui a licença do Kaspersky Security Center Linux com o recurso Gerenciamento de patches e vulnerabilidades, você pode usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Essa tarefa corrige automaticamente várias vulnerabilidades instalando as correções recomendadas. Para esta tarefa, você pode configurar manualmente certas regras para corrigir várias vulnerabilidades.

Se você não possui a licença do Kaspersky Security Center Linux com o recurso Gerenciamento de patches e vulnerabilidades, pode usar a tarefa *Corrigir vulnerabilidades*. Usando essa tarefa, você pode corrigir vulnerabilidades instalando as correções recomendadas para o software da Microsoft e as correções do usuário para outros softwares de terceiros.

Por motivos de segurança, todas as atualizações de softwares de terceiros instaladas usando o recurso Gerenciamento de patches e vulnerabilidades são verificadas automaticamente pelas tecnologias da Kaspersky em busca de malwares. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Para corrigir algumas vulnerabilidades de software, é necessário aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software, se o aceite do EULA for solicitado. Se você recusar o EULA, a vulnerabilidade do software não será corrigida.

Cenário: Encontrar e corrigir vulnerabilidades de software de terceiros

Esta seção fornece um cenário para localizar e corrigir vulnerabilidades nos dispositivos gerenciados que executam o Windows. Você pode detectar e corrigir vulnerabilidades no sistema operacional e em software de terceiros, incluindo software da Microsoft.

Pré-requisitos

- O Kaspersky Security Center Linux está implementado em sua organização.
- Há dispositivos gerenciados executando o Windows na sua organização.
- Uma conexão com a Internet é necessária para que o Servidor de Administração execute as seguintes tarefas:
  - Para fazer uma lista de correções recomendadas para vulnerabilidades em softwares da Microsoft. A lista é criada e atualizada regularmente por especialistas da Kaspersky.
  - Para corrigir vulnerabilidades em software de terceiros que não sejam software da Microsoft.

Fases

A localização e a correção de vulnerabilidades de software ocorre em fases:

1. **Verificar vulnerabilidades no software instalado nos dispositivos gerenciados**

   Para encontrar vulnerabilidades no software instalado nos dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa é concluída, o Kaspersky Security Center Linux recebe uma lista de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

   A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo assistente de início rápido do Kaspersky Security Center Linux. Se você não tiver executado o assistente, inicie-o agora ou crie a tarefa manualmente.

Você pode criar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* somente para dispositivos Windows. Você não pode criar esta tarefa para dispositivos em execução em outros sistemas operacionais.

2 Visualizar a lista de vulnerabilidades de software detectadas

Visualize a lista **Vulnerabilidades de software** e decida quais vulnerabilidades devem ser corrigidas. Para visualizar informações detalhadas sobre cada vulnerabilidade, clique no nome da vulnerabilidade na lista. Para cada vulnerabilidade na lista, você também pode visualizar as estatísticas sobre a vulnerabilidade nos dispositivos gerenciados.

3 Configurar a correção de vulnerabilidades

Quando vulnerabilidades de software são detectadas, é possível corrigi-las nos dispositivos gerenciados usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa permite instalar várias atualizações e corrigir várias vulnerabilidades, de acordo com determinadas regras. Observe que esta tarefa pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades. Para corrigir vulnerabilidades de software, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* usa as atualizações de software recomendadas.

A tarefa *Corrigir vulnerabilidades* não requer a opção de licença para o recurso Gerenciamento de patches e vulnerabilidades. Para usar essa tarefa, você deve especificar manualmente as correções para vulnerabilidades em softwares de terceiros definidas pelo usuário listadas nas configurações da tarefa. A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para softwares de terceiros.

Você pode criar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* e a tarefa *Corrigir vulnerabilidades* somente para dispositivos Windows. Você não pode criar essas tarefas para dispositivos em execução em outros sistemas operacionais.

É possível iniciar o assistente para correção de vulnerabilidades, que cria uma dessas tarefas automaticamente ou criá-las manualmente.

Se você criou e configurou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, as vulnerabilidades são corrigidas nos dispositivos gerenciados automaticamente. Quando a tarefa é iniciada, ela correlaciona a lista de atualizações de software disponíveis com as regras especificadas nas configurações da tarefa. Todas as atualizações de software que atendem aos critérios das regras especificadas são baixadas no repositório do Servidor de Administração e instaladas para correção de vulnerabilidades de software.

Se você criou a tarefa *Corrigir vulnerabilidades*, apenas as vulnerabilidades no software da Microsoft são corrigidas.

4 Agendar as tarefas

Agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para ser executada automaticamente e periodicamente para manter a lista de vulnerabilidades atualizada. A frequência recomendada é de uma vez por semana.

Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência. Ao agendar a tarefa *Corrigir vulnerabilidades*, é necessário selecionar correções para o software da Microsoft ou especificar correções de usuário para o software de terceiros sempre que iniciar a tarefa.

Ao agendar as tarefas, certifique-se que uma tarefa criada para corrigir vulnerabilidades é iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

5. **Ignorar vulnerabilidades de software (opcional)**

   Você pode ignorar certas vulnerabilidades de software em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

6. **Executando uma tarefa de correção de vulnerabilidades**

   Inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*. Quando a tarefa estiver concluída, certifique-se que possui o status *Conclusão com êxito* na lista de tarefas.

7. **Criar o relatório sobre os resultados da correção de vulnerabilidades de software (opcional)**

   Para visualizar estatísticas detalhadas sobre as vulnerabilidades corrigidas, gere o Relatório de vulnerabilidades. Esse relatório exibe informações sobre vulnerabilidades de software que não são corrigidas. Ele permite identificar e solucionar vulnerabilidades em softwares de terceiros, incluindo softwares da Microsoft, que são usados em sua organização.

8. **Verificar a configuração para encontrar e corrigir vulnerabilidades em software de terceiros**

   Certifique-se de ter feito o seguinte:

   - Obtenção e revisão da lista de vulnerabilidades de software detectadas nos dispositivos gerenciados.
   - Você pode ignorar certas vulnerabilidades de software, se desejado.
   - A tarefa para Corrigir vulnerabilidades está configurada.
   - As tarefas para localizar e corrigir vulnerabilidades de software estão agendadas para que sejam iniciadas sequencialmente.
   - Verificar se a tarefa para correção de vulnerabilidades de software foi iniciada.

Corrigindo vulnerabilidades de software de terceiros

Para localizar vulnerabilidades de software de terceiros, você pode criar e executar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* e receber uma lista de vulnerabilidades de software. Depois de obter a lista de vulnerabilidades de software, você pode corrigir as vulnerabilidades nos dispositivos gerenciados que executam o Windows.

É possível corrigir vulnerabilidades de software no sistema operacional e em softwares de terceiros, incluindo softwares da Microsoft, criando e executando a tarefa Corrigir vulnerabilidades ou a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades.

> Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Como opção, é possível criar uma tarefa para corrigir vulnerabilidades de software das seguintes maneiras:

- Abrindo a lista de vulnerabilidades e especificando quais vulnerabilidades corrigir.

  Como resultado, é criada uma nova tarefa para corrigir vulnerabilidades de software. Como opção, você pode adicionar as vulnerabilidades selecionadas a uma tarefa existente.

- Executando o assistente para correção de vulnerabilidades.

O Assistente para correção de vulnerabilidades só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

O assistente simplifica a criação e a configuração de uma tarefa Correção de vulnerabilidades e permite eliminar a criação de tarefas redundantes.

Corrigindo vulnerabilidades de software usando a lista de vulnerabilidades

Para corrigir vulnerabilidades de software usando a lista de vulnerabilidades:

1. Abra a lista de vulnerabilidades executando uma das seguintes ações:

   - No menu principal, vá para **Gerenciamento de software** → **Gerenciamento de patches** → **Vulnerabilidades de software**.
   - No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados** → <nome do dispositivo> → **Avançado** → **Vulnerabilidades de software**.
   - Na janela principal do aplicativo, vá para **Gerenciamento de software** → **Aplicativos de terceiros** → **Registro de aplicativos** → <nome do aplicativo> → **Vulnerabilidades**.

   Uma tabela com a lista de vulnerabilidades em softwares de terceiros instalados em dispositivos gerenciados é exibida.

2. Na lista de vulnerabilidades, marque as caixas de seleção ao lado das vulnerabilidades que deseja corrigir e clique no botão **Corrigir vulnerabilidade**.

   Se a atualização de software recomendada para corrigir uma das vulnerabilidades selecionadas estiver ausente, uma mensagem informativa será exibida.

   Para corrigir algumas vulnerabilidades de software, é necessário aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software, se o aceite do EULA for solicitado. Se você recusar o EULA, a vulnerabilidade do software não será corrigida.

3. Escolha uma das seguintes opções:

   - **Nova tarefa**

     O Assistente para novas tarefas inicia. Se você tiver a licença do Gerenciamento de patches e vulnerabilidades, a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades será pré-selecionada. Se você não tiver a licença, a tarefa Corrigir vulnerabilidades será pré-selecionada. Seguem abaixo as etapas do assistente para concluir a criação da tarefa.

   - **Corrigir vulnerabilidade (adicionar a regra à tarefa especificada)**

     Selecione uma tarefa à qual deseja adicionar as vulnerabilidades selecionadas. Se você tiver a licença de Gerenciamento de patches e vulnerabilidades, selecione a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades. Uma nova regra para corrigir as vulnerabilidades selecionadas será adicionada automaticamente à tarefa escolhida. Se você não tiver a licença, selecione a tarefa Corrigir vulnerabilidades. As vulnerabilidades selecionadas são adicionadas às propriedades da tarefa.

A janela de propriedades da tarefa é aberta. Clique em **Salvar** para salvar as alterações.

Se você escolheu criar uma nova tarefa, ela será criada e exibida na lista de tarefas em **Tarefas**. Se você optou por adicionar as vulnerabilidades a uma tarefa existente, as vulnerabilidades serão salvas nas propriedades da tarefa.

Para corrigir as vulnerabilidades de software de terceiros, inicie a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades ou a tarefa Corrigir vulnerabilidades. Se você criou a tarefa Corrigir vulnerabilidades, deve especificar manualmente as atualizações de software listadas nas configurações da tarefa.

Corrigir vulnerabilidades de software usando o assistente para correção de vulnerabilidades

O Assistente para correção de vulnerabilidades só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

Para corrigir vulnerabilidades de software usando o assistente para correção de vulnerabilidades:

1. No menu principal, vá para **Gerenciamento de software → Gerenciamento de patches → Vulnerabilidades de software**.

   É exibida uma tabela com uma lista de vulnerabilidades no software de terceiros instalado nos dispositivos gerenciados.

2. Marque a caixa de seleção ao lado da vulnerabilidade que deseja corrigir.

3. Clique no botão **Executar o assistente para correção de vulnerabilidades**.

   O botão é desativado se você selecionar mais de uma vulnerabilidade.

   O assistente para correção de vulnerabilidades é iniciado. A lista de tarefas existentes é exibida. Essa lista pode conter os seguintes tipos de tarefas:

   - Instalar as atualizações necessárias e corrigir vulnerabilidades
   - Corrigir vulnerabilidades

   Você não pode modificar a tarefa Corrigir vulnerabilidades para instalar novas atualizações. Para instalar novas atualizações, você só pode usar a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades.

4. Se desejar que o assistente exiba apenas as tarefas que corrigem a vulnerabilidade selecionada, ative a opção **Mostrar apenas tarefas que corrigem esta vulnerabilidade**.

5. Execute uma das seguintes ações:

   - Para iniciar uma tarefa, marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Iniciar**.

     Nenhuma outra ação será necessária. Você pode fechar o assistente. A tarefa será concluída no modo de segundo plano.

- Para adicionar uma nova regra para instalação da atualização a uma tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades existente:

  a. Marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Adicionar regra**.

  > O botão **Adicionar regra** é desativado se você selecionar mais de uma tarefa.

  Você não pode adicionar uma regra para uma tarefa Corrigir vulnerabilidades. Se você selecionar uma tarefa Corrigir vulnerabilidades, a seguinte notificação é exibida: "Para instalar atualizações, use a tarefa "Instalar as atualizações necessárias e corrigir vulnerabilidades.""

  b. Na página aberta, configure a nova regra:

  - **Regra para corrigir vulnerabilidades deste nível de gravidade**

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

    Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

    Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

    Por padrão, esta opção está desativada.

  - **Regra para correção de vulnerabilidades por meio de atualizações do mesmo tipo da atualização definida como recomendada para a vulnerabilidade selecionada**

    Essa regra é exibida somente para vulnerabilidades de software Microsoft.

  - **Regra para corrigir vulnerabilidades em aplicativos por fornecedor selecionado**

    Esta regra é exibida somente para vulnerabilidades de software de terceiros.

  - **Regra para corrigir uma vulnerabilidade em todas as versões do aplicativo selecionado**

    Esta regra é exibida somente para vulnerabilidades de software de terceiros.

  - **Regra para corrigir a vulnerabilidade selecionada**

  - **Aprovar as atualizações que corrigem esta vulnerabilidade**

    A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

    Por padrão, esta opção está desativada.

  c. Clique em **Adicionar**.

  A janela de propriedades da tarefa é aberta. A nova regra já foi adicionada às propriedades da tarefa. Você pode visualizar ou modificar a regra ou outras configurações de tarefa. Clique em **Salvar** para salvar as alterações.

- Para criar uma tarefa:

  a. Clique no botão **Nova tarefa**.

  b. Na página aberta, configure a nova regra:

  - **Regra para corrigir vulnerabilidades deste nível de gravidade**

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

    Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

    Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

    Por padrão, esta opção está desativada.

  - **Regra para correção de vulnerabilidades por meio de atualizações do mesmo tipo da atualização definida como recomendada para a vulnerabilidade selecionada**

    Essa regra é exibida somente para vulnerabilidades de software Microsoft.

  - **Regra para corrigir vulnerabilidades em aplicativos por fornecedor selecionado**

    Esta regra é exibida somente para vulnerabilidades de software de terceiros.

  - **Regra para corrigir uma vulnerabilidade em todas as versões do aplicativo selecionado**

    Esta regra é exibida somente para vulnerabilidades de software de terceiros.

  - **Regra para corrigir a vulnerabilidade selecionada**

  - **Aprovar as atualizações que corrigem esta vulnerabilidade**

    A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

    Por padrão, esta opção está desativada.

  c. Clique em **Adicionar**.

  d. Continue a criar a tarefa no Assistente para novas tarefas.

  A nova regra adicionada no Assistente para correção de vulnerabilidades é exibida na etapa **Especifique regras para a instalação de atualizações** do Assistente para novas tarefas. Ao concluir o assistente, a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades será adicionada na lista de tarefas.

Criar a tarefa Corrigir vulnerabilidades

A tarefa *Corrigir vulnerabilidades* permite corrigir vulnerabilidades de software em dispositivos gerenciados. É possível corrigir vulnerabilidades de software em softwares de terceiros, incluindo softwares da Microsoft.

Você pode criar a tarefa *Corrigir vulnerabilidades* somente para dispositivos Windows. Você não pode criar esta tarefa para dispositivos em execução em outros sistemas operacionais.

Você poderá criar uma nova tarefa *Corrigir vulnerabilidades* somente se não tiver a licença de Gerenciamento de patches e vulnerabilidades.

Para corrigir novas vulnerabilidades, adicione-as a uma tarefa *Corrigir vulnerabilidades* existente. Contudo, recomendamos usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* em vez da tarefa *Corrigir vulnerabilidades*. A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* permite instalar várias atualizações e corrigir várias vulnerabilidades automaticamente, de acordo com as regras definidas por você.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Para criar uma tarefa Corrigir vulnerabilidades:

1. No menu principal, vá para **Tarefas**.

   Como alternativa, você pode criar essa tarefa na janela de propriedades do dispositivo na guia **Tarefas**.

2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na lista suspensa **Aplicativo**, selecione Kaspersky Security Center.

4. Na lista **Tipo de tarefa**, selecione o tipo de tarefa **Corrigir vulnerabilidades**.

5. No campo **Nome da tarefa**, especifique o nome da nova tarefa.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).

6. Selecione os dispositivos aos quais a tarefa será atribuída.

   Vá para a próxima etapa do assistente.

7. Clique em **Adicionar**.

   A lista de vulnerabilidades é aberta.

8. Na lista de vulnerabilidades, marque as caixas de seleção ao lado das vulnerabilidades que deseja corrigir e clique no botão **OK**.

   As vulnerabilidades de software da Microsoft geralmente têm correções recomendadas. Nenhuma ação adicional é necessária para elas.

Para vulnerabilidades em softwares de outros fornecedores, primeiro é necessário especificar uma correção do usuário para cada vulnerabilidade que deseja corrigir. Depois disso, será possível adicionar essas vulnerabilidades à tarefa *Corrigir vulnerabilidades*.

Vá para a próxima etapa do assistente.

9. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

  A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

  Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

  Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

  Por padrão, esta opção está desativada.

Vá para a próxima etapa do assistente.

10. Especificar as configurações da conta:

    - **Conta padrão**

      A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

      Por padrão, esta opção está selecionada.

    - **Especificar conta**

      Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

    - **Conta**

      Conta sob a qual a tarefa é executada.

    - **Senha**

      Senha da conta sob a qual a tarefa será executada.

11. Na etapa **Concluir a criação da tarefa** do assistente, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** para modificar as configurações padrão da tarefa.

    Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois.

12. Clique no botão **Concluir**.

    O assistente cria a tarefa. Caso a opção **Abrir detalhes da tarefa quando a criação for concluída** tenha sido ativada, a janela de propriedades da tarefa abrirá automaticamente. Nesta janela, você pode especificar as configurações gerais da tarefa e, se necessário, alterar as configurações especificadas durante a criação da tarefa.

    > Você também pode abrir a respectiva janela de propriedades clicando no nome da tarefa criada na lista de tarefas.

    A tarefa é criada, configurada e exibida na lista de tarefas em **Tarefas**.

13. Para executar a tarefa, selecione-a na lista de tarefas e, então, clique no botão **Iniciar**.

    Você também pode definir um agendamento de início de tarefa na guia **Agendamento** da janela de propriedades da tarefa.

    Para obter uma descrição detalhada das configurações de início agendado, consulte as configurações gerais da tarefa.

Após a conclusão da tarefa, as vulnerabilidades selecionadas são corrigidas.

Selecionar as correções do usuário para vulnerabilidades em software de terceiros

Para usar a tarefa *Corrigir vulnerabilidades*, você deve especificar manualmente as atualizações de software para corrigir as vulnerabilidades em softwares de terceiros listadas nas configurações da tarefa. A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para outros softwares de terceiros.

As *correções do usuário* são atualizações de software que o administrador especifica manualmente para instalação para corrigir vulnerabilidades.

Para selecionar correções do usuário para vulnerabilidades em software de terceiros:

1. No menu principal, vá para **Gerenciamento de software → Gerenciamento de patches → Vulnerabilidades de software**.

   Uma tabela com a lista de vulnerabilidades em softwares de terceiros instalados em dispositivos gerenciados é exibida.

2. Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade de software para o qual você deseja especificar uma correção do usuário.

   A janela de propriedades da vulnerabilidade selecionada é aberta.

3. No painel esquerdo, selecione a seção **Correções do usuário e outras correções**.

   A lista de correções do usuário para a vulnerabilidade de software selecionada é exibida.

4. Clique em **Adicionar**.

   A lista de pacotes de instalação disponíveis é exibida. A lista de pacotes de instalação exibidos corresponde à lista na pasta **Gerenciamento de software → Pacotes de instalação**.

   Se você não criou um pacote de instalação contendo a correção do usuário para a vulnerabilidade selecionada, poderá criar o pacote agora clicando no botão **Novo** e avançando pelo Assistente de novo pacote.

5. Selecione um pacote de instalação (ou pacotes) que contenha uma correção (ou correções) do usuário para a vulnerabilidade selecionada.

6. Clique no botão **Salvar**.

Os pacotes de instalação que contenham correções do usuário para a vulnerabilidade de software são especificados. Ao iniciar a tarefa *Corrigir vulnerabilidades*, o pacote de instalação é instalado e a vulnerabilidade de software é corrigida.

Visualizar informações sobre vulnerabilidades de software detectadas em todos os dispositivos gerenciados

Depois de verificar o software em dispositivos gerenciados quanto a vulnerabilidades, você pode visualizar a lista de vulnerabilidades de software detectadas. Se você executar a tarefa para a hierarquia de Servidores de Administração, poderá visualizar a lista de dispositivos gerenciados com vulnerabilidades detectadas somente para o Servidor de Administração selecionado.

Você também pode gerar e visualizar um Relatório de vulnerabilidades.

Para exibir a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados,

No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Vulnerabilidades de software**.

A lista de vulnerabilidades de software detectadas nos dispositivos clientes é exibida.

Para ajustar a lista de vulnerabilidades de software:

Clique no ícone de **Filtro** () no canto superior direito da lista de vulnerabilidades de software e selecione os filtros necessários. Você também pode selecionar um dos filtros predefinidos na lista suspensa **Filtros predefinidos**, acima da lista de vulnerabilidades de software.

Você pode obter informações detalhadas sobre qualquer vulnerabilidade na lista.

Para obter informações sobre uma vulnerabilidade de software:

Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade.

A janela de propriedades da vulnerabilidade de software é aberta.

Visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado

Você pode visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado que executa o Windows.

Para visualizar a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo para o qual você deseja visualizar as vulnerabilidades de software detectadas.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Na janela de propriedades do dispositivo selecionado, selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Vulnerabilidades de software**.

A lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado é exibida.

Para visualizar as propriedades da vulnerabilidade de software selecionada,

Clique no link com o nome da vulnerabilidade de software na lista de vulnerabilidades de software.

A janela de propriedades de vulnerabilidade de software selecionada é exibida.

Visualizar as estatísticas de vulnerabilidades em dispositivos gerenciados

Você pode visualizar estatísticas para cada vulnerabilidade de software em dispositivos gerenciados. As estatísticas são representadas como um diagrama. O diagrama exibe o número de dispositivos com os seguintes status:

- *Ignorado em: <número de dispositivos>*. O status será atribuído se, nas propriedades da vulnerabilidade, o usuário tiver definido manualmente a opção para ignorá-la.
- *Corrigido em: <número de dispositivos>*. O status será atribuído se a tarefa para correção de vulnerabilidade for concluída com êxito.
- *Correção agendada em: <número de dispositivos>*. O status será atribuído se o usuário tiver criado a tarefa para correção de vulnerabilidades, mas a tarefa ainda não tiver sido executada.
- *Correção aplicada em: <número de dispositivos>*. O status será atribuído se o usuário tiver selecionado manualmente uma atualização de software para correção de vulnerabilidades, mas essa atualização de software não tiver corrigido a vulnerabilidade.
- *Correção necessária em: <número de dispositivos>*. Esse status é atribuído se a vulnerabilidade tiver sido corrigida somente em alguns dispositivos gerenciados e precisar ser corrigida em mais dispositivos gerenciados.

Para exibir as estatísticas de uma vulnerabilidade nos dispositivos gerenciados:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   A página exibe uma lista de vulnerabilidades para os aplicativos detectados nos dispositivos gerenciados.

2. Selecione a caixa de seleção ao lado de uma vulnerabilidade.
3. Clique no botão **Estatísticas de vulnerabilidades em dispositivos**.

   > O botão **Estatísticas de vulnerabilidades em dispositivos** é desativado se você selecionar mais de uma vulnerabilidade.

O diagrama dos status de vulnerabilidade é exibido. Clicar em um status abre uma lista de dispositivos nos quais a vulnerabilidade tem o status selecionado.

Exportar a lista de vulnerabilidades de software para um arquivo

Você pode baixar a lista de vulnerabilidades exibidas como um arquivo CSV ou TXT. Você pode enviar esses arquivos ao seu gerente de segurança da informação ou armazená-los para fins estatísticos.

Para exportar a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados para um arquivo de texto:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

Uma lista de vulnerabilidades de software nos aplicativos detectados em dispositivos gerenciados é exibida.

Por padrão, somente as vulnerabilidades exibidas na página atual são exportadas.

Se você quiser exportar apenas vulnerabilidades específicas, marque as caixas de seleção ao lado dessas vulnerabilidades.

2. Clique no botão **Exportar para TXT** ou **Exportar para CSV**, dependendo do formato preferido. Se algum desses botões não estiver visível, clique no botão de reticências e selecione a opção necessária na lista suspensa.

Um arquivo contendo a lista de vulnerabilidades de software é baixado em seu dispositivo.

Para visualizar a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo para o qual você deseja visualizar as vulnerabilidades de software detectadas.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Na janela de propriedades do dispositivo selecionado, selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Vulnerabilidades de software**.

A lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado é exibida.

Por padrão, somente as vulnerabilidades exibidas na página atual são exportadas.

Se você quiser exportar apenas vulnerabilidades específicas, marque as caixas de seleção ao lado dessas vulnerabilidades.

1. Clique no botão **Exportar para TXT** ou **Exportar para CSV**, dependendo do formato preferido. Se algum desses botões não estiver visível, clique no botão de reticências e selecione a opção necessária na lista suspensa.

Um arquivo contendo a lista de vulnerabilidades de software é baixado em seu dispositivo.

Ignorar as vulnerabilidades de software

Você pode ignorar as vulnerabilidades do software a ser corrigidas. Os motivos para ignorar vulnerabilidades de software, por exemplo, os seguintes:

- A vulnerabilidade de software não é considerada crítica para sua organização.
- Você entende que a correção de vulnerabilidade do software pode danificar os dados relacionados ao software que exigia a correção da vulnerabilidade.
- Você tem certeza de que a vulnerabilidade do software não é perigosa para a rede da sua organização porque usa outras medidas para proteger seus dispositivos gerenciados.

Você pode ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

Para ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   Uma lista de vulnerabilidades de software nos aplicativos detectados em dispositivos gerenciados é exibida.

2. Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade de software que você deseja ignorar.

   A janela de propriedades da vulnerabilidade de software é aberta.

3. Na guia **Geral**, ative a opção **Ignorar vulnerabilidade**.

4. Clique no botão **Salvar**.

   A janela de propriedades de vulnerabilidade do software está fechada.

A vulnerabilidade de software é ignorada em todos os dispositivos gerenciados.

Para ignorar uma vulnerabilidade de software em um dispositivo gerenciado selecionado:

1. No menu principal, vá para **Gerenciamento de ativos → Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo no qual você deseja ignorar uma vulnerabilidade de software.

   A janela Propriedades do dispositivo é aberta.

3. Na janela Propriedades do dispositivo, selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Vulnerabilidades de software**.

   A lista de vulnerabilidades de software detectadas no dispositivo é exibida.

5. Na lista de vulnerabilidades de software, selecione a vulnerabilidade que você deseja ignorar no dispositivo selecionado.

   A janela de propriedades da vulnerabilidade de software é aberta.

6. Na janela de propriedades da vulnerabilidade de software, na guia **Geral**, ative a opção **Ignorar vulnerabilidade**.

7. Clique no botão **Salvar**.

   A janela de propriedades de vulnerabilidade do software está fechada.

8. Feche a janela Propriedades do dispositivo.

A vulnerabilidade de software é ignorada no dispositivo selecionado.

A vulnerabilidade de software ignorada não será corrigida após a conclusão das tarefas *Corrigir vulnerabilidades* ou *Instalar as atualizações necessárias e corrigir vulnerabilidades*. É possível excluir as vulnerabilidades de software ignoradas na lista de vulnerabilidades por meio do filtro.

Criação de um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky

O Kaspersky Security Center Web Console permite executar a instalação remota de aplicativos de terceiros usando pacotes de instalação. Esses aplicativos de terceiros são incluídos em um banco de dados dedicado da Kaspersky. O banco de dados da Kaspersky é criado automaticamente quando a tarefa *Baixar atualizações no repositório do Servidor de Administração* for executada pela primeira vez.

Você pode criar um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky somente se tiver uma licença de gerenciamento de patches e vulnerabilidades.

Para criar um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky:

1. No menu principal, vá para a seção **Gerenciamento de software → Pacotes de instalação**.
2. Clique em **Adicionar**.

   O Assistente de novo pacote inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Selecione a opção **Selecione um aplicativo no banco de dados da Kaspersky para criar um pacote de instalação**.

   Esta opção está disponível apenas sob a licença de Gerenciamento de patches e vulnerabilidades.

   Vá para a próxima etapa do assistente.
4. Selecione o aplicativo para o qual você deseja criar um pacote de instalação.

   Vá para a próxima etapa do assistente.
5. Selecione o idioma de localização relevante na lista suspensa e clique em Avançar.

   Esta etapa só será exibida se o aplicativo oferecer várias opções de idioma.
6. Se você for solicitado a aceitar um Contrato de Licença para a instalação, na etapa **Contratos de Licença e Políticas de Privacidade** do assistente, faça o seguinte:

   a. Clique no link **Mostrar** para ler o Contrato de Licença no site do fornecedor ou visualizar as atualizações com a licença.

   b. Marque a caixa de seleção **Confirmo que li, entendi e aceito totalmente os termos e condições deste Contrato de Licença de Usuário Final**.

   c. Clique no botão **Aceitar tudo** para aceitar todos os contratos de licença e políticas de privacidade exibidos na lista.

7. Na etapa **Nome do novo pacote de instalação** do assistente, no **Nome do pacote**, digite o nome para o pacote de instalação e clique em **Avançar**.

   O pacote de instalação recém-criado é carregado no Servidor de Administração. O Assistente de novo pacote exibe uma mensagem informando que o pacote de instalação foi criado com êxito.

8. Clique no botão **Concluir**.

O pacote de instalação recém-criado é exibido na lista de pacotes de instalação. Você pode selecionar esse pacote ao criar ou reconfigurar a tarefa Instalar o aplicativo remotamente.

Você pode criar e reconfigurar a tarefa Instalar o aplicativo remotamente usando um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky somente se tiver uma licença de Gerenciamento de patches e vulnerabilidades.

Ver e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky

Se você já criou algum pacote de instalação de aplicativos de terceiros listados no banco de dados da Kaspersky, poderá visualizar e modificar as configurações desse pacote posteriormente.

A modificação das configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky está disponível apenas para a licença de Gerenciamento de patches e vulnerabilidades.

Para visualizar e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky:

1. No menu principal, vá para **Gerenciamento de software → Pacotes de instalação**.
2. Na lista de pacotes de instalação aberta, clique no nome do pacote relevante.

   A janela de propriedades é exibida.

3. Ajuste as configurações, se necessário.
4. Clique no botão **Salvar**.

As configurações que você modificou são salvas.

Configurações do pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky

As configurações do pacote de instalação para um aplicativo de terceiros são agrupadas nas seguintes guias:

Nem todas as configurações listadas abaixo são exibidas por padrão. Você pode adicionar as colunas necessárias clicando no botão **Filtro** e selecionando os nomes das colunas relevantes na lista.

- Guia **Geral**:
  - Campo de entrada que contém o nome do pacote de instalação e que pode ser editado manualmente
  - **Aplicativo**

    O nome do aplicativo de terceiros para o qual o pacote de instalação foi criado.
  - **Versão**

    O número da versão do aplicativo de terceiros para o qual o pacote de instalação foi criado.
  - **Tamanho**

    O tamanho do pacote de instalação de terceiros (em kilobytes).
  - **Criação**

    A data e hora em que o pacote de instalação de terceiros foi criado.
  - **Caminho**

    O caminho para a pasta de rede em que o pacote de instalação de terceiros está localizado.
- Guia **Procedimento de instalação**:
  - **Instalar os componentes obrigatórios gerais do sistema**

    Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional.

    Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

    Por padrão, esta opção está desativada.
  - Tabela que exibe as propriedades da atualização e contém as seguintes colunas:
    - **Nome**

      O nome da atualização.
    - **Descrição**

      A descrição da atualização.

- **Origem**

  A fonte da atualização, isto é, se foi lançada pela Microsoft ou por outro desenvolvedor terceiro.

- **Tipo**

  O tipo da atualização, ou seja, se é destinada a um driver ou aplicativo.

- **Categoria**

  A categoria WSUS (Windows Server Update Services) exibida para atualizações da Microsoft (atualizações críticas, atualizações de definições, drivers, pacotes de recursos, atualizações de segurança, service packs, ferramentas, pacotes cumulativos de atualizações, atualizações ou upgrades).

- **Nível de importância de acordo com o MSRC**

  O nível de importância da atualização definido pelo Microsoft Security Response Center (MSRC).

- **Nível de importância**

  O nível de importância da atualização definido pela Kaspersky.

- **Nível de importância do patch**

  O nível de importância do patch caso se destine a um aplicativo Kaspersky.

- **Artigo**

  O identificador (ID) do artigo na Base de Conhecimento que descreve a atualização.

- **Boletim**

  O ID do boletim de segurança que descreve a atualização.

- **Não atribuído para a instalação (nova versão)**

  Exibe se a atualização tem o status Não atribuída para instalação.

- **A ser instalado**

  Exibe se a atualização tem o status A ser instalada.

- **Instalando**

  Exibe se a atualização tem o status Instalando.

- **Instalado**

  Exibe se a atualização tem o status Instalada.

- **Falhou**

  Exibe se a atualização tem o status Falha.

- **A reinicialização é necessária**

  Exibe se a atualização tem o status Reinicialização necessária.

- **Registrado**

  Exibe a data e a hora em que a atualização foi registrada.

- **Instalado no modo interativo**

  Exibe se a atualização requer interação com o usuário durante a instalação.

- **Status de aprovação da atualização**

  Exibe se a atualização está aprovada para instalação.

- **Revisão**

  Exibe o número da revisão atual da atualização.

- **ID de atualização**

  Exibe o ID da atualização.

- **Versão do aplicativo**

  Exibe o número da versão para a qual o aplicativo deve ser atualizado.

- **Substituído**

  Exibe outras atualizações que podem substituir a atualização.

- **Substituição**

  Exibe outras atualizações que podem ser substituídas pela atualização.

- **Você deve aceitar os termos do Contrato de Licença**

  Exibe se a atualização requer aceitação dos termos de um Contrato de Licença do Usuário Final (EULA).

- **URL de descrição**

  Exibe o nome do fornecedor da atualização.

- **Família do aplicativo**

  Exibe o nome da família de aplicativos à qual a atualização pertence.

- **Aplicativo**

  Exibe o nome do aplicativo ao qual a atualização pertence.

- **Idioma da localização**

  Exibe o idioma da localização da atualização.

- **Não atribuído para a instalação (nova versão)**

  Exibe se a atualização tem o status Não atribuída para instalação (nova versão).

- **Requer a instalação de pré-requisitos**

  Exibe se a atualização tem o status de instalação Requer pré-requisitos.

- **Modo de download**

  Exibe o modo de download da atualização.

- **É um patch**

  Exibe se a atualização é um patch.

- **Não instalado**

  Exibe se a atualização tem o status Não instalada.

- **Criação**

- Guia **Configurações** que exibe as configurações do pacote de instalação, com seus nomes, descrições e valores usados como parâmetros de linha de comando durante a instalação. Se o pacote não fornecer essas configurações, uma mensagem correspondente será exibida. Você pode modificar os valores destas configurações.

- Guia **Histórico de revisões** que exibe as revisões do pacote de instalação e contém as seguintes colunas:

  - **Revisão** - O número da revisão dos pacotes de instalação.

  - **Hora** - Data e hora em que as configurações do pacote de instalação foram modificadas.

  - **Usuário** - Nome do usuário que modificou as configurações do pacote de instalação.

  - **Endereço IP do dispositivo do usuário** – Endereço IP do dispositivo a partir do qual o objeto foi modificado.

  - **Endereço IP do Web Console** – Endereço IP do Kaspersky Security Center Web Console com o qual o objeto foi modificado.

  - **Ação** - Ação executada no pacote de instalação dentro da revisão.

  - **Descrição** - Descrição da revisão relacionada à alteração feita nas configurações do pacote de instalação.

    Por padrão, a descrição da revisão fica em branco. Para adicionar uma descrição a uma revisão, selecione a revisão relevante e clique no botão **Editar descrição**. Na janela aberta, insira algum texto para a descrição da revisão.

Correção de vulnerabilidades em uma rede isolada

Esta seção descreve as etapas necessárias para corrigir vulnerabilidades de softwares de terceiros em dispositivos gerenciados conectados a Servidores de Administração que não têm acesso à Internet.

Cenário: correção de vulnerabilidades de softwares de terceiros em uma rede isolada

É possível instalar as atualizações e corrigir as vulnerabilidades do software de terceiros instalado em dispositivos gerenciados em uma rede isolada. Essas redes incluem Servidores de Administração e dispositivos gerenciados conectados a eles sem acesso à Internet. Para corrigir as vulnerabilidades neste tipo de rede, será necessário um Servidor de Administração conectado à Internet. Usando o Servidor de Administração com acesso à Internet, você poderá baixar patches (atualizações necessárias) e depois transmiti-los para Servidores de Administração isolados.

> É possível baixar as atualizações de softwares de terceiros emitidas por fornecedores de software, mas não é possível baixar as atualizações de software da Microsoft em Servidores de Administração isolados usando o Kaspersky Security Center.

Para mais detalhes sobre o processo de correção de vulnerabilidades em uma rede isolada, consulte a descrição e o esquema do processo.

Pré-requisitos

Antes de começar, faça o seguinte:

1. Aloque um dispositivo para estabelecer conexão com a Internet e baixar patches. Esse dispositivo será considerado o Servidor de Administração com acesso à Internet.
2. Instale o Kaspersky Security Center Linux, posterior à versão 15.1, nos seguintes dispositivos:
   - Dispositivo alocado, que atuará como Servidor de Administração com acesso à Internet
   - Dispositivos isolados, que atuarão como Servidores de Administração isolados da Internet (também chamados de Servidores de Administração isolados)
3. Certifique-se de que cada Servidor de Administração tenha espaço em disco suficiente para baixar e armazenar as atualizações e patches.

Fases

A instalação de atualizações e a correção de vulnerabilidades de software de terceiros em dispositivos gerenciados de Servidores de Administração isolados consiste nas seguintes etapas:

1. **Configuração do Servidor de Administração com acesso à Internet**

   Prepare o Servidor de Administração com acesso à Internet para lidar com as solicitações para atualizações de softwares de terceiros necessárias e para fazer download de patches.

2. **Configuração de Servidores de Administração isolados**

   Prepare os Servidores de Administração isolados para que possam formar regularmente listas de atualizações necessárias e lidar com patches baixados pelo Servidor de Administração com acesso à Internet. Após a configuração, os Servidores de Administração isolados não tentam mais baixar os patches da Internet. Em vez disso, eles recebem atualizações por meio de patches.

3. **Transmissão de patches e instalação de atualizações em Servidores de Administração isolados**

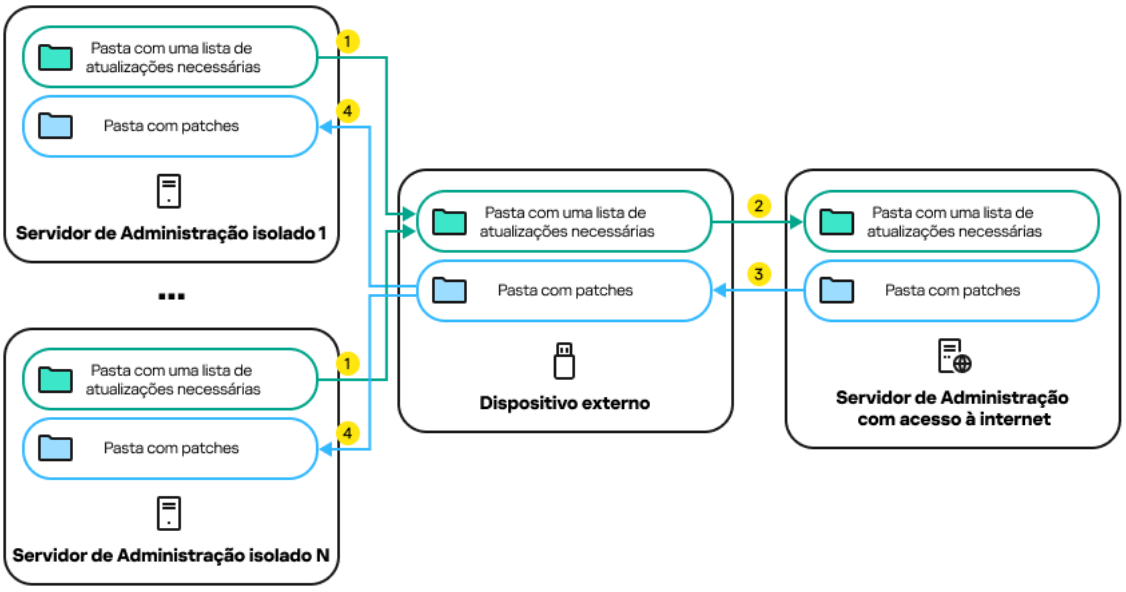
   Depois de configurar os Servidores de Administração, é possível transmitir as listas de atualização e patches necessários do Servidor de Administração com acesso à Internet para os Servidores de Administração isolados. Em seguida, as atualizações de patches serão instaladas em dispositivos gerenciados usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

Resultados

Assim, as atualizações de softwares de terceiros são transmitidas para Servidores de Administração isolados e instaladas em dispositivos gerenciados conectados usando o Kaspersky Security Center Linux. Basta configurar os Servidores de Administração uma vez e, depois disso, será possível obter as atualizações quantas vezes precisar, por exemplo, uma ou várias vezes por dia.

Sobre a correção de vulnerabilidades de softwares de terceiros em uma rede isolada

O processo de correção de vulnerabilidades de software de terceiros em uma rede isolada é mostrado na figura abaixo. Você pode repetir esse processo periodicamente.



O processo de transmissão de patches e a lista de atualizações necessárias entre o Servidor de Administração com acesso à Internet e Servidores de Administração isolados

Cada Servidor de Administração isolado da Internet (aqui denominado Servidor de Administração isolado) gera uma lista de atualizações que devem ser instaladas em dispositivos gerenciados conectados a esse Servidor de Administração. Essa lista de atualizações é armazenada em uma pasta específica como um conjunto de arquivos binários, cada um nomeado com o ID do patch que contém a atualização necessária. Portanto, cada arquivo na lista corresponde a um patch específico.

A lista de atualizações necessárias é transferida do Servidor de Administração isolado para o Servidor de Administração atribuído com acesso à Internet usando um dispositivo externo. Depois disso, o Servidor de Administração atribuído baixa os patches da Internet e os coloca em uma pasta designada.

Quando todos os patches são baixados e colocados na pasta designada, eles são, então, transferidos de volta para cada Servidor de Administração isolado do qual a lista de atualizações necessárias foi obtida. Os patches são salvos em uma pasta criada especificamente para eles em cada Servidor de Administração isolado.

Como resultado, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* executa os patches e instala as atualizações nos dispositivos gerenciados dos Servidores de Administração isolados.

Configuração do Servidor de Administração com acesso à Internet para corrigir vulnerabilidades em uma rede isolada

Para preparar a correção de vulnerabilidades e transmissão de patches dentro de uma rede isolada, a etapa inicial é configurar um Servidor de Administração com acesso à Internet e, em seguida, configurar Servidores de Administração isolados.

Para configurar um Servidor de Administração com acesso à Internet:

1. Crie duas pastas no disco onde o Servidor de Administração estiver instalado:

   - Pasta para a lista de atualizações necessárias
   - Pasta para patches

   Você pode dar a essas pastas qualquer nome que desejar.

2. Conceda a permissão **Modificar** ao grupo KLAdmins nas pastas criadas por meio das ferramentas administrativas padrão do sistema operacional.

3. Use o utilitário klscflag para especificar os caminhos para as pastas nas propriedades do Servidor de Administração.

   Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

4. Execute os seguintes comandos na linha de comando:

   - Para definir o caminho para a pasta de patches:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<caminho para a pasta>"`
   - Para definir o caminho para a pasta para a lista de atualizações necessárias:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<caminho para a pasta>"`

   Exemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/FolderForPatches"`

5. Se necessário, use o utilitário klscflag para especificar com que frequência o Servidor de Administração deve verificar novas solicitações de patch:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <valor em segundos>
```

A configuração padrão é de 120 segundos.

Exemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Crie a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para obter informações sobre patches para o software de terceiros instalado nos dispositivos gerenciados e, em seguida, defina o agendamento da tarefa.

7. Crie a tarefa *Corrigir vulnerabilidades* para especificar patches para o software de terceiros usado para corrigir vulnerabilidades e, em seguida, defina o agendamento da tarefa.

   Execute a tarefa manualmente se desejar que ela seja executada antes do especificado no agendamento. A ordem em que as tarefas são iniciadas é importante. A tarefa *Corrigir vulnerabilidades* deve ser executada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

8. Reinicie o serviço do Servidor de Administração.

O Servidor de Administração com acesso à Internet está pronto para baixar e transmitir as atualizações para os Servidores de Administração isolados. Antes de começar a corrigir as vulnerabilidades, configurar os Servidores de Administração isolados.

Configuração de Servidores de Administração isolados para corrigir vulnerabilidades em uma rede isolada

Depois de configurar o Servidor de Administração com acesso à internet, prepare cada Servidor de Administração isolado dentro de sua rede para correção de vulnerabilidades e instalação de atualizações em dispositivos gerenciados conectados a esses Servidores de Administração isolados.

Para configurar Servidores de Administração isolados, siga as etapas abaixo para cada Servidor de Administração:

1. Ative uma chave de licença para o recurso Gerenciamento de patches e vulnerabilidades (VAPM).

2. Crie duas pastas no disco onde o Servidor de Administração estiver instalado:

   - Pasta para a lista de atualizações necessárias
   - Pasta para patches

   Você pode dar a essas pastas qualquer nome que desejar.

3. Conceda a permissão **Modificar** ao grupo KLAdmins nas pastas criadas por meio das ferramentas administrativas padrão do sistema operacional.

4. Use o utilitário klscflag para especificar os caminhos para as pastas nas propriedades do Servidor de Administração.

   Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

5. Execute os seguintes comandos na linha de comando:

   - Para definir o caminho para a pasta de patches:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<caminho da pasta>"`
   - Para definir o caminho para a pasta para a lista de atualizações necessárias:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<caminho para a pasta>"`

   Exemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`

6. Se necessário, use o utilitário klscflag para especificar com que frequência o Servidor de Administração isolado deve verificar novos patches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <valor em segundos>`

   A configuração padrão é de 120 segundos.

   Exemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`

7. Se necessário, use o utilitário klscflag para calcular os hashes SHA256 dos patches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Ao executar este comando, você pode garantir que os patches não foram modificados durante sua transferência para o Servidor de Administração isolado e que recebeu os patches corretos contendo as atualizações necessárias.

   Por padrão, o Kaspersky Security Center Linux não calcula os hashes SHA256 dos patches. Caso queira habilitar essa opção, depois que o Servidor de Administração isolado receber os patches, o Kaspersky Security Center Linux calculará os hashes e comparará os valores adquiridos com os hashes armazenados no banco de dados do Servidor de Administração. Caso o hash calculado não corresponda ao hash no banco de dados, ocorrerá um erro e será necessário substituir os patches incorretos.

8. Crie a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para obter informações sobre patches para o software de terceiros instalado nos dispositivos gerenciados e, em seguida, defina o agendamento da tarefa.

9. Crie a tarefa *Corrigir vulnerabilidades* para especificar patches para o software de terceiros usado para corrigir vulnerabilidades e, em seguida, defina o agendamento da tarefa.

   Execute a tarefa manualmente se desejar que ela seja executada antes do especificado no agendamento. A ordem em que as tarefas são iniciadas é importante. A tarefa *Corrigir vulnerabilidades* deve ser executada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

10. Reinicie o serviço do Servidor de Administração.

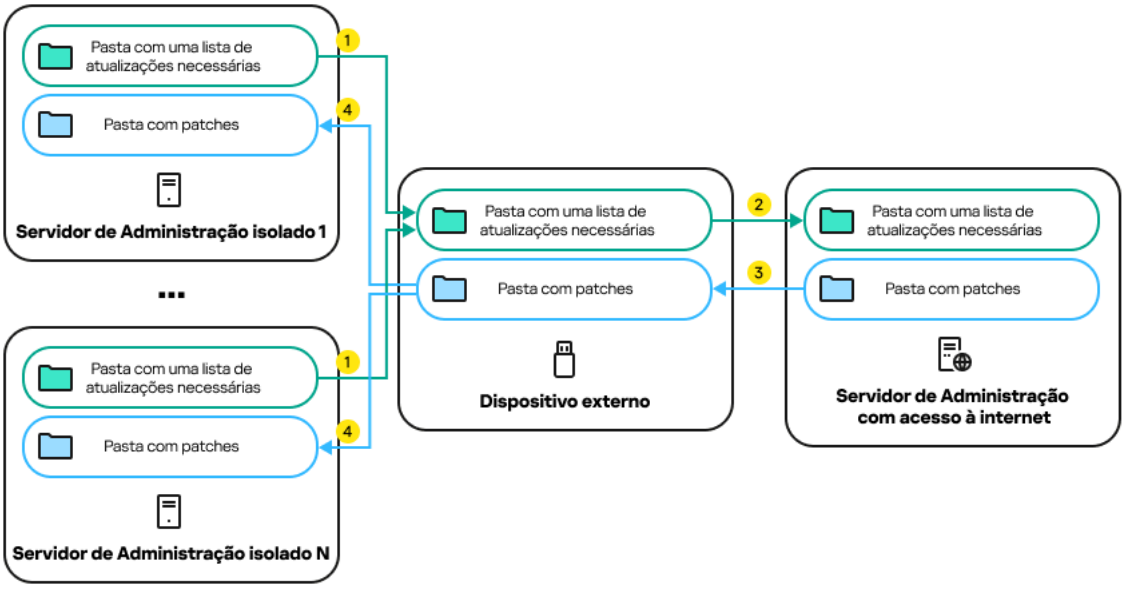
Após configurar todos os Servidores de Administração, será possível transmitir os patches e listas de atualizações necessárias e corrigir as vulnerabilidades de software de terceiros em dispositivos gerenciados dentro da rede isolada.

Transmissão de patches e instalação de atualizações em uma rede isolada

Depois de ter terminado a configuração dos Servidores de Administração, é possível transferir os patches com as atualizações necessárias do Servidor de Administração com acesso à Internet para os Servidores de Administração isolados. É possível transmitir e instalar as atualizações sempre que precisar, por exemplo, uma ou várias vezes por dia.

É necessário um dispositivo externo, como uma unidade removível, para transferir os patches e a lista de atualizações entre os Servidores de Administração. Portanto, certifique-se de que o dispositivo externo tenha espaço em disco suficiente para baixar e armazenar patches.

O processo de transmissão de patches e a lista de atualizações necessárias são exibidos na figura abaixo:



O processo de transmissão de patches e a lista de atualizações necessárias entre o Servidor de Administração com acesso à Internet e Servidores de Administração isolados

Para instalar as atualizações e corrigir as vulnerabilidades em dispositivos gerenciados conectados aos Servidores de Administração isolados:

1. Comece a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* se ainda não estiver em execução.

2. Conecte um dispositivo externo a qualquer Servidor de Administração isolado.

3. Crie duas pastas no dispositivo externo: uma para a lista de atualizações necessárias e outra para os patches. Você pode dar a essas pastas qualquer nome que desejar.

   Caso tenha criado essas pastas anteriormente, basta limpá-las.

4. Copie a lista de atualizações necessárias de cada Servidor de Administração isolado e cole essa lista na pasta para a lista de atualizações necessárias no dispositivo externo.

   Como resultado, você une todas as listas adquiridas de todos os Servidores de Administração isolados em uma pasta. Essa pasta contém os arquivos binários com os IDs de patches necessários para todos os Servidores de Administração isolados.

5. Conecte o dispositivo externo ao Servidor de Administração com acesso à Internet.

6. Copie a lista de atualizações necessárias do dispositivo externo e cole essa lista na pasta da lista de atualizações necessárias no Servidor de Administração com acesso à Internet.

   Todos os patches necessários são baixados automaticamente da Internet para a pasta de patches no Servidor de Administração. Isso pode levar várias horas.

7. Certifique-se de que todos os patches necessários foram baixados. Nesse caso, é possível fazer o seguinte:

   - Verifique a pasta para os patches no Servidor de Administração com acesso à Internet. Todos os patches especificados na lista de atualizações necessárias devem ser baixados para a pasta necessária. Isso é mais conveniente caso seja necessário um pequeno número de patches.

   - Prepare um script especial, por exemplo, um script de shell. Caso obtenha um grande número de patches, será difícil verificar por conta própria se todos os patches foram baixados. Nesses casos, é melhor automatizar a verificação.

8. Copie os patches do Servidor de Administração com acesso à Internet e cole-os na pasta correspondente do dispositivo externo.

9. Transfira os patches para cada Servidor de Administração isolado. Coloque os patches em uma pasta específica para eles.

Como resultado, cada Servidor de Administração isolado cria uma lista real de atualizações necessárias para os dispositivos gerenciados conectados ao Servidor de Administração atual. Após o Servidor de Administração com acesso à Internet receber a lista de atualizações necessárias, o Servidor de Administração baixa os patches da Internet. Quando esses patches aparecem nos Servidores de Administração isolados, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* lidará com os patches. Assim, as atualizações são instaladas em dispositivos gerenciados e as vulnerabilidades de softwares de terceiros são corrigidas.

Quando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* estiver em execução, não reinicialize o dispositivo do Servidor de Administração e não execute a tarefa *Backup de dados do Servidor de Administração* (também causará uma reinicialização). Como resultado, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será interrompida e as atualizações não serão instaladas. Nesse caso, é preciso reiniciar essa tarefa manualmente ou aguardar o início da tarefa de acordo com o agendamento configurado.

Desativar a transmissão de patches e a instalação de atualizações em uma rede isolada

É possível desativar a transmissão de patches para Servidores de Administração isolados, por exemplo, caso decida retirar um ou mais Servidores de Administração de uma rede isolada. Assim, é possível reduzir o número de patches e o tempo para baixá-los.

Para desativar a transmissão de patches para Servidores de Administração isolados:

1. Caso queira remover todos os Servidores de Administração do isolamento, nas propriedades do Servidor de Administração com acesso à Internet, exclua os caminhos para as pastas destinadas aos patches e a lista de atualizações necessárias. Caso queira manter Servidores de Administração específicos dentro de uma rede isolada, ignore essa etapa.

Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Execute os seguintes comandos na linha de comando:

- Para excluir o caminho para a pasta de patches:
  `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""`
- Para excluir o caminho para a pasta para obter a lista de atualizações necessárias:
  `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""`

2. Reinicie o serviço no Servidor de Administração com acesso à Internet se você excluiu os caminhos para as pastas.

3. Nas propriedades de cada Servidor de Administração isolado que deseja remover da rede isolada, exclua os caminhos para as pastas de patches e a lista de atualizações necessárias.

   Execute os seguintes comandos na linha de comando em uma conta com privilégios de raiz:

   - Para excluir o caminho para a pasta de patches:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""`
   - Para excluir o caminho para a pasta para obter a lista de atualizações necessárias:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""`

4. Reinicie o serviço em cada Servidor de Administração no qual os caminhos para as pastas foram excluídos.

Se você reconfigurou o Servidor de Administração com acesso à Internet, os patches não serão mais transmitidos por meio do Kaspersky Security Center Linux.

Se você reconfigurou somente Servidores de Administração específicos e os removeu da rede isolada, eles não receberão mais patches por meio do Kaspersky Security Center Linux. Somente os Servidores de Administração que permanecem dentro da rede isolada continuarão a receber patches.

Caso queira começar a corrigir as vulnerabilidades nos Servidores de Administração isolados desabilitados no futuro, será necessário configurar esses Servidores de Administração e o Servidor de Administração com acesso à internet outra vez.

Guia de referência de API

Este guia de referência da OpenAPI do Kaspersky Security Center foi projetado para ajudar nas seguintes tarefas:

- Automação e personalização. É possível automatizar tarefas que você não deseja tratar manualmente. Por exemplo, como administrador, é possível usar o Kaspersky Security Center OpenAPI para criar e executar scripts que facilitarão o desenvolvimento da estrutura dos grupos de administração e manterão essa estrutura atualizada.

- Desenvolvimento personalizado. Usando a OpenAPI, você pode desenvolver um aplicativo cliente.

É possível usar o campo de pesquisa à direita da tela para localizar as informações de que precisa no guia de referência da OpenAPI.

GUIA DE REFERÊNCIA DA OPENAPI

Exemplos de scripts

O guia de referência do OpenAPI contém exemplos dos scripts Python listados na tabela abaixo. Os exemplos mostram como é possível chamar os métodos OpenAPI e realizar automaticamente várias tarefas para proteger sua rede, por exemplo, criar uma hierarquia "principal/secundária", executar tarefas no Kaspersky Security Center Linux ou atribuir pontos de distribuição. Você pode executar as amostras como estão ou criar seus próprios scripts com base nos exemplos.

Para chamar os métodos OpenAPI e executar scripts,

Instale o pacote KlAkOAPI do arquivo KlAkOAPI.tar.gz em um dispositivo onde o Servidor de Administração está instalado.

O pacote KlAkOAPI contém um conjunto de amostras que executam operações comuns. Você poderá chamar os métodos OpenAPI, executar os exemplos e seus próprios scripts somente em dispositivos onde o Servidor de Administração e o pacote KlAkOAPI estiverem instalados. O arquivo KlAkOAPI.tar.gz que contém esse pacote está localizado na pasta de instalação do Kaspersky Security Center Linux.

Correspondência entre cenários de usuário e exemplos de métodos de OpenAPI do Kaspersky Security Center

Exemplo	Objetivo do exemplo	Cenário
Log KlAkParams	É possível extrair e processar dados usando a estrutura de dados `KlAkParams`. O exemplo mostra como trabalhar com essa estrutura de dados. A saída, nesse exemplo, pode estar presente de maneiras diferentes. É possível obter os dados para enviar um método HTTP ou para usar em seu código.	Monitoramento e relatórios
Criar e excluir uma hierarquia primária/secundária	Você pode adicionar um Servidor de Administração secundário e estabelecer uma hierarquia "primária/secundária". Como alternativa, é possível desconectar o Servidor de Administração secundário da hierarquia.	Como criar uma hierarquia de Servidores de Administração. adicionando um Servidor de Administração secundário e como excluir uma hierarquia de Servidores de Administração
Baixar arquivos de lista de rede por meio do gateway de conexão para o host especificado	É possível conectar o Agente de Rede no dispositivo necessário usando um gateway de conexão e depois baixar um arquivo com a lista de redes no computador.	Ajuste de pontos de distribuição e gateways de conexão

Exemplo	Objetivo do exemplo	Cenário
Instalar uma chave de licença armazenada no repositório principal do Servidor de Administração nos Servidores de Administração secundários	É possível se conectar ao Servidor de Administração principal, baixar uma chave de licença necessária a partir dele e transmitir essa chave para todos os Servidores de Administração secundários incluídos em uma hierarquia.	Licenciamento de aplicativos gerenciados
Criar um relatório de direitos efetivos do usuário	É possível criar relatórios diferentes. Por exemplo, é possível gerar o relatório dos direitos efetivos do usuário usando este exemplo. Este relatório descreve os direitos de um usuário, dependendo do seu grupo e função. É possível baixar o relatório no formato HTML, PDF ou Excel.	Como gerar e visualizar um relatório
Iniciar a tarefa do dispositivo	É possível se conectar ao Agente de Rede no dispositivo necessário usando um gateway de conexão e executar na sequência a tarefa necessária.	Como iniciar uma tarefa manualmente
Registrar os pontos de distribuição para dispositivos em um grupo	É possível atribuir dispositivos gerenciados como pontos de distribuição (anteriormente conhecidos como agentes de atualização).	Atualização dos bancos de dados e dos aplicativos da Kaspersky
Enumerar todos os grupos	É possível executar as seguintes ações nos grupos de administração: No exemplo é mostrado como fazer o seguinte: • Obtenha um identificador do grupo raiz "Dispositivos gerenciados" • Percorra a hierarquia do grupo • Recupere a hierarquia completa e expandida de grupos, junto com seus nomes e aninhamento	Configurando o Servidor de Administração
Enumerar tarefas, consultar estatísticas de tarefas e executar uma tarefa	É possível descobrir as seguintes informações: • Histórico de progresso da tarefa • Status da tarefa atual • Número de tarefas em diferentes status É possível também executar uma tarefa. Por padrão, a amostra executa uma tarefa depois de gerar estatísticas.	Tarefas de gerenciamento
Criar e executar uma tarefa	É possível criar uma tarefa. Especifique os seguintes parâmetros de tarefa no exemplo: • Tipo • Método de execução • Nome • Grupo de dispositivos para o qual a tarefa será usada Por padrão, no exemplo é criada uma tarefa do tipo "Mostrar mensagem". É possível executar esta tarefa para todos os dispositivos gerenciados do Servidor de Administração. Se necessário, é possível especificar seus próprios parâmetros de tarefa.	Criar uma tarefa
Enumerar chaves de licença	É possível obter uma lista de todas as chaves de licença ativas para os aplicativos Kaspersky instalados em dispositivos gerenciados do Servidor de Administração. A lista contém dados detalhados sobre cada chave de licença, como nome, tipo ou data de término.	Visualizando de informações sobre chaves de licença em uso
Criar e encontrar um usuário interno	É possível criar uma conta para trabalhos futuros.	Adicionar uma conta de usuário interno
Criar uma categoria personalizada	É possível criar a categoria do aplicativo com os parâmetros necessários.	Criar uma categoria de aplicativos com conteúdo adicionado manualmente
Enumerar usuários usando SrvView	É possível usar a classe SrvView para solicitar informações detalhadas do Servidor de Administração. Por exemplo, é possível obter uma lista de usuários usando este exemplo.	Gerenciamento de usuários e funções dos usuários
Criar usuários internos, criar e enviar por e-mail um pacote de instalação do Android	É possível criar usuários internos utilizando a classe SecurityPolicy, além de criar um pacote de instalação do Android e enviá-lo aos usuários por e-mail.	Adicionar uma conta de usuário interno

Aplicativos que interagem com o Kaspersky Security Center Linux por meio da OpenAPI

Alguns aplicativos interagem com o Kaspersky Security Center Linux por meio da OpenAPI. Esses aplicativos incluem, por exemplo, o Kaspersky Anti Targeted Attack Platform ou o Kaspersky Security for Virtualization. Também pode ser um aplicativo cliente personalizado que você pode desenvolver usando a OpenAPI.

Os aplicativos que interagem com o Kaspersky Security Center Linux por meio da OpenAPI conectam-se ao Servidor de Administração. Caso tenha configurado uma lista de permissão de endereços IP para se conectar ao Servidor de Administração, adicione os endereços IP de dispositivos nos quais os aplicativos que usam a OpenAPI do Kaspersky Security Center Linux estão instalados. Para saber se o aplicativo usado funciona por OpenAPI, consulte a Ajuda do aplicativo.

Práticas recomendadas para Provedores de Serviços

Esta seção fornece informações sobre como configurar e usar o Kaspersky Security Center Linux.

Esta seção contém recomendações sobre como implementar, configurar e usar o aplicativo, assim como descreve os modos para solucionar problemas típicos na operação do aplicativo.

Planejamento da implementação do Kaspersky Security Center Linux

Ao planejar a implementação dos componentes do Kaspersky Security Center Linux na rede de uma organização, você deve levar em consideração o tamanho e o escopo do projeto; especificamente, os seguintes fatores:

- Número total de dispositivos
- Número de clientes MSP

Um Servidor de Administração pode suportar um máximo de 50.000 dispositivos. Se o número total de dispositivos na rede de uma organização exceder 50.000, múltiplos Servidores de Administração devem ser implementados no provedor de serviços e combinados em uma hierarquia para o gerenciamento centralizado conveniente.

Até 500 servidores virtuais podem ser criados em um único Servidor de Administração, portanto um Servidor de Administração individual é necessário para cada um dos 500 clientes MSP.

Na etapa do planejamento da implementação, a atribuição do certificado especial X.509 ao Servidor de Administração deve considerada. A atribuição do certificado X.509 ao Servidor de Administração pode ser útil nos seguintes casos (lista parcial):

- Inspecionar tráfego da camada do soquete seguro (SSL) por meio de um proxy de terminação SSL
- Especificação dos valores necessários nos campos do certificado
- Fornecer a força de criptografia necessária de um certificado

Fornecer acesso à Internet ao Servidor de Administração

Para permitir que os dispositivos na rede cliente acessem o Servidor de Administração pela Internet, é necessário tornar as seguintes portas do Servidor de Administração disponíveis:

- Porta 13000 TCP – TLS do Servidor de Administração para conectar Agentes de Rede implementados na rede cliente
- Porta 8061 TCP – HTTPS para publicar pacotes independentes usando ferramentas do Kaspersky Security Center Web Console

- Porta 8060 TCP – HTTP para publicar pacotes independentes usando ferramentas do Kaspersky Security Center Web Console
- Porta 13292 TCP – Porta TLS somente é necessária se houver dispositivos móveis que precisam de ser gerenciados
- Porta 8080 TCP – HTTPS para o Kaspersky Security Center Web Console

Configuração padrão do Kaspersky Security Center Linux

Um ou diversos Servidores de Administração são implementados nos servidores MSP. O número de Servidores de Administração pode ser selecionado com base no hardware disponível ou no número total clientes MSP servidos ou no número total de dispositivos gerenciados.

Um Servidor de Administração pode suportar até 50.000 dispositivos. Você deve considerar a possibilidade de aumentar o número de dispositivos gerenciados no futuro próximo: pode ser útil conectar um número ligeiramente menor de dispositivos a um único Servidor de Administração.

Até 500 servidores virtuais podem ser criados em um único Servidor de Administração, portanto um Servidor de Administração individual é necessário para cada um dos 500 clientes MSP.

Se múltiplos servidores forem usados, recomenda-se que você os combine em uma hierarquia. Usar uma hierarquia de Servidores de Administração permite-lhe evitar políticas e tarefas duplicadas, tratar todo o conjunto de dispositivos gerenciados como se eles fossem gerenciados por um único Servidor de Administração: ou seja, procura por dispositivos, criação de seleções de dispositivos e criação de relatórios.

Em cada servidor virtual correspondente a um cliente MSP, é necessário atribuir um ou diversos ponto(s) de distribuição. Se os clientes MSP e o Servidor de Administração forem vinculados por meio da Internet, pode ser útil criar uma tarefa *Baixar atualizações para os repositórios de pontos de distribuição* referente aos pontos de distribuição, para que baixem as atualizações diretamente dos servidores da Kaspersky e não do Servidor de Administração.

Se alguns dispositivos na rede cliente MSP não tiverem acesso direto à Internet, você tem de trocar os pontos de distribuição para o modo de gateway de conexão. Nesse caso, os Agentes de Rede em dispositivos na rede cliente MSP serão conectados, para a sincronização adicional, ao Servidor de Administração – mas através do gateway, não diretamente.

Como o Servidor de Administração, muito provavelmente, não conseguirá sondar a rede do cliente MSP, pode ser útil transferir esta função para um ponto de distribuição.

O Servidor de Administração não será capaz de enviar notificações para a porta 15000 UDP para dispositivos gerenciados localizados além da NAT na rede cliente MSP. Para solucionar este problema, pode ser útil ativar o modo de conexão contínua para o Servidor de Administração nas propriedades dos dispositivos que atuam como pontos de distribuição e sendo executados no modo de gateway de conexão (opção **Não desconectar do Servidor de Administração**). Este modo de conexão contínua está disponível se o número total de pontos de distribuição não exceder 300.

Um cliente MSP pode querer gerenciar dispositivos Android e dispositivos iOS dos funcionários. O Servidor de Administração gerencia dispositivos móveis por meio de TLS, pela porta TCP 13292.

Sobre os pontos de distribuição

Um dispositivo com o Agente de Rede instalado pode ser usado como um ponto de distribuição. Neste modo, o Agente de Rede pode executar as seguintes funções:

- Transfira arquivos para dispositivos clientes, incluindo:
  - Atualizações de bancos de dados e módulos de software da Kaspersky

    As atualizações podem ser recebidas do Servidor de Administração ou dos servidores de atualização Kaspersky. Nesse caso, a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* deve ser criada para o dispositivo que serve como ponto de distribuição.
  - Atualizações de softwares de terceiros
  - Pacotes de instalação
- Instalar software (incluindo a implementação inicial dos Agentes de Rede) em outros dispositivos.
- Faça a sondagem da rede para detectar novos dispositivos e para atualizar as informações sobre os existentes. Um ponto de distribuição pode aplicar os mesmos métodos de localização dos dispositivos que os do Servidor de Administração.

A implementação de pontos de distribuição em uma rede da organização tem os seguintes objetivos:

- Reduzir a carga do Servidor de Administração se ele funcionar como a fonte de atualização.
- Otimizar o tráfego da Internet, já que, nesse caso, cada dispositivo na rede cliente MSP não precisa acessar os servidores da Kaspersky ou o Servidor de Administração para obter as atualizações.
- Fornecer ao Servidor de Administração o acesso aos dispositivos além do NAT (relativo ao Servidor de Administração) da rede cliente MSP, que permite ao Servidor de Administração executar as seguintes ações:
  - Enviar notificações para dispositivos por UDP na rede IPv4 ou IPv6
  - Sondar a rede IPv4 ou IPv6
  - Executar a implementação inicial
  - Atuar como um servidor push

Um ponto de distribuição é atribuído para um grupo de administração. Neste caso, o escopo do ponto de distribuição inclui todos os dispositivos dentro do grupo de administração e todos dos seus subgrupos. No entanto, o dispositivo que atua como o ponto de distribuição não precisa estar incluído no grupo de administração ao qual foi atribuído.

Você pode criar uma função de ponto de distribuição como um gateway de conexão. Neste caso, os dispositivos no escopo desse ponto de distribuição serão conectados ao Servidor de Administração por meio do gateway, não diretamente. É possível usar esse modo em cenários que não permitem o estabelecimento de uma conexão direta entre dispositivos com o Agente de Rede e um Servidor de Administração.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Hierarquia de Servidores de Administração

Algumas empresas cliente, por exemplo MSP, podem executar vários Servidores de Administração. Pode ser inconveniente administrar diversos Servidores de Administração separados, portanto uma hierarquia pode ser aplicada. Em uma hierarquia, um Servidor de Administração baseado em Linux pode funcionar tanto como um servidor primário quanto como um servidor secundário. O servidor primário baseado em Linux pode gerenciar servidores secundários baseados em Linux e em Windows. Um servidor principal baseado em Windows pode gerenciar um servidor secundário baseado em Linux.

Uma configuração de "principal / secundário" para dois Servidores de Administração fornece as seguintes opções:

- Um Servidor de Administração secundário herda as políticas, tarefas, funções de usuário e pacotes de instalação do Servidor de Administração principal, prevenindo assim a duplicação das configurações.
- As seleções de dispositivos no Servidor de Administração principal podem incluir dispositivos de Servidores de Administração secundários.
- Os Relatórios no Servidor de Administração principal podem conter dados (incluindo informações detalhadas) de Servidores de Administração secundários.
- Um Servidor de Administração principal pode ser usado como uma origem de atualizações para um Servidor de Administração secundário.

O Servidor de Administração principal somente recebe dados de Servidores de Administração secundários não virtuais dentro do escopo das opções listadas acima. Essa limitação não se aplica aos Servidores de Administração virtuais, que compartilham o banco de dados com seu Servidor de Administração principal.

A hierarquia de Servidores de Administração fornece suporte para o modo de multilocação. Este modo permite que um administrador principal gerencie de forma centralizada vários clientes de forma independente. Cada organização cliente ou escritório é isolado de outros e é referido como uma locação. É possível alocar vários dispositivos gerenciados junto com seus dados, configurações, políticas e tarefas associados a uma locação e configurar os direitos do usuário por locação.

Um Servidor de Administração principal, instalado na infraestrutura principal da organização, atua como uma locação principal. O Servidor de Administração principal permite que os Servidores de Administração secundários ou virtuais (suas locações isoladas) recebam e processem de forma independente seus próprios eventos e trabalhem com seus próprios recursos, serviços e configurações.

Um provedor de serviços que tem várias organizações clientes pode fornecer a funcionalidade do Kaspersky Security Center Linux, incluindo agregação de alertas e ações de resposta, para cada organização cliente de forma independente. Para conseguir isso, o provedor de serviços conecta Servidores de Administração secundários ou virtuais como locatários para cada organização cliente. O provedor de serviços fornece serviços por meio de equipe e recursos próprios.

Servidores de Administração virtual

Com base em um Servidor de Administração físico, múltiplos Servidores de Administração virtuais podem ser criados, que serão semelhantes a Servidores de Administração secundários. Em comparação com o modelo de acesso discricionário, que tem base em listas de controle de acesso (ACLs), o modelo de Servidor de Administração virtual é mais funcional e fornece um maior grau de isolamento. Além de uma estrutura dedicada de grupos de administração para dispositivos atribuídos com políticas e tarefas, cada Servidor de Administração virtual apresenta seu próprio grupo de dispositivos não atribuídos, conjuntos próprios de relatórios, dispositivos e eventos selecionados, pacotes de instalação, regras de movimentação etc. Para isolamento mútuo máximo de clientes MSP, recomendamos que escolha Servidores de Administração virtuais como a funcionalidade a ser usada. Além disso, criar um Servidor de Administração virtual para cada cliente MSP permite-lhe fornecer opções básicas clientes da administração da rede através do Kaspersky Security Center Web Console.

Os Servidores de Administração virtuais são muito semelhantes aos Servidores de Administração secundários, mas com as seguintes distinções:

- Em um Servidor de Administração virtual falta a maior parte das configurações globais e as suas próprias portas TCP.
- Um Servidor de Administração virtual não tem Servidores de Administração secundários.
- Um Servidor de Administração virtual não tem outros Servidores de Administração virtuais.
- Um Servidor de Administração físico exibe dispositivos, grupos, eventos e objetos em dispositivos gerenciados (itens em Quarentena, registro de aplicativos e etc.) de todos os seus Servidores de Administração virtuais.
- Um Servidor de Administração virtual somente pode verificar a rede com pontos de distribuição conectados.

Implementação e configuração inicial

O Kaspersky Security Center Linux é um aplicativo distribuído. O Kaspersky Security Center Linux inclui os seguintes aplicativos:

- Servidor de Administração – o componente principal, projetado para gerenciar os dispositivos de uma organização e armazenar dados em um DBMS.
- Kaspersky Security Center Web Console – Uma interface da Web para o Servidor de Administração projetado para operações básicas. Você pode instalar este componente em qualquer dispositivo que atende aos requisitos de hardware e software.
- Agente de Rede: projetado para gerenciar o aplicativo de segurança instalado em um dispositivo, assim como obter informações sobre aquele dispositivo. Os Agentes de Rede são instalados em dispositivos de uma organização.

A implementação do Kaspersky Security Center Linux em uma rede da organização é executada da seguinte maneira:

- Instalação do Servidor de Administração
- Instalação do Kaspersky Security Center Web Console
- Instalação do Agente de Rede e do aplicativo de segurança em dispositivos da empresa

Recomendações sobre a instalação do Servidor de Administração

Esta seção contém recomendações sobre como instalar o Servidor de Administração. Esta seção também fornece cenários para usar uma pasta compartilhada no dispositivo do Servidor de Administração para implementar o Agente de Rede em dispositivos cliente.

Criar contas para os serviços do Servidor de Administração em um cluster para falhas

Antes de iniciar a implementação do Kaspersky Security Center Linux em um cluster de failover, você deve criar contas para os serviços do Kaspersky Security Center Linux.

Para isso, execute as seguintes etapas no nó ativo, no nó passivo e no servidor de arquivos:

1. Crie um grupo com o nome "kladmins" e atribua o mesmo GID a todos os três grupos.
2. Crie uma conta de usuário com o nome "ksc" e atribua o mesmo UID a todas as três contas de usuário. Defina o grupo principal como "kladmins" para as contas criadas.
3. Crie uma conta de usuário com o nome "rightless" e atribua o mesmo UID a todas as três contas de usuário. Defina o grupo principal como "kladmins" para as contas criadas.

Selecionar um DBMS

A tabela a seguir lista as opções válidas de DBMS, assim como as recomendações e restrições quanto ao seu uso.

Recomendações e restrições no DBMS

DBMS	Recomendações e restrições
MySQL (consulte as versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 20.000 dispositivos.
MariaDB (consulte as versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 20.000 dispositivos.

PostgreSQL, Postgres Pro (ver versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos.
Tantor (ver versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos. O Tantor DBMS é compatível somente com o Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.8).

Para obter informações sobre como instalar o DBMS selecionado, consulte a sua documentação.

Recomendamos desativar a tarefa de Inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados.

Se você decidir instalar o DBMS PostgreSQL ou Postgres Pro, certifique-se de ter especificado uma senha para o superusuário. Se a senha não for especificada, o Servidor de Administração pode não conseguir se conectar ao banco de dados.

Caso o MySQL, MariaDB, PostgreSQL ou Postgres Pro seja instalado, use as configurações recomendadas para garantir que o DBMS funcione corretamente.

Caso um DBMS PostgreSQL, MariaDB ou MySQL seja usado, a guia **Eventos** poderá exibir uma lista incompleta de eventos para o dispositivo cliente selecionado. Isso ocorre quando o DBMS armazena uma quantidade muito grande de eventos. É possível aumentar o número de eventos exibidos com a execução de um dos seguintes procedimentos:

- Remoção de eventos desnecessários.
- Redução do prazo de armazenamento para eventos desnecessários.

Para ver uma lista completa de eventos registrados no Servidor de Administração para o dispositivo, use Relatórios.

Especificar o endereço do Servidor de Administração

Ao instalar o Servidor de Administração, você deve especificar o nome DNS ou o endereço IP estático do Servidor de Administração. Este endereço será usado como o endereço padrão ao criar pacotes de instalação do Agente de Rede. Depois disso, você poderá alterar o endereço do host do Servidor de Administração usando as ferramentas do Kaspersky Security Center Web Console; o endereço não será alterado automaticamente nos pacotes de instalação do Agente de Rede que já foram criados.

Manter conexões ociosas

Recomendamos que você configure os seguintes parâmetros de keepalive nos dispositivos de gateway para melhorar a estabilidade da conexão:

- `net.ipv4.tcp_keepalive_intvl` especifica com que frequência enviar mensagens keepalive após a primeira. Defina este parâmetro como `1`.
- `net.ipv4.tcp_keepalive_probes` especifica quantas mensagens keepalive podem ser enviadas sem uma resposta antes que a conexão seja considerada inativa. Defina este parâmetro como `10`.
- `net.ipv4.tcp_keepalive_time` especifica quanto tempo esperar após o recebimento do último pacote de dados antes de enviar a primeira mensagem keepalive. Defina este parâmetro como `900`.

Para configurar os parâmetros keepalive:

1. Abra o arquivo /etc/sysctl.conf.
2. Adicione os seguintes valores de parâmetro:

   ```
   net.ipv4.tcp_keepalive_intvl = 1
   net.ipv4.tcp_keepalive_probes = 10
   net.ipv4.tcp_keepalive_time = 900
   ```

3. Execute o seguinte comando para atualizar os parâmetros do keepalive:

   ```
   sudo sysctl -p /etc/sysctl.conf
   ```

4. Execute os seguintes comandos para assegurar que os valores dos parâmetros tenham sido aplicados:

   ```
   sudo sysctl net.ipv4.tcp_keepalive_intvl
   sudo sysctl net.ipv4.tcp_keepalive_probes
   sudo sysctl net.ipv4.tcp_keepalive_time
   ```

Implementar o Agente de Rede e os aplicativos de segurança

Para gerenciar dispositivos em uma organização e protegê-los contra ameaças de segurança, você precisa instalar o Agente de Rede e um aplicativo de segurança Kaspersky em cada um deles.

Para obter informações sobre a implementação de proteção, consulte a seção Implementando o Agente de Rede e o aplicativo de segurança.

Para obter informações sobre proteção de dispositivos móveis, consulte a seção Gerenciamento de dispositivos móveis.

No Microsoft Windows XP, o Agente de Rede pode não executar as seguintes operações corretamente: baixar atualizações diretamente dos servidores da Kaspersky (como um ponto de distribuição); funcionar como servidor proxy da KSN (como um ponto de distribuição); e detectar vulnerabilidades de terceiros (caso o Gerenciamento de patches e vulnerabilidades seja usado).

Configurar a proteção em uma rede da organização cliente

Após a instalação de Servidor de Administração ter sido concluída, o Kaspersky Security Center Web Console é iniciado e lhe solicita executar a configuração inicial através do Assistente relevante. Quando o Assistente de início rápido estiver em execução, as seguintes políticas e as tarefas são criadas no grupo de administração raiz:

- Política do Kaspersky Endpoint Security
- Tarefa de grupo para atualizar o Kaspersky Endpoint Security
- Tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security
- Política de Agente de Rede
- Tarefa de verificação de vulnerabilidades (tarefa do Agente de Rede)
- Tarefa de instalação de atualizações e correção de vulnerabilidades (tarefa do Agente de Rede)

As políticas e tarefas são criadas com as configurações padrão, que podem resultar em sub-ótimas ou até inadmissíveis para a organização. Portanto, você deve verificar as propriedades dos objetos que foram criados e os modificá-las manualmente, se necessário.

Esta seção contém informações sobre a configuração manual de políticas, tarefas e outras configurações do Servidor de Administração, e as informações sobre o ponto de distribuição, criando uma estrutura de grupo de administração e a hierarquia de tarefas e outras configurações.

Configuração manual da política do Kaspersky Endpoint Security

Esta seção fornece recomendações sobre como configurar a política do Kaspersky Endpoint Security, que é criada pelo Assistente de início rápido. É possível executar a configuração na janela de propriedades da política.

Ao editar uma configuração, não se esqueça de que é possível bloquear ou desbloquear a configuração para proibir ou permitir a edição do valor em uma estação de trabalho.

Configurar a política na seção Proteção Avançada Contra Ameaças

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Proteção Avançada Contra Ameaças**, é possível configurar o uso da Kaspersky Security Network para o Kaspersky Endpoint Security for Windows. Você também pode configurar os módulos do Kaspersky Endpoint Security for Windows, tal como a Detecção de Comportamento, Prevenção de Exploit, Prevenção de Intrusão do Host e Mecanismo de Correção.

Na subseção **Kaspersky Security Network**, recomendamos a ativação da opção **Kaspersky Security Network**. Use esse recurso para redistribuir e otimizar o tráfego na rede. Se a opção **Kaspersky Security Network** estiver desativada, será possível ativar o uso direto de servidores KSN.

Configurar a política na seção Proteção Essencial Contra Ameaças

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Proteção Essencial Contra Ameaças** da janela de propriedades da política, recomendamos que especifique configurações adicionais nas subseções **Firewall** e **Proteção Contra Ameaças ao Arquivo**.

A subseção **Firewall** contém configurações que permitem controlar a atividade de rede dos aplicativos nos dispositivos cliente. Um dispositivo cliente usa uma rede à qual um dos seguintes status é atribuído: pública, local ou confiável. Dependendo do status da rede, o Kaspersky Endpoint Security pode permitir ou negar atividade de rede em um dispositivo. Ao adicionar uma nova rede à sua organização, você deve atribuir um status de rede apropriado a ela. Por exemplo, se o dispositivo cliente for um laptop, recomendamos que esse dispositivo use a rede pública ou confiável, porque o laptop nem sempre está conectado à rede local. Na subseção **Firewall**, é possível verificar se foram atribuídos corretamente os status às redes usadas na organização.

Para verificar a lista de redes:

1. Nas propriedades de política, acesse **Proteção Essencial Contra Ameaças → Firewall**.
2. Na seção **Redes disponíveis**, clique no botão **Configurações**.
3. Na janela **Firewall** que se abre, vá para a guia **Redes** para visualizar a lista de redes.

Na subseção **Proteção Contra Ameaças ao Arquivo**, é possível desativar a verificação de unidades de rede. A verificação das unidades de rede pode colocar uma carga significativa nas unidades de rede. É mais conveniente executar a verificação indireta em servidores de arquivos.

Para desativar a verificação de unidades de rede:

1. Nas propriedades de política, acesse **Proteção Essencial Contra Ameaças → Proteção Contra Ameaças ao Arquivo**.
2. Na seção **Nível de segurança**, clique no botão **Configurações**.
3. Na janela **Proteção Contra Ameaças ao Arquivo** que é aberta, na guia **Geral**, desmarque a caixa de seleção **Todas as unidades de rede**.

Configurar a política na seção Configurações Gerais

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security.

Abaixo estão descritas as ações de configuração avançada, que recomendamos executar na janela de propriedades da política do Kaspersky Endpoint Security, na seção **Configurações gerais**.

Seção Configurações gerais, subseção Relatórios e Armazenamento

Na seção **Transferência de dados para o Servidor de Administração**, observe a caixa de seleção **Sobre os aplicativos iniciados**. Caso essa caixa de seleção seja marcada, o banco de dados do Servidor de Administração salvará as informações sobre todas as versões de todos os módulos do software nos dispositivos em rede. Estas informações podem necessitar de uma quantidade significativa do espaço disponível em disco para o banco de dados do Kaspersky Security Center Linux (muitos gigabytes). Portanto, caso a caixa de seleção **Sobre aplicativos iniciados** ainda esteja marcada na política de nível superior, ela deverá ser desmarcada.

Seção Configurações gerais, subseção Interface

Caso a proteção contra ameaças na rede da organização precise ser gerenciada no modo centralizado por meio do Kaspersky Security Center Web Console, será necessário desativar a exibição da interface do usuário do Kaspersky Endpoint Security nas estações de trabalho (ao desmarcar a caixa de seleção **Exibir interface do aplicativo** na seção **Interação com o usuário**) e ativar a proteção por senha (marcando a caixa de seleção **Ativar proteção por senha** na seção **Proteção por senha**).

Configurando a política na seção Configuração de eventos

Na seção **Configuração de eventos**, é necessário desativar a função de salvar quaisquer eventos no Servidor de Administração, exceto os seguintes:

- Na guia **Crítico**:
  - *A execução automática do aplicativo está desativada*
  - *Acesso negado*
  - *Proibida a inicialização do aplicativo*
  - *Não é possível desinfectar*
  - *O Contrato de Licença do Usuário Final foi violado*
  - *Não foi possível carregar o módulo de criptografia*
  - *Não é possível iniciar duas tarefas simultaneamente*
  - *Ameaça ativa detectada. A Desinfecção avançada deve ser iniciada*
  - *Ataque de rede detectado*

- *Nem todos os componentes foram atualizados*
- *Erro de ativação*
- *Erro ao ativar o modo portátil*
- *Erro de interação com o Kaspersky Security Center*
- *Erro ao desativar o modo portátil*
- *Erro ao alterar componentes do aplicativo*
- *Erro na aplicação das regras de criptografia/descriptografia do arquivo*
- *A política não pode ser aplicada*
- *Processo encerrado*
- *Atividade de rede bloqueada*

- Na guia **Falha funcional**: *Configurações de tarefa inválidas. Configurações não aplicadas*
- Na guia **Advertência**:
  - *A Autodefesa está desativada*
  - *Chave de reserva inválido*
  - *O usuário optou por cancelar a política de criptografia*
- Na guia **Informações**: *Proibida a inicialização do aplicativo em modo de teste*

Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security

Se o Servidor de Administração atuar como a fonte de atualização, a opção de agendamento ideal e recomendada para o Kaspersky Endpoint Security é **Quando novas atualizações são baixadas no repositório** com a caixa de seleção **Usar atraso randomizado automaticamente para início da tarefas**.

Se uma tarefa local para baixar as atualizações dos servidores da Kaspersky para o repositório que for criado em cada ponto de distribuição, o agendamento periódico será ótimo e recomendado para a tarefa de atualização em grupo do Kaspersky Endpoint Security. Neste caso, o valor de intervalo de randomização deve ser estabelecido em 1 hora.

Configuração manual da tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security

O Assistente de início rápido cria uma tarefa de grupo para verificar um dispositivo. Caso o agendamento especificado automaticamente da tarefa de verificação de grupo não seja adequado para sua organização, é preciso configurar manualmente o agendamento mais conveniente para essa tarefa de acordo com as regras do local de trabalho adotadas na organização.

Por exemplo, é atribuído um agendamento para a tarefa **Executar às sextas-feiras as 19h** com aleatorização automática, e a caixa de seleção **Executar tarefas ignoradas** deve estar desmarcada. Isso significa que se os dispositivos em uma organização são desligados às sextas-feiras, por exemplo, às 18h30, a tarefa de verificação de dispositivo nunca será executada. Nesse caso, é necessário configurar a tarefa de verificação de grupo manualmente.

Agendar a tarefa Encontrar vulnerabilidades e atualizações necessárias

O Assistente de início rápido cria a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para o Agente de Rede. Por padrão, à tarefa é atribuído um agendamento **Executar às terças-feiras as 19:00** com aleatorização automática e se a caixa de seleção **Executar tarefas ignoradas** estiver marcada.

Se as regras do local de trabalho da organização proverem o desligamento de todos os dispositivos nessa hora, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* será executada após os dispositivos serem novamente ligados, ou seja, na quarta-feira pela manhã. Tal atividade pode ser indesejável porque uma verificação de vulnerabilidades pode aumentar a carga de subsistemas de disco e da CPU. Você deve definir o agendamento mais conveniente para a tarefa com base nas regras do local de trabalho adotadas na organização.

Configuração manual da tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades

O Assistente de início rápido cria uma tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades para o Agente de Rede. Por padrão, a tarefa é configurada para ser executada todos os dias à 1h, com randomização automática, e a opção **Executar tarefas perdidas** não está habilitada.

Se as regras do local de trabalho da organização proverem o desligamento dos dispositivos durante a noite, a instalação da atualização nunca será executada. Você deve definir o agendamento mais conveniente da tarefa de verificação de vulnerabilidades com base nas regras do local de trabalho adotadas na organização. Também é importante ter em mente que a instalação das atualizações pode necessitar o reinício do dispositivo.

Criação de uma estrutura de grupos de administração e atribuir pontos de distribuição

Uma estrutura de grupos de administração no Kaspersky Security Center Linux executa as seguintes funções:

- Define o escopo das políticas

  Há um modo alternativo para aplicar configurações relevantes nos dispositivos, usando perfis de política. Nesse caso, o escopo das políticas é definido, por exemplo, com tags de dispositivo ou funções de usuário.

- Define o escopo da tarefas de grupo

  Há uma abordagem para definir o escopo da tarefas de grupo que não tem base em uma hierarquia de grupos de administração: uso de tarefas para seleções de dispositivos e tarefas para dispositivos específicos.

- Define os direitos de acesso aos dispositivos, Servidores de Administração virtuais e Servidores de Administração secundários

- Atribui os pontos de distribuição

Ao criar a estrutura de grupos de administração, você deve levar em conta a topologia da rede da organização para a atribuição ótima de pontos de distribuição. A distribuição ótima dos pontos de distribuição permite poupar tráfego na rede da organização.

Dependendo do organograma da empresa e da topologia da rede adotado pelo MSP cliente, as seguintes configurações padrão podem ser aplicadas à estrutura de grupos de administração:

- Escritório único
- Múltiplos pequenos escritórios remotos

Configuração de cliente MSP padrão: escritório único

Em uma configuração de "escritório único" padrão, todos os dispositivos estão dentro da rede da organização, portanto eles podem se "ver" mutuamente. A rede da organização pode consistir em algumas partes separadas (redes ou segmentos de rede) vinculadas por canais estreitos.

Os seguintes métodos de criar a estrutura de grupos de administração são possíveis:

- Criar uma estrutura de grupos de administração levando em consideração a topologia da rede. A estrutura de grupos de administração pode não refletir a topologia da rede com uma precisão absoluta. Uma coincidência entre as partes separadas da rede e determinados grupos de administração seria suficiente. Você pode usar a atribuição automática de pontos de distribuição ou atribui-los manualmente.
- Criar uma estrutura de grupos de administração não levando em consideração a topologia da rede. Neste caso, você deve desativar a atribuição automática de pontos de distribuição e, a seguir, atribuir um ou diversos dispositivos para atuar como pontos de distribuição de um grupo de administração raiz em cada uma das partes separadas da rede, por exemplo, para o grupo **Dispositivos gerenciados**. Todos os pontos de distribuição estarão no mesmo nível e apresentarão a mesma expansão de escopo para todos os dispositivos na rede da organização. Nesse caso, cada Agente de Rede se conectará ao ponto de distribuição que tenha a rota mais curta. Você pode rastrear a rota até um ponto de distribuição usando o utilitário tracert ou traceroute.

Configuração de cliente MSP padrão: múltiplos pequenos escritórios remotos

Esta configuração padrão proporciona uma série de pequenos escritórios remotos, que podem se comunicar com a sede através da Internet. Cada escritório remoto é localizado além da NAT, ou seja, a conexão de um escritório remoto ao outro não é possível porque os escritórios estão isolados entre si.

A configuração deve ser refletida na estrutura de grupos de administração: um grupo de administração separado deve ser criado para cada escritório remoto (grupos **Escritório 1** e **Escritório 2** na figura abaixo).



Os escritórios remotos estão incluídos na estrutura do grupo de administração

Um ou vários pontos de distribuição devem ser atribuídos à cada grupo de administração que corresponda a um escritório. Os pontos de distribuição devem ser dispositivos nos escritórios remotos que têm espaço livre suficiente em disco. Os dispositivos implementados no grupo **Escritório 1**, por exemplo, acessarão os pontos de distribuição atribuídos ao grupo de administração **Escritório 1**.

Se alguns usuários se moverem entre escritórios fisicamente, com os seus computadores portáteis, você deve selecionar dois ou mais dispositivos (além dos pontos de distribuição existentes) em cada escritório remoto e atribui-los para atuar como pontos de distribuição para um grupo de administração de nível superior (**Grupo de raiz para escritórios** na figura acima).

Exemplo: Um computador portátil é implementado no grupo de administração **Escritório 1** e então é movido fisicamente para o escritório que corresponde ao grupo de administração **Escritório 2**. Após o computador portátil ter sido movido, o Agente de Rede tenta acessar os pontos de distribuição atribuídos ao grupo **Escritório 1**, mas aqueles pontos de distribuição estão indisponíveis. Então, O Agente de Rede começa a tentar acessar os pontos de distribuição que foram atribuídos ao **Grupo de raiz para escritórios**. Como os escritórios remotos estão isolados entre si, as tentativas de acessar os pontos de distribuição atribuídos ao grupo de administração **Grupo raiz para escritórios** somente terão êxito quando o Agente de Rede tentar acessar os pontos de distribuição no grupo **Escritório 2**. Ou seja, o computador portátil permanecerá no grupo de administração que corresponde ao escritório inicial, mas o computador portátil usará o ponto de distribuição do escritório onde estiver fisicamente localizado no momento.

Hierarquia de políticas, usando perfis de política

Essa seção fornece informações sobre como aplicar políticas aos dispositivos em grupos de administração. Esta seção também fornece informações sobre os perfis da política.

Hierarquia de políticas

No Kaspersky Security Center Linux, você usa políticas para definir uma coleção única de configurações para múltiplos dispositivos. Por exemplo, o escopo do aplicativo P definido para o grupo de administração G inclui dispositivos gerenciados com o aplicativo P instalado o que foi implementado no grupo G e em todos dos seus subgrupos, exceto para os subgrupos onde a caixa de seleção **Herdar do grupo de origem** estiver desmarcada nas propriedades.

Uma política se diferencia de qualquer configuração local pelos ícones de cadeado (🔒) ao lado de suas configurações. Se uma configuração (ou um grupo de configurações) estiver bloqueada nas propriedades da política, será necessário, em primeiro lugar, usar essa configuração (ou o grupo de configurações) ao criar configurações efetivas e, em segundo lugar, salvar as configurações ou o grupo de configurações no fluxo abaixo da política.

A criação das configurações efetivas em um dispositivo pode ser descrita como se segue: os valores de todas as configurações que não foram bloqueadas são tiradas da política, então elas são sobregravadas com os valores das configurações locais, e então a coleção resultante é sobregravada com os valores de configurações bloqueadas tiradas da política.

As políticas do mesmo aplicativo se afetam entre si através da hierarquia de grupos de administração: as configurações bloqueadas da política de fluxo acima substituem as mesmas políticas do fluxo abaixo.

Há uma política especial para usuários fora do escritório. Esta política entra em vigor em um dispositivo quando o dispositivo muda para o modo de fora do escritório. As políticas de ausência não afetam outras políticas através da hierarquia de grupos de administração.

Perfis da política

Aplicar políticas aos dispositivos somente através da hierarquia de grupos de administração pode ser inconveniente em muitas circunstâncias. Pode ser necessário criar diversas instâncias de uma política única que se diferem em uma ou duas configurações para diferentes grupos de administração e que sincronizam os conteúdos destas políticas no futuro.

Para ajudar você a evitar tais problemas, o Kaspersky Security Center Linux suporta os *perfis da política*. Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos de destino em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo cliente (computador ou dispositivo móvel). A ativação de um perfil modifica as configurações da política que estavam ativas no dispositivo antes do perfil ser ativado. As configurações modificadas assumem valores que foram especificados no perfil.

As seguintes restrições são atualmente impostas aos perfis da política:

- Uma política pode incluir no máximo 100 perfis.
- Um perfil da política não pode conter outros perfis.
- Uma política não pode conter configurações de notificação.

Conteúdo de um perfil

Um perfil da política contém as seguintes partes constituintes:

- Os perfis com nomes idênticos afetam uns aos outros por meio da hierarquia de grupos de administração com regras comuns.
- Subconjunto de configurações da política. Diferente da política, que contém todas as configurações, um perfil somente contém configurações que são de fato necessárias (configurações bloqueadas).
- Condição de ativação é uma expressão lógica com as propriedades do dispositivo. Um perfil está ativo (complementa a política) somente quando a condição de ativação de perfil se torna verdadeira. Em todos os outros casos, o perfil está inativo e é ignorado. As seguintes propriedades de dispositivo podem estar incluídas naquela expressão lógica:
  - Status do modo ausente.
  - Propriedades do ambiente de rede: nome da regra ativa para a conexão do Agente de Rede.
  - Presença ou ausência de identificadores especificados no dispositivo.
  - A alocação do dispositivo em uma unidade organizacional (UO) do Active Directory: explícita (o dispositivo está diretamente na UO especificada), ou implícito (o dispositivo está em uma UO, que está dentro da UO especificada em qualquer nível de aninhamento).
  - A associação do dispositivo no grupo de segurança do Active Directory (explícita ou implícita).
  - A associação do proprietário do dispositivo no grupo de segurança do Active Directory (explícita ou implícita).

- Desativando a caixa de seleção Perfil. Os perfis desativados sempre serão ignorados e as suas respetivas condições de ativação não serão verificadas.

- Prioridade do perfil. As condições de ativação de perfis diferentes são independentes, portanto vários perfis podem ser ativados simultaneamente. Se os perfis ativos contiverem coleções de configurações não de sobreposição, nenhum problema surgirá. No entanto, se dois perfis ativos contiverem valores diferentes da mesma configuração, uma ambiguidade ocorrerá. Esta ambiguidade deve ser evitada através das prioridades do perfil: o valor da variável ambígua será tomado do perfil que tiver a prioridade mais alta (aquele que é classificado como mais alto na lista de perfis).

O comportamento de perfis quando as políticas afetam uma a outra através da hierarquia

Os perfis com o mesmo nome são mesclados de acordo com as regras de mesclagem de política. Os perfis de uma política com fluxo acima têm uma prioridade mais alta do que os perfis de uma política de fluxo abaixo. Se a edição das configurações for proibida na política de fluxo acima (está bloqueada), a política de fluxo abaixo usa as condições de ativação da política de fluxo acima. Se a edição das configurações for permitida na política de fluxo acima, as condições de ativação do perfil da política de fluxo abaixo são usadas.

Como um perfil da política pode conter a propriedade **O dispositivo está offline** em sua condição de ativação, os perfis substituem completamente as políticas de usuário ausente, que não são mais compatíveis.

Uma política de usuário ausente pode conter perfis, mas os seus perfis somente podem ser ativados após que o dispositivo muda para o modo ausente.

Tarefas

O Kaspersky Security Center Linux gerencia os aplicativos de segurança da Kaspersky instalados nos dispositivos cliente criando e executando *tarefas*. As tarefas são necessárias para a instalação, inicialização e interrupção de aplicativos, verificação de arquivos, atualização de bancos de dados e módulos de software e para a realização de outras ações em aplicativos.

As tarefas de um aplicativo específico podem ser criadas apenas se o plugin de gerenciamento desse aplicativo estiver instalado.

As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

As seguintes tarefas que são realizadas no Servidor de Administração:

- Distribuição automática de relatórios

- Baixar atualizações no repositório do Servidor de Administração

- Backup de dados do Servidor de Administração

- Manutenção do banco de dados

Os seguintes tipos de tarefas são executados nos dispositivos:

- *Tarefas locais* – Tarefas que são executadas em um dispositivo específico

  As tarefas locais podem ser modificadas pelo administrador, usando o Kaspersky Security Center Web Console ou por um usuário de um dispositivo remoto (por exemplo, por meio da interface do aplicativo de segurança). Se uma tarefa local tiver sido modificada simultaneamente pelo administrador e pelo usuário de um dispositivo gerenciado, as modificações feitas pelo administrador entrarão em vigor porque elas têm uma maior prioridade.

- *Tarefas de grupo* – Tarefas que são executadas em todos os dispositivos de um grupo específico

  Salvo de especificado de outra maneira nas propriedades de tarefa, uma tarefa de grupo também afeta todos os subgrupos do grupo selecionado. Uma tarefa de grupo também afeta (opcionalmente) os dispositivos que foram conectados aos Servidores de Administração secundários e virtuais implementados no grupo ou em algum dos seus subgrupos.

- *Tarefas globais* – Tarefas que são realizadas em um conjunto de dispositivos, independentemente se os mesmos estão incluídos em qualquer grupo

Para cada aplicativo, você pode criar qualquer número de tarefas de grupo, tarefas globais ou tarefas locais.

Você pode efetuar alterações nas configurações de tarefas, exibir o andamento das tarefas, copiar, exportar, importar e excluir tarefas.

Uma tarefa é iniciada em um dispositivo cliente somente se um aplicativo para o qual a tarefa foi criada estiver sendo executado.

Os resultados das tarefas são salvos no log de eventos do Syslog e no log de eventos do Kaspersky Security Center Linux, tanto centralmente no Servidor de Administração como localmente em cada dispositivo.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Regras de migração de dispositivos

Recomendamos definir a alocação automática de dispositivos em grupos de administração através das *regras de migração de dispositivos*. Uma regra para migrar dispositivo compõe-se de três partes principais: um nome, uma condição de execução (expressão lógica com os atributos de dispositivo) e um grupo de administração alvo. Uma regra move um dispositivo para o grupo de administração alvo se os atributos do dispositivo atendam a condição de execução da regra.

Todas as regras para migrar dispositivo têm prioridades. O Servidor de Administração verifica os atributos do dispositivo quanto a se eles atendem a condição de execução de cada regra, na ordem ascendente da prioridade. Se os atributos do dispositivo atenderem a condição de execução de uma regra, o dispositivo é movido para o grupo alvo, portanto o processamento de regra é completo para este dispositivo. Se os atributos do dispositivo atenderem as condições de múltiplas regras, o dispositivo é movido para o grupo alvo da regra com a prioridade mais alta (ou seja, ele tem a classificação mais alta na lista de regras).

As regras para migrar dispositivo podem ser criadas implicitamente. Por exemplo, nas propriedades de um pacote de instalação ou de uma tarefa de instalação remota, você pode especificar o grupo de administração para o qual o dispositivo deve ser movido após que Agente de Rede seja instalado nele. Além disso, as regras para migrar dispositivos podem ser criadas explicitamente pelo administrador do Kaspersky Security Center Linux na seção **Gerenciamento de ativos → Regras de migração**.

Por padrão, uma regra para mover dispositivo é destinada para a alocação inicial de uma só vez de dispositivos aos grupos de administração. A regra move os dispositivos do grupo dispositivos não atribuídos somente uma vez. Se um dispositivo foi movido uma vez por esta regra, a regra nunca mais o moverá novamente, mesmo se você devolver o dispositivo ao grupo dispositivos não atribuídos manualmente. Esta é a forma recomendada de aplicar regras para mover.

Você pode migrar dispositivos que já foram alocados à alguns dos grupos de administração. Para fazer isso, nas propriedades de uma regra, desmarque a caixa de seleção **Somente mover os dispositivos que não pertencem a um grupo de administração**.

Aplicar regras para mover aos dispositivos que já foram alocados à alguns dos grupos de administração, aumenta significativamente a carga do Servidor de Administração.

A caixa de seleção **Somente mover os dispositivos que não pertencem a um grupo de administração** é bloqueada nas propriedades das regras de movimentação criadas automaticamente. As regras são criadas ao adicionar a tarefa *Instalar aplicativo remotamente* ou ao criar um pacote de instalação independente.

Você pode criar uma regra para mover que iria afetar um único dispositivo repetidamente.

Nós recomendamos com ênfase que você evite mover um dispositivo único de um grupo para outro repetidamente (por exemplo, para poder aplicar uma política especial àquele dispositivo, executar uma tarefa de grupo especial, ou atualizar o dispositivos através de um ponto de distribuição específico).

Tais cenários não são compatíveis, porque eles aumentam a carga no Servidor de Administração e o tráfego da rede para um grau extremo. Estes cenários também estão em conflito com os princípios operacionais do Kaspersky Security Center Linux (em particular na área de direitos de acesso, eventos e relatórios). Outra solução deve ser encontrada, por exemplo, por meio do uso de perfis de política, tarefas para seleções de dispositivo e atribuição de Agentes de Rede de acordo com o cenário padrão.

Categorização de software

A ferramenta principal para monitorar a execução dos aplicativos são as *categorias da Kaspersky* (aqui referidas como *categorias da KL*). As categorias da KL ajudam os administradores do Kaspersky Security Center Linux a simplificar o suporte da categorização de software e minimizar o tráfego indo para os dispositivos gerenciados.

As categorias de usuário somente devem ser criadas para aplicativos que não podem ser classificados em nenhuma das categorias da KL existentes (por exemplo, para o software criado de forma personalizada). As categorias de usuário são criadas com base em um pacote de instalação do aplicativo (MSI) ou uma pasta com pacotes de instalação.

Se uma grande coleção de software estiver disponível, que não foi categorizada através de categorias da KL, pode ser útil criar uma categoria automaticamente atualizada. Os checksums de arquivos executáveis serão automaticamente adicionados a esta categoria em cada modificação da pasta que contém os pacotes de distribuição.

Cópia backup e restauração das configurações do Servidor de Administração

O backup das configurações do Servidor de Administração e de seu banco de dados é executado pela tarefa de backup e com o utilitário klbackup. Uma cópia de backup inclui todas as principais configurações e objetos pertencentes ao Servidor de Administração, como certificados, chaves primárias para criptografia de unidades em dispositivos gerenciados, chaves para várias licenças, estrutura de grupos de administração com todo o seu conteúdo, tarefas, políticas etc. Com uma cópia de backup, é possível recuperar a operação de um Servidor de Administração o mais rápido possível, gastando de uma dúzia de minutos a algumas horas nisso.

Se nenhuma cópia de backup estiver disponível, uma falha pode levar a uma perda irrevogável de certificados e de todas as configurações do Servidor de Administração. Isto exigirá reconfigurar o Kaspersky Security Center Linux do zero e executar a implementação inicial do Agente de Rede novamente na rede da organização. Todas as chaves primárias para a criptografia das unidades em dispositivos gerenciados também serão perdidas, arriscando a perda irrevogável dos dados criptografados nos dispositivos com Kaspersky Endpoint Security. Portanto, não negligencie os backups regulares do Servidor de Administração usando a tarefa de backup padrão.

O assistente de início rápido cria uma tarefa de backup das configurações do Servidor de Administração que é iniciada todos os dias às 4h da manhã. Por padrão, as cópias de backup são salvas na pasta /var/opt/kaspersky/KSC_Backups*.

Como uma cópia de backup contém dados importantes, a tarefa de backup e o utilitário klbackup fornecem a proteção por senha das cópias backup. Por padrão, a tarefa de backup é criada com uma senha em branco. Você deve definir uma senha nas propriedades da tarefa de backup. Negligenciar este requisito causa uma situação em que todas as chaves de certificados do Servidor de Administração, as chaves para as licenças e as chaves primárias para a criptografia de unidades em dispositivos gerenciados permanecem não criptografadas.

Além do backup regular, você também deve criar uma cópia de backup antes de cada mudança significativa, incluindo a instalação de atualizações e patches do Servidor de Administração.

A restauração de uma cópia de backup é executada com o utilitário klbackup em uma instância operável do Servidor de Administração que acaba de ser instalado e que tenha a mesma versão (ou posterior) para o qual a cópia de backup foi criada.

A instância do Servidor de Administração na qual a restauração será executada deve usar um DBMS do mesmo tipo e da mesma versão ou posterior. A versão do Servidor de Administração pode ser a mesma (com uma correção idêntica ou posterior), ou posterior.

Esta seção descreve os cenários padrão para restaurar as configurações e objetos do Servidor de Administração.

Um dispositivo com o Servidor de Administração está inoperável

Se um dispositivo com o Servidor de Administração estiver inoperável devido a uma falha, você é recomendado a executar as seguintes ações:

- O novo Servidor de Administração deve receber o mesmo nome DNS.

  Se um endereço IP estático foi definido no pacote de instalação do Agente de Rede quando os Agentes de Rede foram implementados, você também deve atribuir o mesmo endereço IP ao novo Servidor de Administração. Como alternativa, é possível usar o endereço de conexão que determina o Servidor de Administração ao qual o Agente de Rede se conecta (esse endereço pode ser obtido em dispositivos gerenciados usando o utilitário klnagchk).

- No arquivo de configuração do IAM `var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` , para o `server_iam.ksc_address`, defina exatamente o mesmo endereço do Servidor de Administração especificado no Nome Alternativo da Entidade (SAN) do certificado do Servidor de Administração aplicado anteriormente. Consulte o seguinte artigo para obter informações: Adicionar o endereço do Servidor de Administração à configuração do Servidor IAM.

- Instale o Servidor de Administração, usando um DBMS do mesmo tipo ou da mesma (ou posterior) versão. Você pode instalar a mesma versão do Servidor com a mesma (ou posterior) correção ou uma versão posterior. Após a instalação, não execute a configuração inicial por meio do assistente.

- Execute o utilitário klbackup e realize a restauração. Reinstale o Web Console após a conclusão da restauração.

As configurações do Servidor de Administração ou o do banco de dados estão corrompidas

Se o Servidor de Administração estiver inoperável devido a configurações ou aos bancos de dados corrompidas (p. ex., após uma oscilação de corrente), você é recomendado a usar o seguinte cenário de restauração:

1. Verifique o sistema de arquivos no dispositivo danificado.

2. Desinstale a versão inoperável do Servidor de Administração.

3. Reinstale o Servidor de Administração usando um DBMS do mesmo tipo e da mesma (ou posterior) versão. Você pode instalar a mesma versão do Servidor com a mesma (ou posterior) correção ou uma versão posterior. Após a instalação, não execute a configuração inicial por meio do assistente.

4. Execute o utilitário klbackup e realize a restauração.

É proibido restaurar o Servidor de Administração usando qualquer outro modo que não seja através do utilitário klbackup.

Qualquer tentativa de restaurar o Servidor de Administração através de software de terceiros levará inevitavelmente a dessincronização dos dados nos nós do aplicativo Kaspersky Security Center Linux distribuído e, consequentemente, ao funcionamento impróprio do aplicativo.

Sobre a configuração de perfis de conexão para usuários ausentes

Os usuários ausentes de laptops (aqui também referidos como "dispositivos") podem precisar alterar o método da conexão a um Servidor de Administração ou alternar entre Servidores de Administração dependendo da localização atual do dispositivo na rede corporativa.

Usar endereços diferentes de um Servidor de Administração único

Os dispositivos com o Agente de Rede instalado podem conectar-se ao Servidor de Administração da intranet da organização ou a partir da Internet. Esta situação pode necessitar que o Agente de Rede use endereços diferentes para a conexão ao Servidor de Administração: o endereço do Servidor de Administração externo para a conexão com a Internet e o endereço do Servidor de Administração interno para a conexão da rede interna.

Para fazer isto, você deve adicionar um perfil (para a conexão ao Servidor de Administração a partir da Internet) à política do Agente de Rede. Adicione o perfil nas propriedades da política (Seção **Conectividade**, subsecção **Perfis de conexão**). Na janela de criação do perfil, você deve desativar a opção **Usar somente para receber atualizações** e selecionar a opção **Sincronizar as configurações de conexão com as configurações do Servidor de Administração especificadas nesse perfil**. Se você usa um gateway de conexão para acessar o Servidor de Administração (por exemplo, em uma configuração do Kaspersky Security Center Linux que está descrita em No acesso à Internet: Agente de Rede como um gateway de conexão em DMZ), deverá especificar o endereço do gateway de conexão no campo correspondente do perfil de conexão.

Alternar entre Servidores de Administração dependendo da rede atual

Se a organização tiver múltiplos escritórios com diferentes Servidores de Administração e alguns dispositivos com o Agente de Rede instalado se moverem entre eles, você precisa do Agente de Rede para conectar-se ao Servidor de Administração da rede local no escritório onde o dispositivo está atualmente localizado.

Neste caso, você deve criar um perfil para a conexão ao Servidor de Administração nas propriedades da política do Agente de Rede de cada um dos escritórios, exceto para o escritório doméstico onde o Servidor de Administração mestre original esteja localizado. Você deve especificar os endereços dos Servidores de Administração em perfis de conexão e ativar ou desativar a opção **Usar somente para receber atualizações**:

- Selecione a opção se você precisar que o Agente de Rede seja sincronizado com o Servidor de Administração mestre, usando o Servidor local somente para baixar as atualizações.
- Desative a opção se for necessário que o Agente de Rede seja gerenciado completamente pelo Servidor de Administração local.

Após isso, você deve definir as condições da troca para os perfis recém criados: ao menos uma condição de cada um dos escritórios, exceto para o escritório doméstico. Cada propósito de condição consiste na detecção de itens que são específicos para o ambiente de rede de um escritório. Se uma condição for verdadeira, o perfil correspondente é ativado. Se nenhuma das condições for verdadeira, o Agente de Rede alterna para o Servidor de Administração mestre.

Sobre a mudança do Agente de Rede para outro servidor de Administração

O Kaspersky Security Center Linux oferece a opção de trocar o Agente de Rede em um dispositivo cliente para outros Servidores de Administração, caso as seguintes configurações da rede tenham sido alteradas:

- **Condição do endereço do servidor DHCP** – O endereço IP do servidor Dynamic Host Configuration Protocol (DHCP) da rede foi alterado.

  A configuração **Condição do endereço do servidor DHCP** não está disponível no momento.

- **Adicionar condição para o endereço do gateway de conexão padrão** – O endereço do gateway da rede principal foi alterado.
- **Condição para o domínio DNS** – O sufixo DNS da sub-rede foi alterado.
- **Condição do endereço do servidor DNS** – O endereço IP do servidor DNS da rede foi alterado.
- **Condição do endereço do servidor WINS** – O endereço IP do servidor WINS da rede foi alterado. Essa configuração está disponível apenas para dispositivos que executam o Windows.
- **Condição da capacidade de resolução de nome** – O nome DNS ou NetBIOS do dispositivo cliente foi alterado.
- **Condição para a sub-rede** – Alterações no endereço e máscara da rede.
- **Condição de acessibilidade do Domínio do Windows** – Altera o status do domínio do Windows ao qual um dispositivo cliente está conectado. Essa configuração está disponível apenas para dispositivos que executam o Windows.
- **Condição de acessibilidade do endereço de conexão SSL** – O dispositivo cliente pode ou não (dependendo da opção selecionada) estabelecer uma conexão SSL com um servidor especificado (nome:porta). É necessário utilizar um servidor dedicado com software capaz de lidar com alta carga e com solicitações frequentes de conexão do Agente de Rede. Não especifique a porta do Servidor de Administração. Para cada servidor, é possível especificar adicionalmente um certificado SSL. Nesse caso, o Agente de Rede verifica o certificado do servidor, além de verificar a capacidade de uma conexão SSL. Se o certificado não for correspondente, a conexão falhará.

As configurações iniciais da conexão do Agente de Rede ao Servidor de Administração são definidas durante a instalação do Agente de Rede. Após isso, se regras de troca do Agente de Rede para outros Servidores de Administração tiverem sido criadas, o Agente de Rede responde às alterações nas configurações de rede, como segue:

- Se as configurações de rede estiverem em conformidade com uma das regras criadas, o Agente de Rede conecta-se ao Servidor de Administração especificado nessa regra. Os aplicativos instalados nos dispositivos cliente mudam para as políticas de ausência de escritório, desde que tal comportamento esteja ativado por uma regra.

- Se nenhuma das regras se aplicarem, o Agente de Rede retorna para as configurações padrão de conexão ao Servidor de Administração especificadas durante a instalação. Os aplicativos instalados nos dispositivos cliente alternam de volta para as políticas ativas.

- Se o Servidor de Administração não estiver acessível, o Agente de Rede usa as políticas de ausência de escritório.

O Agente de Rede troca para a política de ausência somente se a opção **Ativar modo ausente quando o Servidor de Administração não estiver disponível** estiver ativada nas configurações da política do Agente de Rede.

As configurações da conexão do Agente de Rede ao Servidor de Administração são salvas em um perfil de conexão. No perfil de conexão, você poderá criar regras de troca de dispositivos clientes para políticas de ausência de escritório, assim como configurar o perfil para que ele possa ser usado apenas para baixar atualizações.

Criando um perfil de conexão para usuários ausentes

Para criar um perfil para a conexão do Agente de Rede ao Servidor de Administração para usuários fora do escritório:

1. Caso queira criar um perfil de conexão para um grupo de dispositivos gerenciados, abra a política do Agente de Rede desse grupo. Para fazer isso, execute como seguintes ações:

   a. No menu principal, vá para **Gerenciamento de ativos** → **Políticas**.

   b. Selecione o grupo de administração para o qual o perfil de conexão deve ser criado:

      - Para o grupo raiz, é possível prosseguir para a próxima etapa.

      - Para um subgrupo, clique no botão **Mostrar a hierarquia** na parte superior da página e, na janela que é exibida, clique no nome do subgrupo desejado.

      O caminho para o grupo selecionado é exibido na parte superior da página. Caso necessário, é possível clicar em um link com o nome do grupo de administração para ir até o grupo. Por padrão, o último link no caminho fica inativo. Além disso, é possível fechar a janela de hierarquia clicando no botão **Ocultar a hierarquia**.

   c. Adicione a política do Agente de Rede para o grupo de dispositivos gerenciados. Caso já tenha sido criado, clique no nome da política do Agente de Rede para abrir as propriedades da política.

2. Caso queira criar um perfil de conexão para um dispositivo gerenciado específico, faça o seguinte:

   a. No menu principal, vá para **Gerenciamento de ativos → Dispositivos gerenciados**.

   b. Clique no nome do dispositivo gerenciado.

   c. Na janela exibida de propriedades do dispositivo gerenciado, acesse a guia **Aplicativos**.

   d. Clique no nome da política do Agente de Rede que se aplique somente ao dispositivo gerenciado selecionado.

3. Na janela de propriedades aberta, acesse **Configurações do aplicativo → Conectividade → Perfis de conexão**.

4. Na seção **Perfis de conexão do Servidor de Administração**, clique no botão **Adicionar**.

   Por padrão, a lista de perfis de conexão contém os perfis <Modo offline> e <Servidor de Administração principal>. O perfil não pode ser editado ou removido.

   O perfil <Modo offline> não especifica nenhum Servidor para conexão. Portanto, o Agente de Rede, quando alternado para esse perfil, não tentará fazer conexão com nenhum Servidor de Administração enquanto os aplicativos instalados nos dispositivos cliente forem executados sob políticas de ausência. O perfil <Modo offline> pode ser usado se os dispositivos estiverem desconectados da rede.

   O perfil <Servidor de Administração principal> especifica para a conexão o Servidor de Administração que foi selecionado durante a instalação do Agente de Rede. O perfil <Servidor de Administração principal> é aplicado quando um dispositivo for reconectado ao Servidor de Administração principal após que ele estava sendo executado em uma rede externa por algum tempo.

5. Na janela **Configurar perfil** que se abre, configure o perfil de conexão:

   - **Nome do perfil**

     No campo de entrada, é possível consultar ou alterar o nome do perfil de conexão.

   - **Endereço do Servidor de Administração**

     O endereço do Servidor de administração ao qual o dispositivo cliente deve conectar-se durante a ativação do perfil.

   - **Número da porta**

     O número da porta que é usada para conexão.

   - **Porta SSL**

     Número da porta para conexão com, uso do protocolo SSL.

   - **Usar conexão SSL**

     Se esta opção estiver ativada, a conexão é estabelecida através de uma porta segura, com o protocolo SSL.

     Por padrão, esta opção está ativada. Recomendamos não desativar a opção para que a conexão permaneça segura.

- Selecione a opção **Usar o servidor proxy** caso queira usar um servidor proxy para se conectar com a Internet. Se essa opção estiver selecionada, os campos estarão disponíveis para inserir configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:

  - **Endereço**

    Endereço do servidor proxy usado para conexão do Kaspersky Security Center Linux à Internet.

  - **Número da porta**

    Número da porta pela qual a conexão proxy do Kaspersky Security Center Linux será estabelecida.

  - **Autenticação do servidor proxy**

    Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

  - **Nome do usuário**

    Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

  - **Senha**

    A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

    Para ver a senha inserida, mantenha pressionado o botão **Mostrar** pelo tempo que você desejar.

- **Endereço do gateway de conexão**

  O endereço do gateway através do qual os dispositivos cliente se conectam com o Servidor de Administração.

- **Ativar modo ausente quando o Servidor de Administração não estiver disponível**

  Marque a caixa de seleção para permitir aos aplicativos instalados em um dispositivo cliente usar perfis da política para dispositivos no modo ausente, assim como políticas de ausência, no momento de qualquer tentativa de conexão, se o Servidor de Administração não estiver disponível. Se a política de ausência do escritório não estiver definida para o aplicativo, a política ativa será usada.

  Se esta opção estiver desativada, os aplicativos usarão as políticas ativas.

  Por padrão, esta caixa de seleção está desmarcada.

- **Usar somente para receber atualizações**

  Se esta opção estiver ativada, o perfil somente será usado para baixar atualizações pelos aplicativos instalados no dispositivo cliente. Para outras operações, a conexão ao Servidor de Administração será estabelecida com as configurações de conexão iniciais definidas durante a instalação do Agente de Rede.

  Por padrão, esta opção está ativada.

- **Sincronizar as configurações de conexão com as configurações do Servidor de Administração especificadas nesse perfil**

  Se esta opção estiver ativada, o Agente de Rede se conecta ao Servidor de Administração utilizando as configurações especificadas nas propriedades do perfil.

  Se esta opção estiver desativada, o Agente de Rede se conecta ao Servidor de Administração utilizando as configurações originais que foram especificadas durante a instalação.

  Essa opção estará disponível se a opção **Usar somente para receber atualizações** estiver desabilitada.

Por padrão, esta opção está desativada.

Um perfil para conectar o Agente de Rede ao Servidor de Administração é criado para usuários fora do escritório. Quando o Agente de Rede se conectar ao Servidor de Administração usando esse perfil, os aplicativos instalados no dispositivo cliente usarão as políticas para dispositivos no modo ausente ou políticas de ausência.

Acesso remoto aos dispositivos gerenciados

Esta seção fornece informações sobre o acesso remoto aos dispositivos gerenciados.

Uso da opção "Não desconectar do Servidor de Administração" para fornecer conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração

Caso os servidores push não sejam usados, o Kaspersky Security Center Linux não fornece conectividade contínua entre dispositivos gerenciados e o Servidor de Administração. Os Agentes de Rede em dispositivos gerenciados periodicamente estabelecem conexões e sincronizam com o Servidor de Administração. O intervalo entre as sessões de sincronização é definido em uma política do Agente de Rede. Caso seja necessária uma sincronização antecipada, o Servidor de Administração (ou um ponto de distribuição, se estiver em uso) enviará um pacote de rede assinado por uma rede IPv4 ou IPv6 para a porta UDP do agente de rede. Por padrão, o número de porta é 15000. Caso nenhuma conexão via UDP seja possível entre o Servidor de Administração e um dispositivo gerenciado por qualquer motivo, a sincronização será executada na próxima conexão regular entre o agente de rede e o Servidor de Administração dentro do intervalo de sincronização.

Algumas operações não podem ser executadas sem uma conexão antecipada entre o Agente de Rede e o Servidor de Administração, como executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado. Para resolver esse problema, caso os servidores push não estejam sendo usados, será possível usar a opção **Não desconectar do Servidor de Administração** para se certificar de que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração.

Para fornecer conexão contínua entre um dispositivo gerenciado e o Servidor de Administração:

1. No menu principal, vá para **Gerenciamento de ativos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo necessário.

3. Na janela de propriedades do dispositivo, na seção **Geral**, ative a opção **Não desconectar do Servidor de Administração**.

A conectividade contínua é estabelecida entre o dispositivo gerenciado e o Servidor de Administração.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Sobre verificar o tempo de conexão entre um dispositivo e o Servidor de Administração

Para desligar um dispositivo, o Agente de Rede notifica o Servidor de Administração sobre este evento. No Kaspersky Security Center Web Console, esse dispositivo é exibido como desligado. No entanto, o Agente de Rede não pode notificar o Servidor de Administração sobre todos tais eventos. O Servidor de Administração, portanto, periodicamente analisa o atributo **Conectado ao Servidor de Administração** (o valor deste atributo é exibido no Kaspersky Security Center Web Console, nas propriedades do dispositivo, na seção **Geral**) para cada dispositivo e compara-o com o intervalo de sincronização a partir das configurações atuais do Agente de Rede. Se um dispositivo não tiver respondido ao longo de mais de três intervalos de sincronização sucessivos, aquele dispositivo é marcado como desligado.

Sobre a sincronização forçada

Embora o Kaspersky Security Center Linux automaticamente sincronize o status, configurações, tarefas e políticas para dispositivos gerenciados, em alguns casos o administrador precisa saber exatamente se a sincronização já foi executada para um dispositivo especificado no presente momento.

A janela de propriedades de um dispositivo gerenciado contém o botão **Forçar a sincronização**. Quando o Kaspersky Security Center Linux executa este comando de sincronização, o Servidor de Administração tenta se conectar ao dispositivo. Se esta tentativa for bem sucedida, a sincronização forçada será executada. Caso contrário, a sincronização será forçada somente após a próxima conexão entre o Agente de Rede e o Servidor de Administração.

Guia de dimensionamento

Esta seção fornece informações sobre o dimensionamento do Kaspersky Security Center Linux.

Sobre este Guia

O guia de dimensionamento do Kaspersky Security Center Linux (também conhecido como "Kaspersky Security Center") é destinado a profissionais que instalam e administram o Kaspersky Security Center, assim como a todos os profissionais que fornecem suporte técnico para as organizações que usam o Kaspersky Security Center.

Todas as recomendações e os cálculos são fornecidos para as redes nas quais o Kaspersky Security Center gerencia a proteção dos dispositivos com o software da Kaspersky instalado.

Para obter e manter o desempenho ideal sob a variação de condições operacionais, você deverá levar em conta o número de dispositivos na rede, a topologia da rede e o conjunto de recursos do Kaspersky Security Center de que você necessita.

Esta Guia fornece as seguintes informações:

- Limitações do Kaspersky Security Center
- Cálculos para os nós-chave do Kaspersky Security Center (Servidores de Administração e pontos de distribuição):
    - Requisitos de hardware para Servidores de Administração e pontos de distribuição
    - Cálculo do número e hierarquia de Servidores de Administração
    - Cálculo do número e da configuração de pontos de distribuição
- Configuração de registro de evento no banco de dados dependendo do número de dispositivos na rede
- Práticas recomendadas comuns para otimização de desempenho
- Configuração de tarefas específicas objetivadas ao ótimo desempenho do Kaspersky Security Center
- Taxa de tráfego (carga da rede) entre Servidor de Administração do Kaspersky Security Center e cada dispositivo protegido

A consulta deste guia é recomendada nos seguintes casos:

- Planejando recursos antes da instalação do Kaspersky Security Center
- Planejando mudanças significativas à escala da rede na qual o Kaspersky Security Center será implementado
- Ao mudar do Kaspersky Security Center em um segmento de rede limitado (um ambiente de teste) para a implantação em larga escala do Kaspersky Security Center na rede corporativa
- Ao efetuar modificações no conjunto de recursos do Kaspersky Security Center utilizados

Limitações do Kaspersky Security Center Linux

A tabela a seguir exibe as limitações da versão atual do Kaspersky Security Center Linux.

Limitações do Kaspersky Security Center Linux

Tipo de limitação	Valor
Número máximo de dispositivos gerenciados por Servidor de Administração	50.000
Número máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada	300
Número máximo de grupos de administração	10.000
Número de eventos a armazenar	45.000.000
Número máximo de políticas	2000
Número máximo de tarefas	2000
Número máximo de perfis em uma política	100
Número máximo de Servidores de Administração secundários em um Servidor de Administração principal único	500
Número máximo de Servidores de Administração virtuais	500
Número máximo de dispositivos que um ponto de distribuição pode atender	10.000
Número máximo de dispositivos que podem usar um único gateway de conexão	10.000, incluindo dispositivos móveis
Número máximo de dispositivos móveis por Servidor de Administração	100.000, menos o número de dispositivos gerenciados estacionários

Cálculos para os Servidores de Administração

Esta seção fornece o os requisitos de software e hardware para dispositivos usados como Servidores de Administração. Também são fornecidas recomendações para calcular o número e a hierarquia de Servidores de Administração dependendo da configuração da rede da organização.

Recomendamos que, após instalar o Servidor de Administração e o DBMS nos dispositivos, você instale o Kaspersky Endpoint Security for Linux neles. Para obter os requisitos de hardware do Kaspersky Endpoint Security, consulte a Ajuda do Kaspersky Endpoint Security for Linux.

A carga criada pelo Kaspersky Endpoint Security for Linux quando integrado ao Managed Detection and Response e ao Kaspersky Endpoint Detection and Response Expert (on-premise) não é levada em conta nos cálculos da instalação simultânea do Kaspersky Security Center Linux e do KES_LIN>.

Cálculo de recursos de hardware para o Servidor de Administração

Esta seção contém cálculos que fornecem a orientação para planejar recursos de hardware para o Servidor de Administração.

Requisitos de hardware para o DBMS e para o Servidor de Administração

As tabelas a seguir fornecem os requisitos mínimos de hardware recomendados para um DBMS e para um Servidor de Administração obtidos durante os testes. Para obter uma lista completa de sistemas operacionais e DBMSs suportados, refira-se à lista de requisitos de hardware e software.

Você precisa ativar o arquivo de troca no dispositivo com o Servidor de Administração instalado. O tamanho mínimo do arquivo de troca deve ser 1,5 vez maior que o volume da RAM.

Depois de instalar o Servidor de Administração e o DBMS em um dispositivo, recomendamos instalar o Kaspersky Endpoint Security for Linux.
Para a instalação simultânea, é necessário ter no mínimo 300 IOPS, além de acrescentar aos requisitos do Servidor de Administração 1,5 GB de RAM e 15% à CPU.
Para obter os requisitos de hardware do Kaspersky Endpoint Security, consulte a Ajuda do Kaspersky Endpoint Security for Linux.

Para obter informações sobre as configurações de segurança necessárias para trabalhar com o Kaspersky Security Center Linux, consulte a Ajuda do Kaspersky Endpoint Security for Linux.

A rede inclui 50,000 dispositivos

Configuração do dispositivo com o Servidor de Administração instalado

Hardware	Valor
CPU	8 núcleos (12 núcleos recomendados), 2500 MHz
RAM	16 GB
Espaço em disco	300 GB, 150 IOPS ou superior

Configuração do dispositivo com o PostgreSQL DBMS instalado

Hardware	Valor
CPU	16 núcleos, 2500 MHz
RAM	32 GB
Espaço em disco	300 GB, 150 IOPS ou superior

Configuração de nós para um cluster de failover

Hardware	Valor
CPU	8 núcleos (12 núcleos recomendados), 2500 MHz
RAM	16 GB
Espaço em disco	300 GB, 150 IOPS ou superior
Controlador de interface de rede	1 Gbps

A configuração do dispositivo que tem o Servidor de Administração e o PostgreSQL DBMS instalados

Hardware	Valor
CPU	24 núcleos (28 núcleos recomendados), 2500 MHz
RAM	48 GB
Espaço em disco	600 GB, 300 IOPS ou superior

A rede inclui 30,000 dispositivos

Configuração do dispositivo com o Servidor de Administração instalado

Hardware	Valor
CPU	6 núcleos (8 núcleos recomendados), 2500 MHz
RAM	12 GB
Espaço em disco	200 GB, 150 IOPS ou superior

Configuração do dispositivo com o PostgreSQL DBMS instalado

Hardware	Valor
CPU	12 núcleos, 2500 MHz
RAM	22 GB
Espaço em disco	250 GB, 150 IOPS ou superior

Configuração de nós para um cluster de failover

Hardware	Valor
CPU	6 núcleos (8 núcleos recomendados), 2500 MHz
RAM	12 GB
Espaço em disco	200 GB, 150 IOPS ou superior
Controlador de interface de rede	1 Gbps

A configuração do dispositivo que tem o Servidor de Administração e o PostgreSQL DBMS instalados

Hardware	Valor
CPU	16 núcleos (20 núcleos recomendados), 2500 MHz
RAM	34 GB
Espaço em disco	450 GB, 300 IOPS ou superior

A rede inclui 10,000 dispositivos

Configuração do dispositivo com o Servidor de Administração instalado

Hardware	Valor
CPU	4 núcleos (6 núcleos recomendados), 2500 MHz
RAM	8 GB
Espaço em disco	100 GB, 150 IOPS ou superior

Configuração do dispositivo com o PostgreSQL DBMS instalado

Hardware	Valor
CPU	6 núcleos, 2500 MHz
RAM	10 GB
Espaço em disco	200 GB, 150 IOPS ou superior

Configuração de nós para um cluster de failover

Hardware	Valor
CPU	4 núcleos (6 núcleos recomendados), 2500 MHz
RAM	8 GB
Espaço em disco	100 GB, 150 IOPS ou superior
Controlador de interface de rede	1 Gbps

A configuração do dispositivo que tem o Servidor de Administração e o PostgreSQL DBMS instalados

Hardware	Valor
CPU	8 núcleos (14 núcleos recomendados), 2500 MHz
RAM	18 GB
Espaço em disco	300 GB, 300 IOPS ou superior

A rede inclui 1000 dispositivos

Configuração do dispositivo com o Servidor de Administração instalado

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	6 GB
Espaço em disco	10 GB, 150 IOPS ou superior

Configuração do dispositivo com o PostgreSQL DBMS instalado

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	4 GB
Espaço em disco	20 GB, 150 IOPS ou superior

Configuração de nós para um cluster de failover

Hardware	Valor
CPU	2 núcleos, 2500 MHz
RAM	6 GB
Espaço em disco	10 GB, 150 IOPS ou superior
Controlador de interface de rede	1 Gbps

A configuração do dispositivo que tem o Servidor de Administração e o PostgreSQL DBMS instalados

Hardware	Valor
CPU	4 cores, 2.500 MHz
RAM	10 GB
Espaço em disco	30 GB, 300 IOPS ou superior

Os testes foram executados sob as seguintes configurações:

- A atribuição automática de Agentes de Atualização é ativada no Servidor de Administração, ou os pontos de distribuição são atribuídos manualmente de acordo com tabela recomendada.
- O PostgreSQL DBMS não inclui nenhuma extensão além de plpgsql.

No dispositivo com o DBMS instalado, o banco de dados consome aproximadamente 100 GB de espaço em disco e o log de transações consome aproximadamente 200 GB de espaço em disco.

Cálculo do espaço do banco de dados

A quantidade aproximada de espaço deve ser reservada no banco de dados pode ser calculado usando a seguinte fórmula:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

onde:

- C é o número de dispositivos.

  > Se os dispositivos gerenciados incluírem máquinas virtuais dinâmicas, C será a soma do número de dispositivos gerenciados não dinâmicos e do número de máquinas virtuais dinâmicas com o Agente de Rede criado entre duas execuções consecutivas da tarefa **Manutenção do Servidor de Administração**.

- E é o número de eventos a armazenar.
- A é o número total do objetos do Active Directory:
  - Contas de dispositivo
  - Contas de usuário
  - Contas dos grupos de segurança
  - Unidades organizacionais do Active Directory

  Se a verificação do Active Directory estiver desativada, A é considerado como igual a zero.
- N é o número médio de arquivos executáveis inventariados em um dispositivo de endpoint.
- F é o número de dispositivos de endpoint onde os arquivos executáveis foram inventariados.

Se você planejar ativar (nas configurações da política do Kaspersky Endpoint Security) a notificação do Servidor de Administração em aplicativos que você executa, precisará de uma quantidade adicional de (0.03 * C) gigabytes para armazenar no banco de dados as informações sobre os aplicativos em execução.

Durante a operação, um determinado *espaço não alocado* sempre estará presente no banco de dados. Portanto, o tamanho real do arquivo de banco de dados geralmente é aproximadamente duas vezes maior que a quantidade de espaço ocupado no banco de dados.

Não é recomendável definir o limite do tamanho do log de transações. Recomenda-se deixar o valor padrão do parâmetro MAXSIZE.

Cálculo do espaço em disco

O espaço em disco do Servidor de Administração necessário para a pasta /var/opt/kaspersky/klnagent_srv/ pode ser estimado aproximadamente usando a fórmula:

(724 * C + 0.15 * E + 0.17 * A), KB

onde:

- C é o número de dispositivos.

  Se os dispositivos gerenciados incluírem máquinas virtuais dinâmicas, C será a soma do número de dispositivos gerenciados não dinâmicos e do número de máquinas virtuais dinâmicas com o Agente de Rede criado entre duas execuções consecutivas da tarefa **Manutenção do Servidor de Administração**.

- E é o número de eventos a armazenar.
- A é o número total do objetos do Active Directory:
  - Contas de dispositivo
  - Contas de usuário
  - Contas dos grupos de segurança
  - Unidades organizacionais do Active Directory

Se a verificação do Active Directory estiver desativada, A é considerado como igual a zero.

Cálculo do número e configuração de Servidores de Administração

Para reduzir a carga do Servidor de Administração principal, você pode atribuir um Servidor de Administração separado à cada grupo de administração. O número de Servidores de Administração secundários não pode exceder 500 para um único Servidor de Administração principal.

Recomendamos que você crie a configuração dos Servidores de Administração em relação à configuração da sua rede corporativa.

Recomendações para conectar máquinas virtuais dinâmicas ao Kaspersky Security Center

As máquinas virtuais dinâmicas (também conhecidas como VMs dinâmicas) consomem mais recursos do que as máquinas virtuais estáticas.

Para obter mais informações sobre máquinas virtuais dinâmicas, consulte Suporte de máquinas virtuais dinâmicas.

Quando uma nova VM dinâmica é conectada, o Kaspersky Security Center Linux cria um registro ícone para ela no Kaspersky Security Center Web Console e a move para o grupo de administração. Depois disso, a VM dinâmica é adicionada ao banco de dados do Servidor de Administração. O Servidor de Administração está totalmente sincronizado com o Agente de Rede instalado nesta VM dinâmica.

Na rede de uma organização, o Agente de Rede cria as seguintes listas de rede para cada VM dinâmica:

- Hardware
- Software instalado
- Vulnerabilidades detectadas
- Eventos e listas de arquivos executáveis do componente de Controle de Aplicativos

O Agente de Rede transfere essas listas de rede para o Servidor de Administração. O tamanho das listas de rede depende dos componentes instalados na VM dinâmica e pode afetar o desempenho do Kaspersky Security Center Linux e do sistema de gerenciamento do banco de dados (DBMS). Observe que a carga pode crescer de forma não linear.

Após o usuário terminar de trabalhar com a VM dinâmica e desligá-la, esta máquina será removida da infraestrutura virtual e as entradas sobre esta máquina serão removidas do banco de dados do Servidor de Administração.

Todas essas ações consomem muitos recursos do banco de dados do Kaspersky Security Center Linux e do Servidor de Administração, e podem reduzir o desempenho do Kaspersky Security Center e do DBMS. Recomendamos conectar até 20 mil VMs dinâmicas no Kaspersky Security Center Linux.

É possível conectar mais de 20 mil VMs dinâmicas no Kaspersky Security Center Linux caso as VMs dinâmicas conectadas executem as operações padrão (por exemplo, atualizações do banco de dados) e caso consumam não mais que 80% da memória e 75 a 80% dos núcleos disponíveis.

Alterar configurações de política, software ou sistema operacional na VM dinâmica pode reduzir ou aumentar o consumo de recursos. O consumo de 80 a 95% dos recursos é considerado ideal.

Cálculos para pontos de distribuição e gateways de conexão

Esta seção fornece os requisitos de hardware para dispositivos usados como pontos de distribuição junto com recomendações sobre como calcular o número de pontos de distribuição e os gateways conexão dependendo da configuração da rede corporativa.

Requisitos para um ponto de distribuição

Os requisitos de hardware e software para pontos de distribuição baseados em Windows e Linux são descritos neste artigo.

Se quaisquer tarefas de instalação remota estiverem disponíveis no Servidor de Administração, o dispositivo com o ponto de distribuição também requer uma quantidade de espaço livre em disco que seja igual ao tamanho total dos pacotes de instalação a serem instalados.

Se uma ou múltiplas instâncias da tarefa para a instalação da atualização (patch) e de correção de vulnerabilidades estiverem pendentes no Servidor de Administração, o dispositivo com o ponto de distribuição também exigirá espaço livre adicional no disco que seja igual ao dobro do tamanho total de todos os patches a serem instalados.

Se você usar o esquema quando os pontos de distribuição receberem atualizações de bancos de dados e módulos de software do aplicativo diretamente dos servidores de atualização da Kaspersky, os pontos de distribuição deverão estar conectados à Internet.

Não é recomendado atribuir o Servidor de Administração como um ponto de distribuição, pois isso aumentará a carga nele.

Requisitos de hardware para pontos de distribuição baseados em Windows

Requisitos mínimos de hardware para pontos de distribuição baseados em Windows

Número de dispositivos clientes	CPU	RAM	RAM, com gerenciamento de patches ativado	Espaço em disco
10.000	4 cores, 2.500 MHz	8 GB	8 GB	120 GB
5 mil	4 cores, 2.500 MHz	6 GB	8 GB	120 GB
1000	2 núcleos, 2500 MHz	4 GB	8 GB	120 GB

Requisitos de hardware para pontos de distribuição baseados em Linux

Requisitos mínimos de hardware para pontos de distribuição baseados em Linux

Número de dispositivos clientes	CPU	RAM	Espaço em disco
10.000	4 cores, 2.500 MHz	10 GB	120 GB
5 mil	4 cores, 2.500 MHz	8 GB	120 GB
1000	2 núcleos, 2500 MHz	6 GB	120 GB

Calcular o número e a configuração de pontos de distribuição

Quanto mais dispositivos clientes uma rede contiver, mais pontos de distribuição ela exigirá. Recomendamos que você não desative a atribuição automática de pontos de distribuição. Quando a atribuição automática de pontos de distribuição estiver ativada, o Servidor de Administração atribui pontos de distribuição se o número de dispositivos clientes for bastante grande e define a sua configuração.

Usar pontos de distribuição exclusivamente atribuídos

Se você planejar usar determinados dispositivos específicos como pontos de distribuição (ou seja, servidores exclusivamente atribuídos), você pode optar por não utilizar a atribuição automática de pontos de distribuição. Neste caso, assegure-se de que os dispositivos aos quais você pretende tornar pontos de distribuição tenham volume suficiente de espaço livre em disco, não sejam desligados regularmente e estejam com o modo Suspenso desativado.

Número de pontos de distribuição dedicados em uma rede com um segmento de rede, dependendo do número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Número de pontos de distribuição dedicados em uma rede com vários segmentos de rede, dependendo do número de dispositivos na rede

Número de dispositivos cliente em cada segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10–100	1
Mais de 100	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Usar dispositivos clientes padrão (estações de trabalho) como pontos de distribuição

Se você planejar usar dispositivos clientes padrão (isto é, estações de trabalho) como pontos de distribuição, recomendamos atribuir pontos de distribuição, como mostrado nas tabelas abaixo, para evitar a carga excessiva dos canais de comunicação e do Servidor de Administração:

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém um segmento de rede único, com base no número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém vários segmentos de rede, com base no número de dispositivos na rede

Número de dispositivos cliente em cada segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10–30	1
31–300	2
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

Se um ponto de distribuição estiver desativado (ou não disponível por algum outro motivo), os dispositivos gerenciados no escopo poderão acessar o Servidor de Administração para as atualizações.

Cálculo do número de gateways de conexão

Se você planejar usar um gateway de conexão, recomendamos que designe um dispositivo especial para essa função.

Um gateway de conexão pode abranger no máximo 10 mil dispositivos gerenciados.

Registro de informações sobre eventos para tarefas e políticas

Esta seção fornece os cálculos associados com o armazenamento de evento no banco de dados do Servidor de Administração e oferece recomendações sobre como minimizar o número de eventos, portanto reduzindo a carga no Servidor de Administração.

Por padrão, as propriedades de cada tarefa e política fornecem o armazenamento de todos os eventos relativos à execução da tarefa e da obrigatoriedade da política.

No entanto, se uma tarefa for executada com bastante frequência (por exemplo, mais do que uma vez por semana) e em um número bem grande de dispositivos (por exemplo, mais de 10.000), o número de eventos pode resultar ser demasiado grande e os eventos podem inundar o banco de dados. Nesse caso, recomendamos selecionar uma das duas opções nas configurações da tarefa:

- **Salvar eventos relacionados ao progresso da tarefa**. Neste caso, o banco de dados somente recebe informações sobre inicialização, andamento e conclusão da tarefa (com êxito, com uma advertência ou erro) de cada dispositivo no qual a tarefa for executada.

- **Salvar apenas os resultados da execução da tarefa**. Neste caso, o banco de dados somente recebe informações sobre a conclusão da tarefa (com êxito, com um aviso ou erro) de cada dispositivo no qual a tarefa for executada.

Caso uma política tenha sido definida para um número bastante grande de dispositivos (por exemplo, mais de 10.000), o número de eventos também pode acabar sendo grande, e os eventos podem inundar o banco de dados. Neste caso, recomenda-se somente selecionar os eventos mais críticos nas configurações da política e ativar o seu registro. Você é aconselhado a desativar o registro de todos outros eventos.

Ao fazer isso, você reduzirá o número de eventos no banco de dados, aumentará a velocidade da execução dos cenários associados com a análise da tabela de eventos no banco de dados e abaixará o risco de que os eventos críticos sejam substituídos por um grande número de eventos.

Você também pode reduzir o período de armazenamento para eventos associados com uma tarefa ou política. O período padrão é de 7 dias para eventos relacionados à tarefa e de 30 dias para eventos relacionados à política. Ao modificar o período de armazenamento do evento, considere os procedimentos de trabalho em vigor na sua organização e quanto tempo o administrador de sistema pode dedicar à análise de cada evento.

É aconselhável modificar as configurações de armazenamento do evento em alguns dos seguintes casos:

- Os eventos relativos a modificações nos estados intermediários de tarefas de grupo e eventos relativos à aplicação de políticas correspondem a um grande percentual de todos os eventos no banco de dados do Kaspersky Security Center Linux.
- O log do sistema operacional começa a mostrar as entradas sobre a remoção automática de eventos quando o limite estabelecido no número total de eventos armazenados no banco de dados for excedido.

Escolha as opções de registro de evento com base na suposição de que o número ótimo de eventos que vêm de um dispositivo único por dia não deve exceder 20. Você pode aumentar este limite ligeiramente, se necessário, mas somente se o número de dispositivos na sua rede for relativamente pequeno (menos do que 10.000).

Melhores práticas para um Servidor de Administração que gerencia um grande número de dispositivos

Práticas recomendadas para usar o DBMS

Configure a tarefa de **Manutenção do Servidor de Administração** a ser executada regularmente, especialmente se um DBMS PostgreSQL for usado.

Exclua a pasta DBMS da verificação de IOC.

Práticas recomendadas para políticas e perfis

Reduza o número de políticas ativas para um componente (como o Kaspersky Endpoint Security for Windows). É possível substituir políticas por perfis de política.

Melhores práticas para um Servidor de Administração que gerencia um grande número de dispositivos

Reduza o número de tarefas executadas de modo simultâneo, especialmente a instalação remota e o gerenciamento de patches.

Reduza o número e otimize o agendamento de tarefas que operam em seleções de dispositivos.

Na seção **Configuração de eventos** das configurações da política, minimize o número de tipos de evento que estão sendo salvos.

Melhores práticas para o armazenamento de eventos

Reduza a frequência de eventos de tipo único do componente Controle de Aplicativos. Consulte o seguinte artigo para obter informações: Sobre o bloqueio de eventos frequentes.

Reduza o período de armazenamento para eventos de componentes (como o Kaspersky Endpoint Security for Windows) e eventos informativos sobre vulnerabilidades corrigidas.

Ative a configuração **Salvar eventos relacionados ao progresso da tarefa** nas propriedades da tarefa para tarefas gerais, como as tarefas de atualização. Consulte o seguinte artigo para obter informações: Registro de informações sobre eventos para tarefas e políticas.

Otimize as configurações da tarefa de inventário. Consulte o seguinte artigo para obter informações: Tarefa de inventário.

Considerações específicas e configurações ótimas de determinadas tarefas

Determinadas tarefas estão sujeitas a considerações específicas relativas ao número de dispositivos na rede. Esta seção oferece recomendações sobre a definição ótima das configurações para tais tarefas.

A descoberta de dispositivos, a tarefa de backup dos dados, a tarefa de manutenção do banco de dados e as tarefas de grupo para atualizar o Kaspersky Endpoint Security fazem da parte da funcionalidade básica do Kaspersky Security Center Linux.

A tarefa de inventário faz parte do recurso de Gerenciamento de patches e vulnerabilidades e está indisponível se este recurso não estiver ativado.

Frequência da descoberta de dispositivos

Não é aconselhável aumentar a frequência padrão da descoberta de dispositivos, já que isso pode criar uma carga excessiva nos controladores de domínio. Ao contrário, recomenda-se agendar a amostragem com a mínima frequência possível permitida pelas necessidades da sua organização. As recomendações sobre o cálculo do agendamento ótimo são fornecidas na tabela abaixo.

Agendamento da descoberta de dispositivos

Número de dispositivos na rede	Frequência da descoberta de dispositivos recomendada
Menos de 10.000	Frequência padrão ou menos
10.000 ou mais	Uma vez por dia ou menos

Tarefa de backup dos dados do Servidor de Administração e tarefa de manutenção do banco de dados

O Servidor de Administração para de funcionar enquanto as seguintes tarefas estão em execução:

- Cópia de backup de dados do Servidor de Administração
- Manutenção do Servidor de Administração

Enquanto estas tarefas estão em execução, o banco de dados não pode receber nenhum dado.

Você poderá ter que reagendar estas tarefas para que eles não sejam executadas ao mesmo tempo que outras tarefas de Servidor de Administração.

Tarefas de grupo para atualizar o Kaspersky Endpoint Security

Se o Servidor de Administração atuar como a fonte de atualização, a opção de agendamento recomendada para o Kaspersky Endpoint Security 10 e versões posteriores é **Quando novas atualizações são baixadas no repositório** com a caixa de seleção **Usar atraso randomizado automaticamente para início da tarefas**.

Se uma tarefa local para baixar as atualizações dos servidores da Kaspersky para o repositório que for criado em cada ponto de distribuição, o agendamento periódico é recomendado para a tarefa de atualização em grupo do Kaspersky Endpoint Security. O valor do período de randomização deve ser uma hora neste caso.

Tarefa de inventário

É possível reduzir a carga no banco de dados enquanto as informações sobre os arquivos executáveis são obtidas. Para isso, recomendamos executar uma tarefa de inventário do Kaspersky Endpoint Security em dispositivos de referência onde esteja instalado um conjunto padrão de softwares.

O número de arquivos executáveis recebidos pelo Servidor de Administração de um único dispositivo não pode exceder 150.000. Quando o Kaspersky Security Center Linux alcançar este limite, ele não poderá receber nenhum novo arquivo.

Normalmente, o número de arquivos em um dispositivo cliente comum não excede 60.000. O número de arquivos executáveis em um servidor de arquivos pode ser maior e pode até exceder o limite de 150.000.

Detalhes da carga da rede espalhada entre o Servidor de Administração e os dispositivos protegidos

Esta seção fornece os resultados de medições de teste do tráfego da rede com uma descrição das condições sob as quais as medições foram executadas. Você pode usar estas informações como referência ao planejar a infraestrutura da rede e a capacidade de produtividade dos canais da rede dentro da sua organização (ou entre o Servidor de Administração e outros dispositivos da organização a proteger). Conhecendo a capacidade de produtividade da rede, você também pode estimar aproximadamente quanto tempo as diferentes operações de transmissão de dados levarão.

Taxa de tráfego sob diversos cenários

A tabela abaixo mostra os resultados dos testes de medição conduzidos no tráfego entre o Servidor de Administração e um dispositivo gerenciado em diferentes cenários.

Por padrão, os dispositivos são sincronizados com o Servidor de Administração a cada 15 minutos ou em um intervalo mais longo. Contudo, se você modificar as configurações de uma política ou tarefa no Servidor de Administração, a primeira sincronização ocorre em dispositivos aos quais a política ou tarefa for aplicável para que as novas configurações sejam transmitidas aos dispositivos.

Taxa de tráfego entre o Servidor de Administração e um dispositivo gerenciado

Cenário	Tráfego do Servidor de Administração ao dispositivo gerenciado	Tráfego de cada dispositivo gerenciado ao Servidor de Administração
Instalação do Kaspersky Endpoint Security for Linux com bancos de dados atualizados	390 MB	3,3 MB
Instalação do Agente de Rede	75 MB	397 KB
Instalação simultânea do Agente de Rede e do Kaspersky Endpoint Security for Linux	459 MB	3,6 MB
Atualização inicial dos bancos de dados antivírus sem atualizar os bancos de dados no pacote (se a participação na Kaspersky Security Network for desativada)	113 MB	1,8 MB
Atualização diária dos bancos de dados antivírus (caso a participação na Kaspersky Security Network esteja ativada)	22 MB	373 MB
Sincronização inicial antes da atualização dos bancos de dados em um dispositivo (transferência de políticas e tarefas)	382 KB	446 KB
Sincronização inicial após atualizar os bancos de dados em um dispositivo	20 KB	157 KB
Sincronização sem modificações no Servidor de Administração (de acordo com o agendamento)	18 KB	23 KB
Sincronização quando uma definição única em uma política de grupo é modificada (assim que a definição for alterada)	19 KB	20 KB
Sincronização quando uma definição única em uma tarefa de grupo é modificada (assim que a definição for alterada)	14 KB	11 KB
Sincronização forçada	110 KB	109 KB
Evento **Vírus detectado** (1 vírus)	44 KB	50 KB
Evento **de Vírus detectado** (10 vírus)	58 KB	77 KB

Cenário	Tráfego do Servidor de Administração ao dispositivo gerenciado	Tráfego de cada dispositivo gerenciado ao Servidor de Administração
Tráfego único após ativar a lista de registro de aplicativos	até 10 KB	até 12 KB
Tráfego diário quando a lista de registro de aplicativo está ativada	até 840 KB	até 1 MB

Uso de tráfego médio durante 24 horas

O uso médio de tráfego de 24 horas entre o Servidor de Administração e um dispositivo gerenciado é o seguinte:

- O tráfego do Servidor de Administração para o dispositivo gerenciado é 840 KB.
- O tráfego do dispositivo gerenciado para o Servidor de Administração é 1 MB.

O tráfego foi medido nas seguintes condições:

- O dispositivo gerenciado tinha o Agente de Rede e o Kaspersky Endpoint Security for Linux instalados.
- O dispositivo não havia sido atribuído a um ponto de distribuição.
- O Gerenciamento de patches e vulnerabilidades não estava ativado.
- A frequência da sincronização com o Servidor de Administração era de 15 minutos.

Problemas conhecidos e limitações

O Kaspersky Security Center Linux tem uma série de limitações que não são críticas para a operação do aplicativo:

- 8698100: a tarefa **Backup de dados do Servidor de Administração** termina com o erro "Verifique se o SQL Server tem acesso à pasta de destino" ao usar a autenticação bidirecional entre o utilitário klpg_dump e o PostgreSQL.

- 10253149: nas propriedades da política do Kaspersky Endpoint Security for Windows (**Configuração de eventos** → **Avisos**), ao acessar as propriedades do tipo de evento **Tarefa interrompida**, o texto sobre o atributo de evento em massa não é exibido na seção expansível.

- 10723777: ao atualizar os bancos de dados usando a tarefa **Baixar atualizações para o repositório do Servidor de Administração**, o Kaspersky Security Center Linux tenta usar bancos de dados com um idioma diferente do seu quando o idioma não é inglês (en).

- 10427694: no Ubuntu 24.04, devido a problemas no processamento de chamadas de sistema assíncronas, o Servidor de Administração gera dumps indevidamente.

- 10007954: depois de criar e iniciar a tarefa **Encontrar as vulnerabilidades e as atualizações necessárias**, ocorre o erro "A conexão com o Servidor de Administração foi interrompida" ao acessar os resultados da tarefa no Servidor secundário.

- 10671377: Ao usar o PostgreSQL ou o Postgres Pro 18.1–18.5, as tarefas em execução podem terminar com o erro "'[53000]' ERROR: no empty local buffer available". Recomendamos atualizar o PostgreSQL para a versão 18.6 ou seguir estas etapas:

  1. Pare o serviço do Servidor de Administração.
  2. Pare o serviço do DBMS.
  3. Adicione a seguinte linha ao final do arquivo postgresql.conf: `[[effective_io_concurrency=0]]`.
  4. Inicie o serviço do DBMS.
  5. Verifique se o valor da configuração `effective_io_concurrency` é `0` executando a seguinte consulta:
     `SELECT setting FROM pg_settings WHERE name = 'effective_io_concurrency';`
  6. Inicie o serviço do Servidor de Administração.

- 10564198: Ao atualizar o Kaspersky Security Center Linux para a versão 16.3 nos nós de um cluster de failover do Kaspersky Security Center Linux, a execução do script postinstall.pl para configurar o Servidor de Administração pode causar erros de instalação.

- 8994760: Se você tiver direitos de acesso em Servidores de Administração virtuais, mas não tiver direitos de acesso no Servidor de Administração principal e tentar fazer login no Kaspersky Security Center Linux, ocorrerá um erro e a mensagem de erro **Não é possível processar sua solicitação no momento. Aguarde um pouco e tente novamente** será exibida incorretamente. O texto do erro deve ser o seguinte: **Verificar os direitos de acesso. É preciso ter direitos de acesso no servidor principal ou em apenas um dos servidores virtuais. Entre em contato com o administrador principal e tente novamente**

- 10302954: Ao especificar as condições para uma regra de movimentação de dispositivo, se, na guia **Rede**, você ativar a configuração **O dispositivo está localizado em um subgrupo do grupo de Domínios**, a lista suspensa de subgrupos será exibida vazia.

- 10253149: Para políticas de aplicativo, se você selecionar um evento em massa na guia **Configuração de eventos**, o bloco expansível **Mostrar mais**, que contém um aviso sobre o impacto desses eventos no desempenho do Servidor de Administração ou do DBMS, não será exibido.

- 9302142: A opção **Usar o Agente de Rede como um gateway de conexão na DMZ** não é compatível com o Microsoft Windows on Arm.

- 9065814: Talvez ocorra um erro durante a tentativa de autenticação do domínio por meio de um dispositivo baseado em Windows em um domínio Samba 4.

- 9335676: Depois de alternar o nó principal em um cluster DBMS de alta disponibilidade, o acesso ao Kaspersky Security Center Web Console talvez fique indisponível ou demasiado atrasado. Caso o Kaspersky Security Center Web Console permaneça inacessível por mais de 10 minutos, reinicie o serviço IAM usando o seguinte comando:

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085: Durante a execução da tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* em um dispositivo gerenciado Windows com a opção **Iniciar a instalação ao reiniciar ou fechar o dispositivo** ativada, a tarefa talvez falhe com um erro. Esse problema pode ocorrer quando um grande número de atualizações estiver agendado para instalação. Para resolver o problema, execute a tarefa sem ativar a opção **Iniciar a instalação ao reiniciar ou fechar o dispositivo**.

- 9272534: Se a tabela de usuários contiver mais de 50 mil usuários, somente os primeiros 50 mil serão exibidos e os restantes não serão exibidos.

- 9291235: Depois de restaurar um backup no Servidor de Administração versão 16.1, o Kaspersky Security Center Web Console exibe a página de login. Após a autenticação bem-sucedida, um código de segurança de uso único para a autenticação de dois fatores será solicitado. Quando um código de segurança de uso único válido é inserido, uma mensagem de erro é exibida indicando que ele está incorreto. Nesse caso, aguarde alguns minutos e atualize manualmente a página para tentar entrar novamente no Kaspersky Security Center Web Console. Depois que o processo de restauração do backup for totalmente concluído, a autenticação será bem-sucedida na próxima tentativa.

- 7939561: Ao tentar modificar uma conta de usuário protegida, clicar no botão **Cancelar** na janela de entrada de credencial **Proteção da conta** resulta em um erro.

- 8562938: Abrir a porta para dispositivos móveis nas propriedades de política do Servidor de Administração não ativa o recurso Gerenciamento de dispositivos móveis e não aciona a geração de um certificado de dispositivos móveis. Para ativar o recurso Gerenciamento de dispositivos móveis, a porta para dispositivos móveis deve ser aberta nas propriedades do Servidor de Administração.

- 8732282: Para um usuário que tenha a opção **O usuário não pode alterar a senha** ativada nas propriedades da conta no Active Directory, a ação de resposta **Redefinir a senha** no Active Directory não será executada. O administrador do controlador de domínio deve desativar a opção **O usuário não pode alterar a senha** para este usuário ou redefinir a senha manualmente. Este problema ocorre se você tiver a licença Kaspersky Next XDR Optimum, a integração com o Active Directory estiver ativada e o usuário estiver incluído em um grupo de segurança do Active Directory.

- 8688182: Se o usuário tiver a opção **A senha nunca expira** ativada nas propriedades da conta no Active Directory, após a execução da ação de resposta **Redefinir a senha**, a opção **A senha nunca expira** será desativada, e o usuário será obrigado a alterar sua senha de domínio no próximo login. Este problema ocorre se você tiver a licença Kaspersky Next XDR Optimum, a integração com o Active Directory estiver ativada e o usuário estiver incluído em um grupo de segurança do Active Directory.

- 8703857: A Conexão com o servidor proxy para o Kaspersky Security Center Web Console e plug-ins de gerenciamento da Web é estabelecida apenas se o servidor proxy for compatível com a autenticação básica.

- 7911778: Ao executar a tarefa **Desinstalar aplicativo remotamente** para desinstalar o Agente de Rede de um dispositivo que está executando um sistema operacional com a arquitetura Arm e que também tem um tempo não sincronizado com o Servidor de Administração, o status da tarefa não muda de **Executando** para **Concluído**, mesmo após o Agente de Rede ter sido desinstalado com êxito do dispositivo. Para resolver esse problema, sincronize a hora no dispositivo com o Agente de Rede instalado e a hora no dispositivo com o Servidor de Administração antes de executar a **Desinstalar aplicativo remotamente**.

- 6896585: Um dispositivo gerenciado não poderá se conectar com a KSN por meio do serviço Proxy da KSN se o Kaspersky Security Center Linux estiver instalado em um dispositivo que tenha símbolos cirílicos em seu nome.

- 7523299: O Agente de Rede não é reiniciado depois de encerrar seu processo em um dispositivo gerenciado que executa o CentOS 6.6.

- 7835858: Se você criar uma tarefa com as configurações de agendamento **A cada N dias** e **Por dias da semana** no Kaspersky Security Center Web Console versão 15.2 ou posterior e, em seguida, abrir a tarefa em versões anteriores do Kaspersky Security Center Web Console ou do Console de Administração (por exemplo, quando a tarefa também for aplicada nos Servidores de Administração secundários que podem ser baseados em Linux e em Windows), é possível que as configurações de agendamento sejam exibidas incorretamente ou que ocorra um erro.

- 7208621: Quando a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* ou *Verificação de atualizações* é importada, a opção **Selecionar dispositivos aos quais a tarefa será atribuída** é ativada. Essas tarefas não podem ser atribuídas para uma seleção de dispositivos ou dispositivos específicos. Caso a tarefa *Baixar atualizações aos repositórios de pontos de distribuição* ou *Verificação de atualizações* seja atribuída aos dispositivos específicos, ela será importada incorretamente.

- 6511063: Caso um aplicativo da seção de **Registro de aplicativos** tenha sido detectado em um dispositivo Linux, as propriedades do aplicativo não conterão as informações sobre os arquivos executáveis relacionados.

- 5915107: Em relatórios com formato carta, uma quebra de página pode cortar uma linha de texto horizontalmente.

- 5556109: Um dispositivo gerenciado que possui mais de um adaptador de rede envia informações ao Servidor de Administração sobre o endereço MAC do adaptador de rede que não é aquele usado para se conectar ao Servidor de Administração.

- 9093038: Se o Servidor de Administração do Kaspersky Security Center Linux não iniciar após a instalação e o registro do sistema operacional contiver o erro 213/SECUREBITS relacionado ao kladminserver_srv.service, execute os seguintes comandos como superusuário:

```
mkdir -p /etc/systemd/system/kladminserver_srv.service.d
echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
```

  Se o Kaspersky Security Center Web Console não iniciar após a instalação e o registro do sistema operacional contiver o erro 213/SECUREBITS relacionados ao KSCWebConsole.service, execute os seguintes comandos como superusuário:

```
mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
```

  Se o serviço kliam_srv não for iniciado após a instalação e o registro do sistema operacional contiver o erro 213/SECUREBITS relacionado ao serviço, execute os seguintes comandos como um superusuário:

```
mkdir -p /etc/systemd/system/kliam_srv.service.d
echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
```

- 9165434: A autenticação NTLM não funciona para contas de usuário dentro do grupo Usuários protegidos.

Contatar o Suporte Técnico

Esta seção descreve como adquirir o suporte técnico e os termos com os quais está disponível.

Como obter suporte técnico

Se você não encontrou uma solução para o problema na documentação ou em outras fontes de informação sobre o Kaspersky Security Center Linux, recomendamos entrar em contato com o Suporte Técnico. Os especialistas do Suporte Técnico responderão a todas as suas dúvidas sobre instalação e uso do Kaspersky Security Center.

A Kaspersky fornece suporte ao Kaspersky Security Center durante seu ciclo de vida (consulte a página do ciclo de vida do suporte do aplicativo). Antes de entrar em contato com o Serviço de Suporte Técnico, leia as regras de suporte.

Você pode entrar em contato com o Suporte Técnico de uma das seguintes maneiras:

- Visitando o site de Suporte Técnico
- Enviando uma solicitação para o Suporte Técnico da Kaspersky a partir do portal Kaspersky CompanyAccount

Suporte técnico via Kaspersky CompanyAccount

O Kaspersky CompanyAccount é um portal para empresas que usam aplicativos Kaspersky. O portal Kaspersky CompanyAccount foi projetado para facilitar a interação entre os usuários e os especialistas da Kaspersky através de solicitações online. Você pode usar o Kaspersky CompanyAccount para acompanhar o status das suas solicitações online enquanto elas são processadas pelos especialistas da Kaspersky e manter um histórico dessas solicitações.

Você pode registrar todos os funcionários da sua empresa com uma única conta no Kaspersky CompanyAccount. Uma única conta permite gerenciar centralmente solicitações de funcionários registrados enviadas para a Kaspersky, além de gerenciar os privilégios desses funcionários através do Kaspersky CompanyAccount.

O portal Kaspersky CompanyAccount está disponível nos seguintes idiomas:

- Inglês
- Espanhol
- Italiano
- Alemão
- Polonês
- Português

- Russo
- Francês
- Japonês

Para saber mais sobre o Kaspersky CompanyAccount, visite o site do Suporte Técnico.

Obter arquivos de dump do Servidor de Administração

Os arquivos de dump do Servidor de Administração contêm todas as informações sobre os processos do Servidor de Administração em um determinado momento. Os arquivos de dump do Servidor de Administração são armazenados no diretório /var/lib/systemd/coredump. Os arquivos de dump são armazenados enquanto o Kaspersky Security Center Linux estiver em uso e serão excluídos permanentemente quando forem removidos. Os arquivos de dump não são enviados para o Kaspersky automaticamente.

Caso o Servidor de Administração trave, é possível entrar em contato com o Suporte Técnico da Kaspersky. Um especialista do Suporte Técnico pode solicitar o envio dos arquivos de dump do Servidor de Administração para que seja feita a análise adicional na Kaspersky.

Os arquivos de dump podem conter dados pessoais. Recomendamos proteger as informações contra acesso não autorizado antes de enviá-las à Kaspersky.

Fontes de informação sobre o aplicativo

Página do Kaspersky Security Center Linux no site da Kaspersky

Na página do Kaspersky Security Center Linux no site da Kaspersky, é possível visualizar as informações gerais sobre o aplicativo, suas funções e recursos.

Página do Kaspersky Security Center Linux na Base de Dados de Conhecimento

A *Base de Dados de Conhecimento* é uma seção do site de Suporte Técnico da Kaspersky.

Na página do Kaspersky Security Center Linux na Base de Conhecimento, é possível ler artigos que fornecem informações úteis, recomendações e respostas às perguntas frequentes sobre como comprar, instalar e usar o aplicativo.

Os artigos na Base de Dados de Conhecimento podem fornecer respostas às perguntas relacionadas ao Kaspersky Security Center Linux como também a outros aplicativos da Kaspersky. Os artigos na Base de dados de Conhecimento também podem conter novidades sobre o suporte técnico.

Discutir questões sobre os aplicativos Kaspersky com a comunidade

Se a sua pergunta não precisar de uma resposta imediata, você pode discuti-la com os especialistas da Kaspersky e outros usuários no nosso Fórum.

No Fórum, você pode visualizar tópicos de discussão, postar seus comentários e criar novos tópicos de discussão.

É necessária uma conexão com a Internet para acessar os recursos do site.

Se você não puder encontrar uma solução para o problema, entre em contato com o Suporte técnico.

Glossário

Administrador cliente

Um membro da equipe de uma organização cliente que é responsável por monitorar o status da proteção antivírus.

Administrador do Kaspersky Security Center Linux

A pessoa que gerencia as operações de aplicativos pelo sistema Kaspersky Security Center Linux do sistema de administração centralizada remota.

Administrador do provedor de serviço

Um membro da equipe em um provedor de serviço de proteção antivírus. Esse administrador efetua tarefas de instalação e manutenção em sistemas de proteção antivírus de acordo com os produtos da Kaspersky e também fornece suporte técnico aos clientes.

Agente de atualização

Um computador que tenha um Agente de Rede instalado e é usado para a distribuição da atualização, instalação remota de aplicativos, obtenção de informações sobre os computadores em um grupo de administração e/ou domínio de broadcasting. Os pontos de distribuição são projetados para reduzir a carga no Servidor de Administração durante a distribuição da atualização e para otimizar o tráfego na rede. Os pontos de distribuição podem ser atribuídos automaticamente pelo Servidor de Administração ou manualmente pelo administrador.

Agente de autenticação

Uma interface que permite concluir a autenticação para acessar discos rígidos criptografados e carregar o sistema operacional após a unidade de disco rígido do sistema ter sido criptografada.

Agente de Rede

Um componente do Kaspersky Security Center Linux que permite a interação entre o Servidor de Administração e os aplicativos Kaspersky instalados em um nó específico da rede (estação de trabalho ou servidor). Este componente é comum a todos os aplicativos da empresa para Windows. Existem versões separadas do Agente de Rede para aplicativos Kaspersky para Novell®, Unix™ e Mac.

Aplicativo incompatível

Um aplicativo antivírus de um desenvolvedor de terceiros ou um aplicativo da Kaspersky que não aceita o gerenciamento através do Kaspersky Security Center Linux.

Application settings

As configurações do aplicativo que forem comuns para todos os tipos de tarefas e controlam a operação total do aplicativo, como: configurações de desempenho do aplicativo, configurações de relatórios e configurações de backup.

Arquivo de chave

Um arquivo com o formato xxxxxxxx.key que torna possível usar um aplicativo da Kaspersky com uma licença de avaliação ou licença comercial. Você pode usar o aplicativo somente se tiver um arquivo de chave.

Ataque de vírus

Uma série de tentativas deliberadas para infectar um dispositivo com um vírus.

Atualização

O procedimento de substituição ou inclusão de novos arquivos (bancos de dados ou módulos de software) obtidos dos servidores de atualização Kaspersky.

Atualização disponível

Um conjunto de atualizações dos módulos de aplicativo da Kaspersky com atualizações críticas acumuladas por um determinado período e alterações à arquitetura do aplicativo.

Bancos de dados antivírus

Bancos de dados que contêm informações sobre ameaças à segurança do computador conhecidas da Kaspersky na data de publicação dos bancos de dados antivírus. As entradas em bancos de dados antivírus permitem a detecção de código malicioso em objetos verificados. Bancos de dados antivírus são criados pelos especialistas da Kaspersky e são atualizados a cada hora.

Certificado compartilhado

Um certificado destinado a identificar o dispositivo móvel do usuário.

Certificado do Servidor de Administração

O certificado do Servidor de Administração é usado para autenticá-lo quando o Console de Administração se conecta a ele e durante a comunicação com dispositivos cliente. O certificado do Servidor de Administração é criado durante a instalação do componente do Servidor de Administração e é armazenado na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert no Servidor de Administração.

Chave ativa

Uma chave usada atualmente pelo aplicativo.

Chave reserva

Uma chave que certifica que o usuário tem o direito de usar o aplicativo, mas que não está sendo usado no momento.

Cloud Discovery

O Cloud Discovery gerencia o acesso do usuário aos serviços em nuvem. Exemplos de serviços em nuvem são Microsoft Teams, Salesforce e Microsoft Office 365. Os serviços em nuvem são agrupados em categorias, por exemplo, *Compartilhamento de arquivos*, *Mensagens instantâneas* e *E-mail*.

Configurações de tarefa

Configurações do aplicativo específicas para cada tipo de tarefa.

Console de Administração

O componente do Kaspersky Security Center Linux que fornece a interface de usuário dos serviços administrativos do Servidor de Administração e do Agente de Rede.

Cópia de backup de dados do Servidor de Administração

Cópia dos dados do Servidor de Administração para backup e subsequente restauração realizada, usando o utilitário de backup. O utilitário pode salvar:

- A base de conhecimento do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração)
- Informações de configuração sobre a estrutura dos grupos de administração e dispositivos cliente

- Repositório dos arquivos de instalação para instalação remota de aplicativos (conteúdo das pastas: Pacotes, Atualizações de Desinstalação)
- Certificado do Servidor de Administração

Direitos de administrador

O nível de direitos e privilégios do usuário para administração de objetos Exchange numa organização Exchange.

Dispositivo MDM do iOS

Um dispositivo móvel que é conectado ao Servidor de MDM do iOS através do protocolo MDM do iOS. Os dispositivos que executam sistema operacional iOS podem ser conectados e gerenciados através de protocolo MDM do iOS.

Dispositivos gerenciados

Dispositivos na rede corporativa que estão incluídos em um grupo de administração.

Domínio de difusão

A área lógica de uma rede na qual todos os nós podem intercambiar dados usando o canal de difusão no nível do OSI (Open Systems Interconnection Basic Reference Model).

Estação de trabalho do administrador

O dispositivo no qual o Console de Administração está instalado atua como o componente que fornece a interface de gerenciamento do Kaspersky Security Center Linux.

A partir da estação de trabalho do administrador, o administrador gerencia o componente de servidor do Kaspersky Security Center, criando e controlando o sistema de proteção centralizada da rede da organização com base nos aplicativos da Kaspersky.

FileTransferBridge

Um componente interno do Kaspersky Security Center Linux que fornece a entrega local de atualizações de aplicativos da Kaspersky. O FileTransferBridge é integrado ao Agente de Rede (klnagent) e é executado localmente em cada dispositivo gerenciado.

Quando os aplicativos da Kaspersky recebem atualizações do Kaspersky Security Center Linux, o Agente de Rede baixa os arquivos de atualização do Servidor de Administração ou de um ponto de distribuição. Em seguida, o FileTransferBridge transfere os arquivos localmente para os aplicativos da Kaspersky instalados, garantindo a entrega confiável de atualizações do banco de dados e patches de software.

O FileTransferBridge usa as portas TCP 30522 e 30523. As portas ficam em escuta somente na interface localhost (127.0.0.1) e não aceitam conexões de entrada de redes externas.

Gateway de conexão

Um *gateway de conexão* é um Agente de Rede atuando em um modo especial. Um gateway de conexão aceita conexões de outros Agentes de Rede e os canaliza para o Servidor de Administração por meio de sua própria conexão com o Servidor. Ao contrário de um Agente de Rede comum, um gateway de conexão aguarda por conexões do Servidor de Administração, em vez de estabelecer conexões com o Servidor de Administração.

Gerenciamento centralizado de aplicativos

O gerenciamento remoto de aplicativo utilizando os serviços de administração fornecidos no Kaspersky Security Center.

Gerenciamento direto de aplicativos

Gerenciamento de aplicativos através de interface local.

Gravidade do evento

Propriedade de um evento encontrado durante a operação de um aplicativo da Kaspersky. Há quatro níveis de gravidade:

- Evento crítico
- Falha funcional
- Advertência
- Informação

Eventos do mesmo tipo podem ter níveis de gravidade diferentes dependendo da situação na qual ocorreu o evento.

Grupo de administração

Um grupo de dispositivos agrupados por função e por aplicativos da Kaspersky instalados. Os dispositivos são agrupados como uma entidade única para a conveniência de gerenciamento. Um grupo pode incluir outros grupos. As políticas de grupo e tarefas de grupo podem ser criadas para cada aplicativo instalado no grupo.

Grupo de funções

Um grupo de usuários de dispositivos móveis Exchange ActiveSync que recebem direitos de administrador idênticos.

HTTPS

Protocolo seguro para transferência de dados, usando criptografia, entre um navegador e um Servidor Web. HTTPS é usado para acessar informações restritas, como dados corporativos e financeiros.

Identity and Access Manager (IAM)

Um componente do Servidor de Administração que permite utilizar a autenticação do domínio (conexão única). O recurso de conexão única permite ao usuário ativar a autenticação segura no Kaspersky Security Center Web Console sem ter que inserir a senha novamente na rede corporativa.

Instalação local

Instalação de um aplicativo de proteção em um dispositivo em uma rede corporativa que envolve iniciar manualmente a instalação a partir de um pacote de distribuição do aplicativo de proteção ou executar manualmente um pacote de instalação publicado que foi baixado previamente no dispositivo.

Instalação manual

Instalação de um aplicativo de proteção em um dispositivo na rede corporativa a partir de um pacote de distribuição. A instalação manual requer uma participação de um administrador ou outro especialista de TI. A instalação manual típica é efetuada caso a instalação remota tenha sido concluída com um erro.

Instalação remota

Instalação de aplicativos Kaspersky usando os serviços fornecidos pelo Kaspersky Security Center Linux.

JavaScript

Uma linguagem de programação que expande o desempenho de páginas da Web. As páginas da Web criadas com JavaScript podem executar funções (por exemplo, alterar a visualização de elementos da interface ou abrir janelas adicionais) sem atualizar a página da Web com novos dados de um Servidor Web. Para visualizar as páginas criadas ao utilizar o JavaScript, ative o suporte do JavaScript na configuração do seu navegador.

Lightweight Nagent (LWNGT)

Um protocolo para interação com o Kaspersky Endpoint Security em dispositivos móveis. O LWNGT (também chamado de protocolo móvel) funciona como um Agente de Rede sem que seja necessário instalá-lo nos dispositivos móveis.

Loja de aplicativos

Componente do Kaspersky Security Center Linux. A Loja de aplicativos é usada para instalar aplicativos em dispositivos Android possuídos por usuários. A Loja de aplicativos permite publicar os arquivos APK de aplicativos e os links aos aplicativos no Google Play.

Nível de importância do patch

Atributo do patch. Há cinco níveis de importância para patches da Microsoft e para patches de terceiros:

- Crítico.
- Alto.
- Médio.
- Baixo.
- Desconhecido.

O nível de importância de uma aplicação de patches de terceiros ou da aplicação de patches da Microsoft é determinado pelo nível de gravidade menos favorável entre as vulnerabilidades que os patches deveriam corrigir.

Operador do Kaspersky Security Center

Usuário que monitora o status e operação de um sistema de proteção gerenciado através do Kaspersky Security Center.

Pacote de instalação

Um conjunto de arquivos criados para a instalação remota de um aplicativo da Kaspersky usando o sistema de administração remota do Kaspersky Security Center. O pacote de instalação contém um intervalo de configurações necessárias para instalar o aplicativo e colocá-lo em funcionamento imediatamente após a instalação. As configurações correspondem aos padrões do aplicativo. O pacote de instalação é criado usando arquivos com as extensões .kpd e .kud incluídas no kit de distribuição do aplicativo.

Pasta de backup

Pasta especial para armazenamento das cópias de dados do Servidor de Administração criados usando o utilitário de backup.

Perfil

Um conjunto de configurações de Dispositivos móveis Exchange que define seu comportamento quando conectado a um Microsoft Exchange Server.

Perfil de configuração

Política que contém um conjunto de configurações e restrições para um dispositivo móvel MDM do iOS.

Perfil de provisionamento

Conjunto de configurações para operação de aplicativos em dispositivos móveis iOS. Um perfil de provisionamento contém informações sobre a licença. Está associado a um aplicativo em específico.

Período da licença

O período durante o qual você pode usar os recursos do aplicativo e os serviços adicionais. Os serviços que você pode usar dependem do tipo de licença.

Política

Uma política determina as configurações de um aplicativo e gerencia a capacidade de configurar esse aplicativo em computadores dentro de um grupo de administração. Uma política individual deve ser criada para cada aplicativo. Você pode criar um número ilimitado de políticas para aplicativos instalados nos dispositivos de cada grupo de administração, mas apenas uma política pode ser aplicada a cada aplicativo por vez em um grupo de administração.

Proprietário do dispositivo

Proprietário do dispositivo é um usuário que pode ser contatado pelo administrador quando a necessidade surgir para executar determinadas operações em um dispositivo cliente.

Provedor de serviço de proteção antivírus

Uma organização que fornece a uma organização cliente serviços de proteção antivírus com base nas soluções da Kaspersky.

Reconhecimento de local de rede (NLA)

Um serviço do Windows que ajuda um sistema operacional a identificar a rede atual. O NLA detecta alterações na rede e ajusta a configuração de segurança do dispositivo.

Repositório de eventos

Uma parte do banco de dados do Servidor de Administração dedicada ao armazenamento de informações sobre eventos que ocorrem no Kaspersky Security Center Linux.

Restauração

A realocação do objeto original da Quarentena ou Backup para sua pasta original onde o objeto foi armazenado antes de entrar na Quarentena, antes de ter sido desinfetado ou excluído, ou realocação para uma pasta definida pelo usuário.

Restauração dos dados do Servidor de Administração

Restauração dos dados do Servidor de Administração a partir de informações salvas na cópia backup usando o utilitário de backup. O utilitário pode restaurar:

- A base de conhecimento do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração)
- Informações de configuração sobre a estrutura dos grupos de administração e dispositivos cliente
- Repositório dos arquivos de instalação para instalação remota de aplicativos (conteúdo das pastas: Pacotes, Atualizações de Desinstalação)
- Certificado do Servidor de Administração

Segurança antivírus da rede

Um conjunto de medidas técnicas e organizacionais que reduzem a probabilidade de penetração de vírus e spam em uma rede da organização e que previnem ataques na rede, phishing e outras ameaças. A segurança antivírus da rede aumenta quando você usa aplicativos e serviços de segurança e quando aplica e segue a política de segurança de dados corporativa.

Servidor de Administração

Um componente do Kaspersky Security Center que armazena centralmente informações sobre todos os aplicativos Kaspersky instalados na rede corporativa e controla esses aplicativos.

Servidor de Administração cliente (Dispositivo cliente)

Um dispositivo, servidor ou estação de trabalho no qual o Agente de Rede e os aplicativos gerenciados da Kaspersky estão instalados e em execução.

Servidor de Administração Principal

Servidor de Administração principal é o Servidor de Administração que foi especificado durante a instalação do Agente de Rede. O Servidor de Administração principal pode ser usado em configurações de perfis de conexão do Agente de Rede.

Servidor de Administração virtual

Um componente do Kaspersky Security Center Linux designado para gerenciamento do sistema de proteção de uma rede corporativa cliente.

O Servidor de Administração virtual é um caso particular de um Servidor de Administração secundário com as seguintes restrições em comparação com o Servidor de Administração físico:

- O Servidor de Administração virtual só pode ser criado no Servidor de Administração principal.
- O Servidor de Administração virtual usa o banco de dados do Servidor de Administração principal. Tarefas de backup e restauração de dados, bem como tarefas de verificação de atualização e download, não são compatíveis com um Servidor de Administração virtual.
- O Servidor virtual não é compatível com a criação de Servidores de Administração secundários (incluindo Servidores virtuais).

Servidor MDM do iOS

Um componente do Kaspersky Security Center instalado em um dispositivo cliente e que permite a conexão de dispositivos móveis iOS ao Servidor de Administração e o gerenciamento de dispositivos móveis iOS através do serviço Apple Push Notifications (APNs).

Servidor Web do Kaspersky Security Center Linux

Um componente do Kaspersky Security Center Linux instalado em conjunto com o Servidor de Administração. O Servidor da Web foi projetado para a transmissão, através de uma rede, de pacotes de instalação independentes, perfis de iOS MDM e arquivos de uma pasta compartilhada.

Servidores de atualização da Kaspersky

Servidores HTTP na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

SSL

Um protocolo de criptografia de dados usado na Internet e em redes locais. O protocolo Secure Sockets Layer (SSL) é usado em aplicativos da Web para criar uma conexão segura entre o cliente e o servidor.

Status de proteção

Status atual da proteção, que reflete o nível de proteção do dispositivo.

Status de proteção da rede

O status de proteção atual, o qual define a segurança dos dispositivos na rede corporativa. O status de proteção da rede inclui fatores como os aplicativos de proteção instalados, o uso de chaves e o número e os tipos de ameaças detectadas.

Tarefa

Funções executadas pelo aplicativo da Kaspersky são implementadas como tarefas, tais como: Proteção do arquivo em tempo real, Verificação Completa do dispositivo, Atualização do banco de dados.

Tarefa de grupo

Uma tarefa definida para um grupo de administração e executada em todos os dispositivos cliente incluídos em tal grupo de administração.

Tarefa local

Uma tarefa definida e executada em um único dispositivo cliente.

Tarefa para dispositivos específicos

Uma tarefa atribuída para um conjunto de dispositivos cliente a partir de grupos de administração arbitrários e executada nesses dispositivos.

Usuários internos

As contas dos usuários internos são usadas para trabalhar com os Servidores de Administração virtuais. O Administrador pode usar uma conta de usuário interno para iniciar o Kaspersky Security Center Web Console e visualizar informações sobre o status da segurança antivírus da rede. No Kaspersky Security Center Linux, os usuários internos têm os direitos de usuários reais.

As contas de usuários internos só são criadas e usadas dentro do Kaspersky Security Center Linux. Os dados sobre os usuários internos não são transferidos para o sistema operacional. O Kaspersky Security Center Linux autentica os usuários internos.

Validador de Integridade do Sistema do Kaspersky Security Center (SHV)

Um componente do Kaspersky Security Center Linux concebido para verificar a operabilidade do sistema operacional em caso da operação simultânea do Kaspersky Security Center Linux e do Microsoft NAP.

Vulnerabilidade

Uma falha de um sistema operacional ou aplicativo que pode ser explorada por invasores para invadir o sistema operacional ou aplicativo e comprometer sua integridade. A presença de um grande número de vulnerabilidades em um sistema operacional o torna não confiável, porque o malware que invade o sistema operacional pode causar interrupções no próprio sistema operacional e nos aplicativos instalados.

Zona desmilitarizada (DMZ)

A zona desmilitarizada é um segmento da rede local que contém servidores, os quais respondem a solicitações da Web global. Para assegurar a segurança da rede local de uma organização, o acesso à LAN a partir da zona desmilitarizada é protegido por um firewall.

Informação sobre código de terceiros

As informações sobre o código de terceiros podem ser encontradas no arquivo legal_notices.txt e armazenadas no diretório de instalação do aplicativo.

Avisos de marca registrada

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

Adobe, Acrobat, Flash, PostScript e Shockwave são marcas comerciais registradas ou marcas comerciais da Adobe nos Estados Unidos e/ou outros países.

AMD, AMD64 são marcas comerciais ou marcas registradas da Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace são marcas comerciais da Amazon.com, Inc. ou de suas afiliadas.

Apache é uma marca registrada ou marca comercial da Apache Software Foundation nos Estados Unidos e/ou em outros países.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime e Touch ID são marcas comerciais da Apple Inc.

Arm é uma marca registrada da Arm Limited (ou de suas subsidiárias) nos Estados Unidos e/ou em outros lugares.

A palavra, marca e os logótipos Bluetooth são propriedade da Bluetooth SIG, Inc.

Ubuntu e LTS são marcas registradas da Canonical Ltd. Cisco, Cisco Jabber, Cisco Systems e IOS são marcas registradas ou marcas comerciais da Cisco Systems, Inc. e/ou de suas afiliadas nos Estados Unidos e em alguns outros países.

Citrix, XenServer são marcas registradas ou marcas comerciais da Cloud Software Group, Inc., e/ou suas subsidiárias nos Estados Unidos e/ou em outros países.

Corel é uma marca comercial ou marca comercial registrada da Corel Corporation e/ou de suas subsidiárias no Canadá, nos Estados Unidos e/ou em outros países.

Cloudflare, o logotipo da Cloudflare e Cloudflare Workers são marcas comerciais e/ou marcas registradas da Cloudflare, Inc. nos Estados Unidos e em outras jurisdições.

Dropbox é uma marca registrada da Dropbox, Inc.

Radmin é marca registrada da Famatech.

Firebird é uma marca comercial registrada da Firebird Foundation.

Foxit é uma marca comercial registrada da Foxit Corporation.

A marca FreeBSD é uma marca comercial registrada da The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Google Public DNS, Hangouts e YouTube são marcas comerciais da Google LLC.

EulerOS, FusionCompute, FusionSphere são marcas comerciais da Huawei Technologies Co., Ltd.

Intel, Core e Xeon são marcas comerciais da Intel Corporation ou de suas subsidiárias.

IBM, QRadar são marcas comerciais da International Business Machines Corporation registradas em muitas jurisdições em todo o mundo.

Node.js é uma marca registrada da Joyent, Inc.

Linux é uma marca comercial registrada da Linus Torvalds nos Estados Unidos e em outros locais.

Logitech é uma marca registrada ou marca comercial da Logitech nos Estados Unidos e/ou em outros países.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, Office 365, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista e Windows Azure são marcas comerciais registradas do grupo de empresas da Microsoft.

Mozilla, Firefox e Thunderbird são marcas registradas da Mozilla Foundation nos EUA e em outros países.

Novell é uma marca comercial registrada da Novell Enterprises Inc. nos Estados Unidos e em outros países.

OpenSSL é uma marca registrada de propriedade da OpenSSL Software Foundation.

OpenVPN é uma marca comercial da OpenVPN, Inc.

Oracle, Java, JavaScript e TouchDown são marcas comerciais registradas da Oracle e/ou suas afiliadas.

Parallels, o logotipo da Parallels e Coherence são marcas comerciais ou marcas registradas da Parallels International GmbH.

Chef é uma marca comercial ou marca registrada da Progress Software Corporation e/ou uma de suas subsidiárias ou afiliadas nos EUA e/ou em outros países.

Puppet é uma marca comercial ou marca registrada da Puppet, Inc.

Python é uma marca comercial ou marca registrada da Python Software Foundation.

Red Hat, Fedora e Red Hat Enterprise Linux são marcas comerciais da Red Hat Inc. ou de suas subsidiárias registradas nos Estados Unidos e em outros países.

Ansible é uma marca comercial registrada da Red Hat, Inc. nos Estados Unidos e em outros países.

CentOS é uma marca comercial ou marca comercial registrada da Red Hat, Inc. ou de suas subsidiárias nos Estados Unidos e em outros países.

A marca comercial BlackBerry é propriedade da Research In Motion Limited e está registrada nos Estados Unidos. Seu registro pode estar pendente ou concluído em outros países.

Rocky Linux é uma marca registrada da The Rocky Enterprise Software Foundation.

Samsung é uma marca registrada da SAMSUNG nos Estados Unidos ou em outros países.

Debian é uma marca registrada da Software in the Public Interest, Inc.

Splunk, SPL são marcas comerciais e marcas comerciais registradas da Splunk Inc. nos Estados Unidos e em outros países.

SUSE é uma marca comercial registrada da SUSE LLC nos Estados Unidos e em outros locais.

A marca comercial Symbian é propriedade da Symbian Foundation Ltd.

OpenAPI é uma marca registrada da Linux Foundation.

UNIX é uma marca comercial registrada nos Estados Unidos e em outros países, licenciada exclusivamente pela X/Open Company Limited.

Zabbix é uma marca comercial registrada da Zabbix SIA.