Para o Google Cloud, você só pode executar a implementação com as ferramentas nativas do Kaspersky Security Center. Se você selecionou o Google Cloud, a opção **Implementar a proteção** não está disponível.

Etapa 5. Seleção de um aplicativo para criar uma política e tarefas

Essa etapa só é exibida caso tenha pacotes de instalação e plug-ins para o Kaspersky Endpoint Security for Windows e o Kaspersky Security for Windows Server. Caso tenha um plugin e um pacote de instalação para apenas um desses aplicativos, essa etapa será ignorada e o Kaspersky Security Center criará uma política e tarefas para o aplicativo existente.

Selecione um aplicativo para o qual deseja criar uma política e tarefas:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

Etapa 6. Configurar o Kaspersky Security Network para o Kaspersky Security Center

Especifique as configurações para encaminhar informações sobre as operações do Kaspersky Security Center à Base de conhecimento da Kaspersky Security Network (KSN). Selecione uma das seguintes opções:

Concordo em usar a Kaspersky Security Network

O Kaspersky Security Center e os aplicativos gerenciados instalados nos dispositivos cliente transferem automaticamente seus detalhes de operação para o 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 usar a Kaspersky Security Network**

  O Kaspersky Security Center e os aplicativos gerenciados não fornecerão informações ao Kaspersky Security Network.

  Se você selecionar esta opção, o uso da Kaspersky Security Network será desativado.

A Kaspersky recomenda a participação na Kaspersky Security Network.

Os contratos da KSN para aplicativos gerenciados também podem ser exibidos. Se você concordar em usar a Kaspersky Security Network, o aplicativo gerenciado enviará dados para a Kaspersky. Se você não concordar em participar da Kaspersky Security Network, o aplicativo gerenciado não enviará dados para a Kaspersky. (Você pode alterar essa configuração posteriormente na política do aplicativo.)

Clique em **Avançar** para prosseguir.

Você poderá verificar a lista de políticas e tarefas que foram criadas.

Aguarde a conclusão da criação de políticas e tarefas e, em seguida, clique em **Avançar** para prosseguir. Na última página do assistente, clique no botão **Concluir** para sair.

Amostragem do segmento de rede por meio do Kaspersky Security Center Web Console

As informações sobre a estrutura da rede (e de seus dispositivos) são recebidas pelo Servidor de Administração por meio da amostragem regular de segmentos da nuvem usando as ferramentas AWS API, Azure API ou Google API. O Kaspersky Security Center usa estas informações para atualizar o conteúdo das pastas Dispositivos não atribuídos e Dispositivos gerenciados. Se você tiver configurado dispositivos a ser movidos automaticamente para grupos de administração, os dispositivos detectados são incluídos nos grupos de administração.

Para permitir que o Servidor de Administração faça amostragem dos segmentos da nuvem, você deve ter os direitos correspondentes fornecidos com uma função do IAM ou conta de usuário IAM (no AWS), com um ID do Aplicativo e senha (no Azure) ou com um e-mail de cliente Google, ID de projeto Google e chave privada (no Google Cloud).

Você pode adicionar e excluir conexões, assim como definir o agendamento da sondagem, para cada segmento da nuvem.

Adicionar conexões para a sondagem do segmento da nuvem

Para adicionar uma conexão para a sondagem do segmento da nuvem para a lista de conexões disponíveis:

1. No menu principal, vá para **Descoberta e implementação** → **Descoberta** → **Nuvem**.
2. Na janela que se abre, clique em **Propriedades**.
3. Na janela **Configurações** que se abre, clique em **Adicionar**.

   A janela **Configurações de segmento da nuvem** se abre.
4. Especifique o nome do ambiente em nuvem para a conexão que será usada para a sondagem adicional do segmento da nuvem:

   Ambiente em nuvem

   Selecione o ambiente em nuvem no qual você está implementando o Kaspersky Security Center: AWS, Azure ou Google Cloud.
   Caso planeje trabalhar com mais de um ambiente em nuvem, selecione um ambiente e execute o assistente novamente.

   Nome da conexão

Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

5. Insira suas credenciais para receber autorização no ambiente em nuvem que especificou.

- Se você selecionou AWS, especifique as seguintes configurações:

  - **Usar função do AWS IAM**

    Selecione esta opção se você já tiver criado uma função do IAM para o Servidor de Administração para usar os serviços AWS.

  - **Credenciais de conta de usuário IAM AWS**

    Selecione esta opção se você tiver uma conta de Usuário do IAM com as permissões necessárias e será possível inserir uma ID da chave e uma chave secreta.

    Se você especificou que tem Credenciais de conta de usuário IAM AWS, especifique o seguinte:

    ID da chave de acesso

    A ID da chave de acesso IAM é uma sequência de caracteres alfanuméricos. Você recebeu a ID da chave quando você criou a conta de usuário IAM.
    O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

    - **Chave secreta**

      A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

      Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

      O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

    Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

  Se você selecionou o Azure, especifique as seguintes configurações:

  - **ID do aplicativo Azure**

    Você criou este ID do aplicativo no portal do Azure.
    É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **ID da assinatura do Azure**

  Você criou a assinatura no portal do Azure.

- **Senha do aplicativo Azure**

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

- **Nome da conta de armazenamento Azure**

  Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center.

  Chave de acesso do armazenamento Azure

  Você recebeu uma senha (chave) quando criou a conta de armazenamento Azure para trabalhar com o Kaspersky Security Center.

  A chave está disponível na seção "Visão geral da conta de armazenamento Azure", na subseção "Chaves."

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

Se você selecionou o Google Cloud, especifique as seguintes configurações:

Endereço de e-mail do cliente

O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

ID do projeto

O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

6. Se quiser, clique em **Definir agendamento da sondagem** e altere as configurações padrão.

A conexão é salva nas configurações do aplicativo.

Após o novo segmento na nuvem ter sido amostrado pela primeira vez, um subgrupo que corresponde àquele segmento aparece no grupo de administração **Dispositivos gerenciados\Cloud**.

Se você especificar as credenciais incorretas, nenhuma instância será encontrada durante a amostragem do segmento na nuvem e um novo subgrupo não aparecerá no grupo de administração **Dispositivos gerenciados\Cloud**.

Excluindo uma conexão para sondagem do segmento da nuvem

Se não for mais necessário sondar um segmento da nuvem específico, é possível excluir a conexão correspondente àquele segmento da lista de conexões disponíveis. Também é possível excluir uma conexão se, por exemplo, as permissões para sondar um segmento da nuvem tiverem sido transferidas para o outro usuário com credenciais diferentes.

Para excluir uma conexão:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Nuvem**.
2. Na janela que se abre, clique em **Propriedades**.
3. Na janela **Configurações** que se abre, clique no nome do segmento que deseja excluir.
4. Clique em **Excluir**.
5. Na janela que se abre, clique no botão **OK** para confirmar a sua seleção.

A conexão é excluída. Os dispositivos no segmento da nuvem correspondentes a essa conexão são excluídos automaticamente dos grupos de administração.

Configurar o agendamento da amostragem por meio do Kaspersky Security Center Web Console

A amostragem do segmento da nuvem é executada segundo um agendamento. Você pode definir a frequência de sondagem.

A frequência de sondagem é automaticamente definida em 5 minutos nas definições Configurar o ambiente em nuvem. É possível alterar esse valor a qualquer momento e definir outro agendamento. Contudo, não é recomendado configurar a execução da sondagem mais frequentemente do que a cada 5 minutos porque isso pode levar a erros na operação da API.

Para configurar um agendamento da sondagem do segmento da nuvem:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Nuvem**.
2. Na janela que se abre, clique em **Propriedades**.
3. Na janela **Configurações** que se abre, clique no nome do segmento para o qual deseja configurar um agendamento de sondagem.

   Isso abre a janela **Configurações de segmento da nuvem**.

4. Na janela **Configurações de segmento da nuvem**, clique no botão **Definir agendamento da sondagem**.

   Isso abre a janela **Agendamento**.

5. Na janela **Agendamento**, defina as seguintes configurações:

   Início agendado

   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 padrão, a sondagem é executada a cada cinco minutos, iniciando na hora atual do sistema.

   - Por dias da semana

     A sondagem é executada regularmente, nos dias da semana e na hora especificados.

     Por padrão, a sondagem é executada todas as sextas-feiras às 18h.

   - Todos os meses em dias especificados das semanas selecionadas

     A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.
     Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

   Intervalo de início (min.)

   Especifique o valor de N (para minutos ou dias).

   A partir das

   Especifique quando iniciar a primeira sondagem.

   - 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 ativada.

6. Clique em **Salvar** para salvar as alterações.

O agendamento da sondagem para o segmento foi configurado e salvo.

Visualizar os resultados da amostragem de segmentos da nuvem por meio do Kaspersky Security Center Web Console

Você pode visualizar os resultados da amostragem de segmentos da nuvem, ou seja, visualizar a lista de dispositivos em nuvem gerenciados pelo Servidor de Administração.

Para visualizar os resultados da sondagem de segmentos da nuvem,

No menu principal, vá para **Descoberta e implementação** → **Descoberta** → **Nuvem**.

Isso exibe os segmentos de nuvem disponíveis para sondagem.

Visualizar as propriedades dos dispositivos na nuvem por meio do Kaspersky Security Center Web Console

É possível visualizar as propriedades de cada dispositivo na nuvem.

Para visualizar as propriedades de um dispositivo na nuvem:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

2. Clique no nome do dispositivo cujas propriedades deseja visualizar.
   Uma janela de propriedades é exibida com a seção **Geral** selecionada.

3. Caso queira visualizar as propriedades específicas de dispositivos na nuvem, selecione a seção **Sistema** na janela de propriedades.
   As propriedades são exibidas dependendo da plataforma na nuvem do dispositivo.

   Para os dispositivos na AWS, as seguintes propriedades são exibidas:

   - **Dispositivo descoberto usando API** (valor: **AWS**)
   - **R...**

- **VPC da nuvem**

  Zona de disponibilidade da nuvem

- **Subrede da nuvem**

  Cloud Placement Group (essa unidade será exibida apenas se a instância pertencer a um grupo de colocação; caso contrário, não será exibida)

Para os dispositivos no Azure, as seguintes propriedades são exibidas:

- **Dispositivo descoberto usando API** (valor: **Microsoft Azure**)
- **Região da nuvem**

  Subrede da nuvem

Para os dispositivos no Google Cloud, as seguintes propriedades são exibidas:

- **Dispositivo descoberto usando API** (valor: **Google Cloud**)
- **Região da nuvem**
- **VPC da nuvem**

  Zona de disponibilidade da nuvem

- **Subrede da nuvem**

Sincronização com a nuvem: configuração da regra móvel

Durante a operação de Configurar o ambiente em nuvem, a regra sincronizar com a nuvem é criada automaticamente. Esta regra permite mover automaticamente os dispositivos detectados em cada sondagem, do grupo Dispositivos não atribuídos para o grupo Dispositivos gerenciados\Nuvem para tornar estes dispositivos disponíveis para o gerenciamento centralizado. Por padrão, a regra está ativa após ter sido criada. Você pode desativar, modificar ou forçar a regra a qualquer momento.

Para editar as propriedades da regra de Sincronizar com a nuvem e/ou forçar a regra:

1. No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Regras de migração**.

   Isso abre uma lista de regras de movimentação.

2. Na lista de regras de movimentação, selecione **Sincronizar com a nuvem**.

   Isso abre a janela de propriedades da regra.

3. Se necessário, especifique as seguintes configurações na guia **Condições da regra**, na guia **Segmentos da nuvem**:

   O dispositivo está no segmento da nuvem

A regra só é aplicada aos dispositivos que estão no segmento da nuvem selecionado. Caso contrário, a regar se aplica a todos os dispositivos que tenham sido descobertos.

Por padrão, esta opção está selecionada.

- Incluir objetos secundários

  A regra se aplica a todos os dispositivos no segmento selecionado e em todas as subsecções da nuvem aninhadas. Caso contrário, a regra só é aplicada aos dispositivos que estão no segmento raiz.
  Por padrão, esta opção está selecionada.

Migrar dispositivos de objetos aninhados para os subgrupos correspondentes

Se essa opção é ativada, os dispositivos de objetos aninhados são automaticamente movidos aos subgrupos que correspondem à sua estrutura.
Se essa opção é desativada, os dispositivos de objetos aninhados são automaticamente movidos para a raiz do subgrupo Nuvem sem nenhuma ramificação adicional.

Por padrão, esta opção está ativada.

- Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente

  Se esta opção estiver ativada, quando a estrutura do grupo **Dispositivos gerenciados\Nuvem** não tiver nenhum subgrupo que corresponda à seção que contém o dispositivo, o Kaspersky Security Center criará os subgrupos. Por exemplo, se uma nova sub-rede for descoberta durante a descoberta de dispositivos, um novo grupo com o mesmo nome será criado abaixo do grupo **Dispositivos gerenciados\Nuvem**.

  Se esta opção estiver desativada, o Kaspersky Security Center não criará nenhum novo subgrupo. Por exemplo, se uma nova sub-rede for descoberta durante a sondagem da rede, um novo grupo com o mesmo nome não será criado sob o grupo **Dispositivos gerenciados\Nuvem**, e os dispositivos naquela sub-rede serão movidos para o grupo **Dispositivos gerenciados\Nuvem**.
  Por padrão, esta opção está ativada.

Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem

Se esta opção estiver ativada, o aplicativo excluirá do grupo Nuvem todos os subgrupos que não correspondem a nenhum dos objetos da nuvem existentes.
Se esta opção estiver desativada, os subgrupos que não correspondem a nenhum dos objetos da nuvem existentes serão mantidos.

Por padrão, esta opção está ativada.

Caso tenha ativado a opção **Sincronizar grupos de administração com estrutura de nuvem** ao usar Configurar o ambiente em nuvem, a regra **Sincronizar com a nuvem** é criada com as opções **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente** e **Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem** ativadas.

Se você não ativou a opção **Sincronizar grupos de administração com estrutura de nuvem**, a regra **Sincronizar com a nuvem** é criada com essas opções desativadas (desmarcadas). Se o seu trabalho com o Kaspersky Security Center precisar que a estrutura de subgrupos no subgrupo **Dispositivos gerenciados\Nuvem** coincida com a estrutura dos segmentos da nuvem, ative as opções **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente** e **Excluir subgrupos sem corr**

4. Na lista suspensa **Dispositivo detectado usando a API**, selecione um dos seguintes valores:

   Não. O dispositivo não pode ser detectado usando AWS, Azure ou Google API, ou seja, está fora do ambiente em nuvem ou está no ambiente em nuvem, mas não pode ser detectado usando uma API por algum motivo.

   - **AWS**. O dispositivo é descoberto usando AWS API, ou seja, o dispositivo está definitivamente no ambiente nuvem do AWS.

     Azure. O dispositivo é descoberto usando Azure API, ou seja, o dispositivo está definitivamente no ambiente nuvem do Azure.

     Google Cloud. O dispositivo é descoberto usando Google API, ou seja, o dispositivo está definitivamente no ambiente nuvem do Google.

   - Nenhum valor. Este critério não pode ser aplicado.

5. Se necessário, defina outras propriedades da regra nas outras seções.

A regra de movimentação é configurada.

Instalação remota de aplicativos nas máquinas virtuais do Azure

Você deve ter uma licença válida para instalar aplicativos nas máquinas virtuais do Microsoft Azure.

O Kaspersky Security Center suporta os seguintes cenários:

- Um dispositivo cliente é detectado via API do Azure. A instalação é executada por meio de uma API. Usar a API do Azure significa que será possível instalar os seguintes aplicativos:
  - Kaspersky Endpoint Security for Linux

    Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- Um dispositivo cliente é detectado por meio da Azure API. A instalação é realizada por meio de ponto de distribuição ou, se não houver um ponto de distribuição, manualmente, usando pacotes de instalação independente. Você pode instalar qualquer aplicativo compatível com o Kaspersky Security Center desta forma.

Para criar uma tarefa para instalação remota do aplicativo nas máquinas virtuais do Azure:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.

3. Siga as instruções do assistente:

   a. Selecionar **Instalar o aplicativo remotamente** como o tipo de tarefa.

   b. Na página **Pacotes de instalação**, selecione **Instalação remota pela API do Microsoft Azure**.

c. Ao selecionar a conta para acessar os dispositivos, use uma conta existente do Azure ou clique em **Adicionar** e insira as credenciais de sua conta do Azure:

- Nome da conta do Azure

  Digite qualquer nome para as credenciais que você está especificando. Este nome será exibido na lista das contas a executarem a tarefa.

  ID do aplicativo Azure

  Você criou este ID do aplicativo no portal do Azure.

  É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- Senha do aplicativo Azure

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

d. Selecione os dispositivos relevantes no grupo **Dispositivos gerenciados\Nuvem**.

Após a conclusão do assistente, a tarefa para a instalação remota do aplicativo aparece na lista de tarefas.

Criação da tarefa de Backup dos dados do Servidor de Administração usando um DBMS na nuvem

Tarefas de Backup são tarefas do Servidor de Administração. Você cria uma tarefa de backup se desejar usar um DBMS localizado em um ambiente de nuvem (AWS ou Azure).

Para criar uma tarefa de backup de dados do Servidor de Administração:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.
   O Assistente para novas tarefas inicia.
3. Na primeira página do assistente, na lista **Aplicativo**, selecione **Kaspersky Security Center 14.2**, e na lista **Tipo de tarefa**, selecione **Backup de dados do Servidor de Administração**.
4. Na página correspondente do assistente, especifique as seguintes informações:

   Se estiver trabalhando com um banco de dados no AWS:

   - Nome do bucket S3

     O nome do S3 bucket que você criou para o Backup.

- **ID da chave de acesso**

  Você recebeu o ID da chave (sequência de caracteres alfanuméricos) quando criou a Conta de Usuário do IAM para trabalhar com a instância de armazenamento do S3 bucket.

  O campo está disponível se você selecionou o banco de dados RDS em um S3 bucket.

- **Chave secreta**

  A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

  Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

  O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

- Se estiver trabalhando com um banco de dados no Microsoft Azure:

  - **Nome da conta de armazenamento do Azure**

    Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center.

  - **ID de assinatura do Azure**

    Você criou a assinatura no portal do Azure.

  - **Senha do Azure**

    Você recebeu a senha quando criou o ID do aplicativo.

    Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

  - **ID do aplicativo Azure**

    Você criou este ID do aplicativo no portal do Azure.

    É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

  - **Nome do servidor Azure SQL**

    O nome e o grupo do recurso estão disponíveis nas propriedades do Azure SQL Server.

  - **Grupo de recursos do servidor Azure SQL**

    O nome e o grupo do recurso estão disponíveis nas propriedades do Azure SQL Server.

- Chave de acesso ao armazenamento do Azure

  Disponível nas propriedades da conta de armazenamento, na seção Chaves de Acesso. Você pode usar qualquer uma das chaves (key1 ou key2).

A tarefa é criada e exibida na lista de tarefas. Caso a opção **Abrir detalhes da tarefa quando a criação for concluída** seja habilitada, será possível modificar as configurações padrão da tarefa imediatamente após a criação. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

Diagnóstico remoto de dispositivos cliente

É possível usar o diagnóstico remoto para execução remota das seguintes operações nos dispositivos clientes:

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.

O diagnóstico remoto é realizado usando o Servidor de Administração.

Abertura da janela de diagnóstico remoto

Para executar diagnóstico remoto em um dispositivo cliente, 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, vá para **Dispositivos → Dispositivos gerenciados**.
   - Caso o dispositivo pertença ao grupo de dispositivos não atribuídos, No menu principal, vá para **Descoberta e implementação → Dispositivos não atribuídos**.

   Clique no nome do dispositivo necessário.

3. Na janela de propriedades do dispositivo exibida, selecione a guia **Avançado**.

4. Na janela que se abre, clique em **Diagnóstico remoto**.
   Isso abre a janela de **Diagnóstico remoto** do dispositivo cliente.

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, clique em **Diagnóstico remoto**.

3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.

   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.

4. Na lista de aplicativos, selecione o aplicativo para o qual deseja ativar ou desativar o rastreamento.
   A lista de opções de diagnóstico remoto é exibida.

5. Se desejar ativar o rastreamento:

   a. Na seção **Rastreamento** da lista, 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. Estão disponíveis as seguintes configurações:

   - **Nível de rastreamento**

     O nível de rastreamento define o volume de detalhes que o arquivo de rastreamento contém.

     Rastreamento baseado em rotatividade

     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 em **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.

6. Caso deseje desativar o rastreamento para o aplicativo selecionado, clique em **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:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.

   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.
4. 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.
5. Na seção **Rastreamento do Xpref** da lista, clique em **Ativar rastreio do Xperf**.
   Se o rastreamento do Xperf já estiver ativado, o botão **Desativar rastreamento Xperf** é exibido.
6. 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* e podem ser solicitadas pelos especialistas de 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 na reinicialização

  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 pode receber a solicitação de ativar a opção **Tamanho do arquivo de rotatividade, 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 em **Salvar**.

O rastreamento do Xperf está ativado e configurado.

Para desativar o rastreamento do Xperf:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.

   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.
4. Na lista de aplicativos, selecione Kaspersky Endpoint Security for Windows.
   As opções de rastreamento do Kaspersky Endpoint Security for Windows são exibidas.
5. Na seção **Rastreamento do Xpref** da lista, clique em **Desativar rastreamento Xperf**.

   Se o rastreamento do Xperf já estiver desativado, o botão **Ativar rastreamento Xperf** é exibido.

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, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.
   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.

Na s

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 o arquivo desejado.
5. Execute uma das seguintes ações:
   - Faça o download do arquivo selecionado clicando em **Baixar todo o arquivo**.
   - Baixe uma parte do arquivo selecionado:
     a. Clique em **Baixar uma parte**.
     b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada, de acordo com suas necessidades.
     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 exibida, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, verifique se a seção **Registros do sistema operacional** está selecionada.
4. Na seção **Arquivos de rastreamento**, clique no botão **Logs do Windows Update** ou **Logs de instalação remota**, dependendo de quais arquivos de rastreamento deseja excluir.
   Isso abre a lista de arquivos de rastreio.
5. Na lista de arquivos de rastreamento, selecione o arquivo que deseja excluir.
6. Clique no botão **Remover**.

O arquivo de rastreamento selecionado é excluído.

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 exibida, clique em **Diagnóstico remoto**.

3. Na janela **Status e logs** que se abre, certifique-se de que o **Registros do sistema operacional** esteja selecionado no painel direito.
   - Na seção **Informações do sistema**, clique no botão **Baixar arquivo** para baixar as informações do sistema sobre o dispositivo cliente.
   - Na seção **Configurações do aplicativo**, clique no botão **Baixar arquivo** para baixar informações sobre as configurações dos aplicativos instalados no dispositivo.

As informações são baixadas no local especificado como um arquivo.

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, clique em **Logs do dispositivo**.
3. Na janela **Todos os logs do dispositivo**, selecione o log relevante.
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**.

     b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada, de acordo com suas necessidades.

     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, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.
   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.
4. Na lista de aplicativos, selecione o aplicativo que deseja iniciar, parar ou reiniciar.

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 de um aplicativo e download dos resultados

Para iniciar o diagnóstico para um aplicativo 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, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.
   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.
4. Na lista de aplicativos, selecione o aplicativo para o qual deseja executar o diagnóstico remoto.

   A lista de opções de diagnóstico remoto é exibida.
5. Na seção **Relatório de diagnóstico** da lista, 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.
6. Baixe o relatório clicando no botão **Baixar o relatório de diagnóstico**.

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.

Para executar um aplicativo no dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto exibida, clique em **Diagnóstico remoto**.

3. Na janela **Status e logs** exibida, selecione a seção **Executando um aplicativo remoto**.

4. Na janela **Executando um aplicativo remoto**, na seção **Arquivos do aplicativo**, siga um destes procedimentos, de acordo com o que o especialista da Kaspersky solicitar que você faça:

   Selecione um arquivo comprimido contendo o aplicativo que deseja executar no dispositivo cliente clicando no botão **Procurar**.

   > O arquivo comprimido deve incluir a pasta do utilitário. Essa pasta contém o arquivo executável a ser executado em um dispositivo remoto.

   - Especifique um aplicativo de linha de comando e seus argumentos, se necessário. Para fazer isso, preencha os campos **Arquivo executável em um arquivo comprimido para ser executado em um dispositivo remoto** e os campos **Argumentos da linha de comando**.

5. Clique no botão **Carregar e executar** para executar o aplicativo especificado em um dispositivo cliente.

6. Siga as instruções do especialista.

Gerar um arquivo de dump para um aplicativo

Um arquivo de despejo do aplicativo permite visualizar os parâmetros do aplicativo em execução em um dispositivo cliente em um dado momento. Esse arquivo também contém informações sobre os módulos que foram carregados para um aplicativo.

> A geração de arquivos de despejo está disponível apenas para processos de 32 bits em execução em dispositivos cliente baseados no Windows. Para processos de 64 bits, esse recurso não é compatível.

Para criar um arquivo de despejo para um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto exibida, clique em **Diagnóstico remoto**.

3. Na janela **Status e logs** exibida, selecione a seção **Executando um aplicativo remoto**.

4. Na seção **Gerando o arquivo de dump do processo**, especifique o arquivo executável do aplicativo para o qual deseja gerar um arquivo de despejo.

5. Clique no botão **Baixar arquivo de dump** para salvar o arquivo de despejo do aplicativo especificado.

   Caso o aplicativo especificado não esteja em execução no dispositivo cliente, a mensagem de erro será exibida.

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, acesse as configurações da conta e, a seguir, selecione **Idioma**.
2. Selecione um dos idiomas compatíveis com a localização.

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 pode não querer tratar manualmente usando o Console de Administração. Você também pode implementar cenários personalizados que ainda não são compatíveis no Console de Administração. 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. Por exemplo, é possível desenvolver um Console de Administração baseado em MMC alternativo para seus clientes, que permite um conjunto limitado de ações.

No Guia de referência da OpenAPI, é possível usar o campo de pesquisa à direita da tela para localizar as informações necessárias.

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 você pode chamar métodos OpenAPI e realizar automaticamente várias tarefas para proteger sua rede, por exemplo, criar uma hierarquia "principal/secundária", executar tarefas no Kaspersky Security Center 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:

1. Baixe o arquivo KlAkOAPI.tar.gz. Este arquivo inclui o pacote e exemplos KlAkOAPI (você pode copiá-los do arquivo ou do guia de referência OpenAPI). O arquivo KlAkOAPI.tar.gz também está localizado na pasta de instalação do Kaspersky Security Center.
2. Instale o pacote KlAkOAPI do arquivo KlAkOAPI.tar.gz em um dispositivo onde o Servidor de Administração está instalado.
   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.

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.	Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de

		Administração secundário ▪ Excluir uma hierarquia de Servidores de Administração
Criar a hierarquia do grupo com uma estrutura baseada na unidade do Active Directory	É possível pesquisar a unidade do Active Directory e formar uma hierarquia de grupos de dispositivos descobertos.	Criação de grupos de administração
Criar a hierarquia do grupo com uma estrutura baseada na unidade do Active Directory em cache	É possível formar uma hierarquia dos grupos de dispositivos gerenciados com base na unidade do Active Directory pesquisada anteriormente. Se novos dispositivos aparecerem no Active Directory após a última pesquisa, eles não serão adicionados ao grupo porque não estão nos resultados de pesquisa salvos.	Criação de grupos de administração
Baixar arquivos de lista de rede por meio do gateway de conexão para o dispositivo 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
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 uma tarefa para um 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
Criar subredes IP com base no site e nos serviços do Active Directory	É possível criar uma subrede IP com base na unidade do Active Directory usada por você. No exemplo, é iniciada a pesquisa do intervalo de IP especificado, excluindo as subredes descobertas para evitar conflito com uma nova subrede. Portanto, não execute as operações desse exemplo em uma rede onde é importante salvar subredes.	Configuração da proteção da rede

	Após a pesquisa, o exemplo é referenciado no Active Directory, examina todos os dispositivos nele e cria a subrede IP. Para tanto, no exemplo são usadas máscaras e endereços IP de todos os dispositivos.	
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.	Monitoramento de execução de tarefa
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 expiração.	Visualizando de informações sobre chaves de licença em uso
Criar e encontrar um usuário interno	É possível criar uma conta para trabalhos futuros.	Selecionar a conta para iniciar o Servidor de Administração

personalizada	parâmetros necessários.	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.	Como gerenciar contas de usuário

Aplicativos que interagem com o Kaspersky Security Center via OpenAPI

Alguns aplicativos interagem com o Kaspersky Security Center via OpenAPI. Esses aplicativos incluem, por exemplo, Kaspersky Anti Targeted Attack Platform ou Kaspersky Security for Virtualization. Também pode ser um aplicativo cliente personalizado, desenvolvido por terceiros, baseado em OpenAPI.

Os aplicativos que interagem com o Kaspersky Security Center via 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 o Kaspersky Security Center OpenAPI 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.

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.

Planejar a implementação do Kaspersky Security Center

Ao planejar a implementação dos componentes do Kaspersky Security Center em uma rede da organização você deve levar em conta 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 100.000 dispositivos. Se o número total de dispositivos na rede de uma organização exceder 100.000, 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 necessitado 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 Console de Administração
- Porta 8060 TCP – HTTP para publicar pacotes independentes usando ferramentas do Console de Administração
- Porta 13292 TCP – Porta TLS somente é necessária se houver dispositivos móveis que precisam de ser gerenciados

Caso tenha de fornecer aos clientes as opções básicas de administração de rede pelo Kaspersky Security Center Web Console, será necessário também abrir a porta TCP 8080 (porta HTTPS) do Kaspersky Security Center Web Console.

Configuração padrão do Kaspersky Security Center

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 100.000 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 necessitado 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 que corresponde a um cliente MSP, você deve 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 provavelmente não será capaz de amostrar a rede cliente MSP, pode ser útil passar essa 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 (caixa de seleção **Não desconectar do Servidor de Administração**). Este modo de conexão contínua está disponível se o número total de pontos de distribuição não exceder 300.

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:

- Distribuir atualizações (estas podem ser recuperadas do Servidor de Administração ou dos servidores da 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.
- 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 busca 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

Um MSP pode executar múltiplos Servidores de Administração. Pode ser inconveniente administrar diversos Servidores de Administração separados, portanto uma hierarquia pode ser aplicada. Uma configuração de "principal / secundário" para dois Servidores de Administração fornece as seguintes opções:

Um Servidor de Administração secundário herda as políticas e tarefas 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.

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.

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.

Gerenciar dispositivos móveis com o Kaspersky Endpoint Security for Android

Os dispositivos móveis com o Kaspersky Endpoint Security for Android™ instalado (aqui referidos como dispositivos KES) são gerenciados por meio do Servidor de Administração. O Kaspersky Security Center oferece suporte aos seguintes recursos para gerenciar dispositivos do KES:

- Tratar dispositivos móveis como dispositivos cliente:

  Associação em grupos de administração

  - Monitoramento, como visualização de status, eventos e relatórios
  - Modificar as configurações locais e atribuir políticas para o Kaspersky Endpoint Security for Android

  Enviar comandos em modo centralizado
- Instalar pacotes de aplicativos móveis remotamente

O Servidor de Administração gerencia dispositivos KES por meio de TLS, pela porta TCP 13292.

Implementação e configuração inicial

O Kaspersky Security Center é um aplicativo distribuído. O Kaspersky Security Center suporta os seguintes aplicativos:

- Servidor de Administração – o componente principal, projetado para gerenciar os dispositivos de uma organização e armazenar dados em um DBMS.
- Console de Administração – A ferramenta básica do administrador. A Console de Administração é fornecido junto com o Servidor de Administração, mas também pode ser instalado individualmente em um ou diversos dispositivos executados pelo administrador.
- 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 em uma rede da organização é executada como segue:

- Instalação do Servidor de Administração
- Instalação do Kaspersky Security Center Web Console

  Instalação do Console de Administração no dispositivo do administrador
- 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

Por padrão, o instalador automaticamente cria contas não-privilegiadas para os serviços do Servidor de Administração. Este comportamento é o mais conveniente para a instalação do Servidor de Administração em um dispositivo comum.

No entanto, a instalação do Servidor de Administração em um cluster de correção de falha necessita de um cenário diferente:

1. Crie contas de domínio não privilegiado para os serviços do Servidor de Administração e torne-as membros de um grupo de segurança de domínio global denominado KL Admins.