Guia de dimensionamento

Esta seção fornece informações sobre o dimensionamento do Kaspersky Security Center.

Sobre este Guia

O Guia de Dimensionamento do Kaspersky Security Center 14.2 (também conhecido como "Kaspersky Security Center") destina-se aos profissionais que instalam e administram o Kaspersky Security Center, assim como a todos os que fornecem suporte técnico a organizações que usam o Kaspersky Security Center.

Todas as recomendações e os cálculos são fornecidos para redes nas quais o Kaspersky Security Center gerencia a proteção dos dispositivos com o software da Kaspersky instalado, incluindo dispositivos móveis. Se os dispositivos móveis ou algum outro dispositivo gerenciado precisar ser considerado separadamente, isso será mencionado especificamente.

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
- 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

A tabela a seguir exibe as limitações da versão atual do Kaspersky Security Center.

Limitações do Kaspersky Security Center

Tipo de limitação	Valor
Número máximo de dispositivos gerenciados por Servidor de Administração	100.000
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 total máximo de objetos do Active Directory (unidades organizacionais, UOs) e contas de usuários, dispositivos e grupos de segurança)	1.000.000
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
O número máximo de dispositivos que um ponto de distribuição único pode cobrir (os pontos de distribuição podem cobrir dispositivos não móveis somente)	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.

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. Uma recomendação no cálculo de espaço disponível quando o recurso de Gerenciamento de patches e vulnerabilidades é usado, é fornecida separadamente.

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.

Servidor de Administração e DBMS estão em dispositivos diferentes, a rede inclui 50 mil dispositivos

Configuração do dispositivo com o Servidor de Administração instalado

Hardware	Valor
CPU	4 cores, 2.500 MHz
RAM	8 GB
Disco rígido	300 GB, RAID recomendado
Adaptador de rede	1 Gbits

Configuração do dispositivo com o DBMS instalado

Hardware	Valor
CPU	4 cores, 2.500 MHz
RAM	16 GB
Disco rígido	200 GB, SATA RAID
Adaptador de rede	1 Gbits

Servidor de Administração e DBMS estão no mesmo dispositivo, a rede inclui 50 mil dispositivos

Configuração do dispositivo com o Servidor de Administração e o DBMS instalados

Hardware	Valor
CPU	8 cores, 2.500 MHz
RAM	16 GB
Disco rígido	500 GB, SATA RAID
Adaptador de rede	1 Gbits

Servidor de Administração e DBMS estão em dispositivos diferentes, a rede inclui 100.000 dispositivos

Configuração do dispositivo com o Servidor de Administração instalado

Hardware	Valor
CPU	8 núcleos, 2,13 GHz
RAM	8 GB
Disco rígido	1 TB, com RAID
Adaptador de rede	1 Gbits

Configuração do dispositivo com o DBMS instalado

Hardware	Valor

CPU	8 núcleos, 2,53 GHz
RAM	26 GB
Disco rígido	500 GB, SATA RAID
Adaptador de rede	1 Gbits

DBMS SQL Server na máquina virtual, a rede inclui 50 mil dispositivos

Configuração da máquina virtual com o SQL Server instalado, até 50 mil dispositivos

Recursos reservados no Hypervisor	Valor
CPU	10 GHz
RAM	16 GB
IOPS do disco	150 IOPS
Espaço livre em disco	200 GB
Compartilhamento de instâncias do SQL Server	Sem compartilhamento

DBMS SQL Server na máquina virtual, a rede inclui 100 mil dispositivos

Configuração da máquina virtual com o SQL Server instalado, até 100 mil dispositivos

Recursos reservados no Hypervisor	Valor
CPU	20 GHz
RAM	26 GB
IOPS do disco	150 IOPS
Espaço livre em disco	500 GB
Compartilhamento de instâncias do SQL Server	Sem compartilhamento

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.
- A tarefa de backup salva cópias backup em um recurso de arquivo localizado em um servidor dedicado.

  O intervalo de sincronização para Agentes de Rede é definido como especificado na tabela abaixo.

  Intervalo de sincronização para Agentes de Rede

Intervalo de sincronização (minutos)	Número de dispositivos gerenciados
15	10.000
30	20.000
45	30.000
60	40.000
75	50.000
150	100.000

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.
- 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.

Se o Servidor de Administração distribui atualizações do Windows (agindo como o servidor Windows Server Update Services), o banco de dados exigirá 2,5 GB adicionais.

Durante a operação, um determinado *espaço não alocado* sempre estará presente no banco de dados. Portanto, o tamanho real do arquivo do banco de dados, (por padrão o arquivo KAV.MDF se você usa o SQL Server como o DBMS) com frequência é de aproximadamente o dobro de tamanho do que a quantidade de espaço ocupado pelo banco de dados.

Não se recomenda limitar explicitamente o tamanho do log de transações (por padrão, o arquivo KAV_log. LDF, se você usa o SQL Server como o DBMS). Recomenda-se deixar o valor padrão do parâmetro MAXSIZE. Contudo, se você precisar limitar o tamanho desse arquivo, leve em consideração que o valor necessário típico do parâmetro MAXSIZE para KAV_log.LDF é 20.480 MB.

Cálculo de espaço em disco (sem e com o uso do recursos de Gerenciamento de vulnerabilidade e de correção)

Cálculo de espaço em disco sem o uso do recurso de Gerenciamento de patches e vulnerabilidades

O espaço em disco do Servidor de Administração necessário para a pasta %ALLUSERSPROFILE %\ApplicationData\KasperskyLab\adminkit pode ser estimado aproximadamente usando a fórmula:

(724 * C + 0.15 * E + 0.17 * A), KB

onde:

- C é o número de dispositivos.

  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 de espaço em disco com o uso do recurso de Gerenciamento de patches e vulnerabilidades

- Atualizações. A pasta compartilhada requer ao menos 4 GB adicionais para armazenar as atualizações.

  Pacotes de instalação. Se alguns pacotes de instalação forem armazenados no Servidor de Administração, a pasta compartilhada necessitará de uma quantidade adicional de espaço em disco livre, igual ao tamanho total de todos os pacotes de instalação disponíveis para instalação.

- Tarefas de instalação remota. Se alguma tarefas de instalação remota estiverem presentes no Servidor de Administração, uma quantidade adicional de espaço livre no disco (na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit) igual ao tamanho total de todos os pacotes de instalação a ser instalados será necessário.

  Correções. Se o Servidor de Administração estiver envolvido na instalação de correções, uma quantidade adicional de espaço no disco será necessária:

  - A pasta de correções deve ter uma quantidade de espaço em disco igual ao tamanho total de todas as correções que foram baixadas. Por padrão, os patches são armazenados na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles.

    É possível usar o utilitário klsrvswch para especificar uma pasta diferente para armazenar patches. O utilitário klsrvswch 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.

    Se o Servidor de Administração for usado como o servidor WSUS, você é aconselhado a alocar ao menos 100 GB para esta pasta.

  - A pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit deve ter uma quantidade de e

da instalação da atualização (correção) e de tarefas de correção de vulnerabilidades.

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 cria um ícone para essa VM dinâmica no Console de Administração e move a VM dinâmica 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 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 e do Servidor de Administração e podem reduzir o desempenho do Kaspersky Security Center e do DBMS. Recomendamos que você conecte até 20.000 VMs dinâmicas ao Kaspersky Security Center.

Você pode conectar mais de 20.000 VMs dinâmicas ao Kaspersky Security Center se as VMs dinâmicas conectadas executarem operações padrão (por exemplo, atualizações do banco de dados) e consumirem não mais que 80% da memória e 75–80% 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

Para processar até 10.000 dispositivos cliente, um ponto de distribuição deve atender aos seguintes requisitos mínimos (é fornecida uma configuração para teste):

- CPU: Intel® Core™ i7-7700 CPU, 3,60 GHz 4 núcleos.
- RAM: 8 GB.

  Espaço de armazenamento livre: 120 GB.

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.

Calcular o número e a configuração de pontos de distribuição

Quanto mais dispositivos cliente 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 de cliente 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 exclusivamente atribuídos em uma rede que contém um segmento de rede único, com base no número de dispositivos na rede

Núm	

segmento da rede	
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 exclusivamente atribuídos em uma rede que contém vários segmentos de rede, com base no número de dispositivos na rede

Número de dispositivos cliente por 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 cliente padrão (estações de trabalho) como pontos de distribuição

Se você planejar usar dispositivos cliente 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 em o segmento da 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 por 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.

gateway de conexão pode cobrir no máximo 10.000 dispositivos gerenciados, inclusive dispositivos móveis.

Registro de informações sobre eventos de 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. Neste caso, recomenda-se 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.

Se uma política tiver sido definida para um número bem grande de dispositivos (por exemplo, mais de 10.000), o número de eventos também pode resultar ser 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.
- O Log de Eventos Kaspersky 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).

Considerações específicas e configurações ótimas de determinadas tarefas

Determinadas tarefas estão sujeitas a considerações específicas relativas ao número de dispositivos na rede. Esta seção c

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.

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:

- Backup de dados do Servidor de Administração

  Manutenção do banco de dados

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 de software

É possível reduzir a carga no banco de dados enquanto as informações sobre os aplicativos instalados são obtidas. Para fazer isso, recomendamos executar uma tarefa de inventário em dispositivos de referência nos quais um conjunto padrão de software está instalado.

O número de arquivos executáveis recebidos pelo Servidor de Administração de um único dispositivo não pode exceder 150.000. Quando o Kaspersky Security Center 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.

Medições de teste demonstraram que a tarefa de inventário tem os seguintes resultados em um dispositivo que executa o sistema operacional Windows 7 com o Kaspersky Endpoint Security 11 instalados e nenhum outro aplicativo de terceiros instalado:

Com as caixas de seleção **Inventário de módulos DLL** e **Inventário de arquivos de script** desmarcadas: aproximadamente 3000 arquivos.

- Com as caixas de seleção **Inventário de módulos DLL** e **Inventário de arquivos de script** marcadas: 10.000 a 20.000 arquivos, dependendo do número de service packs do sistema operacional instalados.
- Com somente a caixa de seleção **Inventário de arquivos de script** marcada: aproximadamente 10.000 arquivos.

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.

Consumo 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
Instalar o Kaspersky Endpoint Security 11.7 for Windows	390 MB	3.3 MB

com bancos de dados atualizados		
Instalação do Agente de Rede	75 MB	397 KB
Instalação simultânea do Agente de Rede e do Kaspersky Endpoint Security 11.7 for Windows	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
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.

Contatar o Suporte Técnico

Esta seção descreve como adquirir o suporte técnico e os termos com os quais está disponível.

Como obter suporte técnico

Caso não consiga encontrar uma solução para seu problema na documentação do Kaspersky Security Center ou em nenhuma das fontes de informação sobre o aplicativo, contate o Suporte Técnico da Kaspersky. Os especialistas do Suporte Técnico responderão a todas as suas dúvidas sobre instalação e uso do Kaspersky Security Center.

A Kaspersky fornece suporte para o Kaspersky Security Center durante o ciclo de vida útil (consulte a página de ciclo de vida de suporte do produto). 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 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 monitorar o status e também armazenar um histórico das suas solicitações online.

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
- Fran[illegible]

- Japonês

Para saber mais sobre o Kaspersky CompanyAccount, visite o site do Suporte Técnico.

Fontes de informação sobre o aplicativo

Página do Kaspersky Security Center no site da Kaspersky

Na página do Kaspersky Security Center no site da Kaspersky, é possível exibir informações gerais sobre o aplicativo, suas funções e recursos.

Página do Kaspersky Security Center na Base de conhecimento

A *Base de Dados de Conhecimento* é uma seção do site de suporte técnico da Kaspersky.

Na página do Kaspersky Security Center 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 como também a outros aplicativos 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 empresa cliente que é responsável por monitorar o status da proteção antivírus.

Administrador do Kaspersky Security Center

A pessoa que gerencia a operação de aplicativos através do sistema Kaspersky Security Center 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 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 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 Microsoft® Windows®. Existem versões separadas do Agente de Rede para os aplicativos da Kaspersky desenvolvidos os SO Unix e macOS.

Ambiente nuvem

Máquinas virtuais e outros recursos virtuais que são baseados em uma plataforma na nuvem e são combinados em redes.

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.

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.

Ataque de vírus

Uma série de tentativas deliberadas para infectar um dispositivo com um vírus.

Ataque MITM

Man in The Middle. Um ataque à infraestrutura de TI de uma organização no qual um hacker sequestra o link de comunicação entre dois pontos de acesso, o retransmite e modifica a conexão entre esses pontos de acesso, caso necessário.

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.

Atualizar

O procedimento de substituição ou inclusão de novos arquivos (bancos de dados ou módulos de aplicativo), recebidos a partir dos servidores de atualização da Kaspersky.

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:

- O banco de dados 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

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 que o Servidor de Administração usa para os seguintes propósitos:

- Autenticação de Servidor de Administração ao conectar-se ao Console de Administração baseado em MMC ou ao Kaspersky Security Center Web Console
- Interação segura entre o Servidor de Administração e os Agentes de Rede em dispositivos gerenciados
- Autenticação de Servidores de Administração ao conectar um Servidor de Administração principal a um Servidor de Administração secundário

O certificado é criado automaticamente quando o servidor de administração é instalado e, a seguir, armazenado no servidor de administração.

Chave ativa

Uma chave usada atualmente pelo aplicativo.

Chave de acesso AWS IAM

Uma combinação consistindo na ID da chave (que se parece com "AKIAIOSFODNN7EXAMPLE") e uma chave secreta (que se parece com "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Este par pertence ao Usuário do IAM e é usado para obter o acesso aos serviços AWS.

Chave de assinatura adicional

Uma chave que certifica que o usuário tem o direito de usar o aplicativo, mas que não está sendo usado no momento.

Configurações de Programa

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.

Configurações de tarefa

Configurações do aplicativo específicas para cada tipo de tarefa.

Console de Administração

Um componente do Kaspersky Security Center baseado no Windows (também chamado de Console de Administração baseado em MMC). Este componente fornece uma interface de usuário para os serviços administrativos do Servidor de Administração e do Agente de Rede.

Console de Gerenciamento AWS

A interface da Web para visualizar e gerenciar recursos AWS. Console de Gerenciamento AWS está disponível na Web em https://aws.amazon.com/pt/.

Direitos de administrador

O nível de direitos e privilégios do usuário para administração de objetos Exchange numa organização Exchange.

Dispositivo de proteção UEFI

O dispositivo com o Kaspersky Anti-Virus para UEFI integrado no nível da BIOS. A proteção integrada assegura a segurança do dispositivo do momento do início do sistema, enquanto a proteção nos dispositivos sem software integrado somente começa a funcionar após o início do aplicativo de segurança.

Dispositivo EAS

Um dispositivo móvel conectado ao Servidor de Administração através do protocolo Exchange ActiveSync. Os dispositivos com os sistemas operacionais iOS, Android e Windows Phone® podem ser conectados e gerenciados usando o protocolo Exchange ActiveSync.

Dispositivo KES

Um dispositivo móvel conectado a um Servidor de Administração do Kaspersky Security Center e gerenciado pelo aplicativo Kaspersky Endpoint Security for Android.

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

Um dispositivo no qual o Console de Administração está instalado ou que você usa para abrir o Kaspersky Security Center Web Console. Este componente fornece uma interface de gerenciamento do Kaspersky Security Center.

A estação de trabalho do administrador é usada para configurar e gerenciar o lado do servidor do Kaspersky Security Center. Usando a estação de trabalho, o administrador cria e gerencia um sistema centralizado de proteção antivírus para uma LAN corporativa, com base em aplicativos Kaspersky.

Função do IAM

Conjunto de direitos para fazer solicitações aos serviços com base no AWS. As funções do IAM não são vinculadas à um usuário específico ou grupo; elas fornecem direitos de acesso sem as chaves de acesso AWS IAM. Você pode atribuir uma função do IAM aos usuários IAM, instâncias EC2, e aplicativos com base em AWS ou serviços.

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 de identidades e acesso (IAM)

O serviço AWS que ativa o gerenciamento de acesso do usuário a outros serviços e recursos AWS.

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. Existem os seguintes 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 aplicativos licenciados

Um grupo de aplicativos criado com base no critério definido pelo administrador (por exemplo, por fornecedor), para o qual as estatísticas de instalações dos dispositivos cliente são mantidas.

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 da Web. HTTPS é usado para acessar informações restritas, como dados corporativos e financeiros.

Imagem de máquina da Amazon (AMI, Amazon Machine Image)

O modelo que contém a configuração do software necessária para executar a máquina virtual. Múltiplas instâncias podem ser criadas com base em uma única AMI.

Instalação forçada

O método para a instalação remota de aplicativos da Kaspersky que permite instalar o software em dispositivos cliente específicos. Para a conclusão com êxito da instalação forçada, a conta usada para essa tarefa deve ter direitos suficientes para a iniciar o aplicativo remotamente em dispositivos cliente. Esse método é recomendado para instalar aplicativos em dispositivos que executam os sistemas operacionais Microsoft Windows e que são compatíveis com essa funcionalidade.

Instalação local

Instalação de um aplicativo de segurança em um dispositivo em uma rede corporativa que supõe a inicialização de instalação manual do pacote de distribuição do aplicativo de segurança ou a inicialização manual de um pacote de instalação publicado que foi baixado previamente no dispositivo.

Instalação manual

A instalação de um aplicativo de segurança em um dispositivo na rede corporativa do 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.

Instância Amazon EC2

Uma máquina virtual criada com base em uma imagem AMI usando Amazon Web Services.

Interface do Programa de Aplicativo AWS (AWS API)

A interface de programação do aplicativo da plataforma AWS que é usada pelo Kaspersky Security Center. Especificamente, as ferramentas AWS API são usadas para a sondagem do segmento da nuvem e para instalar o Agente de Rede nas instâncias.

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 da Web. Para visualizar as páginas criadas ao utilizar o JavaScript, ative o suporte do JavaScript na configuração do seu navegador.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network é uma solução que dá a usuários de dispositivos com aplicativos instalados da Kaspersky acesso a bancos de dados de reputação do Kaspersky Security Network e outros dados estatísticos sem enviar dados dos dispositivos ao Kaspersky Security Network. O Kaspersky Private Security Network foi projetado para clientes corporativos que não podem participar do Kaspersky Security Network por algum dos seguintes motivos:

- Os dispositivos 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.

Kaspersky Security Network (KSN)

Uma infraestrutura de serviços online que fornece o acesso aos banco de dados da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software constantemente atualizadas. 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.

Limite de atividade de vírus

Número máximo permitido de eventos do tipo especificado dentro de um tempo limitado; quando excedido, é interpretado como um aumento da atividade de vírus e como uma ameaça de um ataque de vírus. Este recurso é importante durante períodos de ataques de vírus, já que permite aos administradores reagirem de modo oportuno às ameaças de ataques de vírus.

Loja de aplicativos

Componente do Kaspersky Security Center. 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 MDM do iOS

Conjunto de configurações para a conexão de dispositivos móveis iOS ao Servidor de Administração. O usuário instala um perfil de MDM do iOS a um dispositivo móvel, a partir do qual o dispositivo móvel conecta-se ao Servidor de Administração.

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

Um período durante o qual você tem acesso aos recursos do aplicativo e possui direitos de usar serviços adicionais. Os serviços que você pode usar dependem do tipo de licença.

Plugin de gerenciamento

Um componente especializado que fornece a interface para o gerenciamento de aplicativos através do Console de Administração. Cada aplicativo possui seu próprio plugin. Ele está incluído em todos os aplicativos Kaspersky que podem ser gerenciados através do Kaspersky Security Center.

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 várias políticas para aplicativos instalados nos computadores de cada grupo de administração, mas apenas uma política pode ser aplicada a cada aplicativo por vez em um grupo de administração.

Ponto de distribuição

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. O ponto de distribuição era anteriormente conhecido como agente de atualização.

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.

Proteção 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 da rede menta quando você usa aplicativos e serviços de segurança e ao aplicar e aderir à política de segurança de dos c

Provedor de serviço de proteção antivírus

Uma organização que fornece a uma organização cliente serviços de proteção antivírus com base nas soluções da Kaspersky.

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.

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:

- O banco de dados 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 computadores cliente

- Repositório dos arquivos de instalação para instalação remota de aplicativos (conteúdo das pastas: Pacotes, Atualizações de Desinstalação)

  Certificado do Servidor de Administração

Servidor de Administração

Um componente do Kaspersky Security Center que armazena centralmente informações sobre todos os aplicativos Kaspersky instalados na rede empresarial. Pode também ser usado para gerenciar estes aplicativos.

Servidor de Administração cliente (Dispositivo cliente)

Um dispositivo, servidor ou estação de trabalho no qual o Agente de Rede está instalado e os aplicativos Kaspersky gerenciados estão em execução.

rvid 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 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 (inclusive Servidores virtuais).

Servidor de dispositivos móveis

Um componente do Kaspersky Security Center que fornece acesso a dispositivos móveis e permite gerenciá-los através do Console de Administração.

Servidor de dispositivos móveis Exchange

Um componente do Kaspersky Security Center que permite conectar os dispositivos móveis Exchange ActiveSync com o Servidor de Administração.

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

Um componente do Kaspersky Security Center que é 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 MDM do iOS e arquivos de uma pasta compartilhada.

rvidores de atualização da Kaspersky

Servidores HTTP(S) 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 de proteção atual, que reflete o nível de segurança do computador.

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 segurança instalados, o uso de chaves de licença 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 computador 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.

Usuário do IAM