Agora, o usuário pode fazer login no Kaspersky Security Center com a conta personalizada e monitorar as estatísticas de proteção de rede no modo somente painel.

Relatórios

Esta seção descreve como usar relatórios, gerenciar modelos de relatórios personalizados, usar modelos de relatórios para gerar novos relatórios e criar tarefas de entrega de relatórios.

Usar os relatórios

O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las.

Os relatórios estão disponíveis no Kaspersky Security Center Web Console, na seção **Monitoramento e relatórios**, clicando em **Relatórios**.

Por padrão, os relatórios contém informações dos últimos 30 dias.

O Kaspersky Security Center tem um conjunto padrão de relatórios para as seguintes categorias:

- **Status da proteção**

  Implementação

- **Atualizando**

  Estatísticas de ameaças

- **Outro**

Você pode criar modelos de relatório personalizados, editar modelos de relatório e excluí-los.

Você pode criar relatórios que são baseados em modelos existentes, exportar relatórios para arquivos e criar tarefas para entrega de relatório.

Criação de um modelo de relatório

Para criar um modelo de relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. Clique em **Adicionar**.

   O assistente de novo modelo de relatório é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
3. Na primeira página do assistente, digite o nome de relatório e selecione o tipo de relatório.
4. Na página **Escopo** do assistente, selecione o conjunto de dispositivos cliente (grupo de administração, seleção de dispositivos, dispositivos selecionados ou todos os dispositivos em rede) cujos dados serão exibidos em relat

5. Na página **Período do relatório** do assistente, especifique o período de relatório. Os valores disponíveis são:

   Entre as duas datas especificadas

   - A partir da data especificada até à data de criação do relatório

     Desde a data de criação do relatório menos o número especificado de dias, até a data de criação do relatório

   Essa página pode não aparecer para alguns relatórios.

6. Clique em **OK** para fechar o assistente.

7. Execute uma das seguintes ações:

   Clique no botão **Salvar e executar** para salvar o novo modelo de relatório e executar um relatório baseado nele.

   O modelo de relatório é salvo. O relatório é gerado.

   Clique no botão **Salvar** para salvar o novo modelo de relatório.

   O modelo de relatório é salvo.

Você pode usar o novo modelo para gerar e visualizar relatórios.

Visualização e edição das propriedades do modelo de relatório

Você pode visualizar e editar propriedades básicas de um modelo de relatório como, por exemplo, o nome do modelo de relatório ou os campos exibidos no relatório.

Para visualizar e editar propriedades de um modelo de relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.

2. Marque a caixa de seleção ao lado do modelo de relatório cujas propriedades deseja visualizar e editar.

   Como uma alternativa, você pode primeiro gerar o relatório e depois clicar no botão **Editar**.

3. Clique no botão **Abrir propriedades do modelo de relatório**.

   A janela **Edição de relatório <Nome do relatório>** é exibida com a guia **Geral** selecionada.

4. Edite as propriedades do modelo de relatório:

   - Guia **Geral**:

     Nome do modelo de relatório

     - Número máximo de entradas a exibir

Se esta opção estiver ativada, o número de entradas exibidas na tabela com dados de relatório detalhados não será maior que o valor especificado.

As entradas de relatório são primeiro classificadas segundo as regras especificadas na seção **Campos → Campos de detalhes** das propriedades do modelo de relatório e, em seguida, apenas a primeira das entradas resultantes é mantida. O cabeçalho da tabela com dados de relatório detalhados mostra o número de entradas exibidas e o número total de entradas disponíveis que combinam com outras configurações do modelo de relatório.

Se esta opção estiver desativada, a tabela com dados de relatório detalhados exibe todas as entradas disponíveis. Não recomendamos que você desative essa opção. Limitar o número de entradas de relatório exibidas reduz a carga do sistema de gerenciamento de banco de dados (DBMS) e reduz o tempo necessário para gerar e exportar o relatório. Alguns dos relatórios contêm entradas excessivas. Se este for o caso, você pode ter dificuldade para ler e analisar todas elas. Além disso, o seu dispositivo pode ficar sem memória ao gerar um relatório e, consequentemente, você não poderá exibir o relatório.

Por padrão, esta opção está ativada. O valor predefinido é de 1.000.

- **Grupo**

  Clique no botão **Configurações** para alterar o conjunto de dispositivos cliente para os quais o relatório é criado. Para alguns tipos dos relatórios, o botão pode estar indisponível. As configurações reais dependem das configurações especificadas durante a criação do modelo de relatório.

- **Intervalo de tempo**

  Clique no botão **Configurações** para modificar o período de relatório. Para alguns tipos dos relatórios, o botão pode estar indisponível. Os valores disponíveis são:

  - Entre as duas datas especificadas

    A partir da data especificada até à data de criação do relatório

  - Desde a data de criação do relatório menos o número especificado de dias, até a data de criação do relatório

Incluir dados dos Servidores de Administração secundários e virtuais

Se esta opção estiver ativada, o relatório inclui as informações dos Servidores de Administração secundário e virtual subordinados ao Servidor de Administração para o qual o modelo de relatório é criado.

Desative esta opção se você quiser visualizar dados somente do Servidor de Administração atual.

Por padrão, esta opção está ativada.

- **Até o nível de aninhamento**

  O relatório inclui dados de servidores de administração secundários e virtuais localizados sob o Servidor de administração atual a um nível de agrupamento menor ou igual ao valor especificado.

  O valor padrão é 1. Convém alterar esse valor caso necessite recuperar as informações dos Servidores de administração secundários localizados em níveis mais baixos na árvore.

Intervalo de espera dos dados (min.)

Antes de gerar o relatório, o Servidor de administração para o qual o modelo de relatório é criado aguarda pelos dados de Servidores de administração secundários durante o número de minutos especificado. Se nenhum dado for recebido de um Servidor de administração secundário ao fim desse período, o relatório é executado mesmo assim. Em vez de dados reais, o relatório exibe os dados retirados do cache (se a opção **Dados em cache dos Servidores de Administração secundários** estiver ativada) ou, caso contrário, **N/A** (não acessível).
O valor predefinido é de 5 (minutos).

- **Dados em cache dos Servidores de Administração secundários**

Os Servidores de Administração secundários regularmente transferem dados para o Servidor de Administração para o qual o modelo de relatório é criado. Nesse local, os dados transferidos são armazenados em cache.
Se o Servidor de administração atual não puder receber dados de um Servidor de administração secundário enquanto o relatório estiver sendo gerado, o relatório exibirá dados retirados do cache. A data em que os dados foram transferidos para o cache também é exibida.

Ativar essa opção permite a visualização das informações dos Servidores de administração secundários, mesmo se os dados atualizados não puderem ser recuperados. Entretanto, os dados exibidos podem ser obsoletos.

Por padrão, esta opção está desativada.

- **Frequência de atualização de cache (h)**

Os Servidores de administração secundários regularmente transferem dados para o Servidor de administração para o qual o modelo de relatório é criado. É possível especificar o período em horas. Se o valor for 0, os dados serão transferidos somente quando o relatório for gerado.

O valor padrão é 0.

- **Transferir informações detalhadas dos Servidores de Administração secundários**

No relatório gerado, a tabela contendo dados de relatório detalhados inclui dados dos Servidores de Administração secundários do Servidor de Administração para o qual o modelo de relatório é criado.

Ativar esta opção reduz a velocidade de geração de relatórios e aumenta o tráfego entre Servidores de Administração. Entretanto, você pode visualizar todos os dados em um relatório.
Em vez de ativar a opção, convém analisar dados de relatório detalhados para detectar um Servidor de administração secundário defeituoso e, em seguida, gerar o mesmo relatório apenas para o Servidor de administração defeituoso.

Por padrão, esta opção está desativada.

Guia **Campos**

Selecione os campos que serão exibidos no relatório e use os botões **Para cima** e **Para baixo** para alterar a ordem desses campos. Use o botão **Adicionar** ou **Editar** para especificar se as informações no relatório devem ser classificadas e filtradas segundo cada um dos campos.
Na seção **Filtros dos campos Detalhes**, você também pode clicar em **Converter filtros** para começar a usar o formato de filtragem estendido. Este formato permite combinar as condições de filtragem especificadas em vários campos, usando a operação lógica OR. Depois de clicar no botão, o painel **Converter filtros** abre à direita. Clique no botão **Converter filtros** para confirmar a conversão. Agora, você pode definir um filtro convertido com as condições da seção **Campos de detalhes**, que são aplicadas usando a operação lógica OR.

A conversão de um relatório para o formato compatível com as condições de filtragem complexas tornará o relatório incompatível com as versões anteriores do Kaspersky Security Center (11 e anteriores). Além disso, o relatório convertido não conterá nenhum dado dos Servidores de Administração secundários executando tais versões incompatíveis.

5. Clique em **Salvar** para salvar as alterações.
6. Feche a janela **Editar relatório <Nome do relatório>**.

O modelo de relatório atualizado aparece na lista de modelos de relatório.

Exportar um relatório para um arquivo

Você pode exportar um relatório para um arquivo XML, HTML ou PDF.

Para exportar um relatório para um arquivo:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. Marque a caixa de seleção ao lado do relatório que deseja exportar para um arquivo.
3. Clique no botão **Exportar relatório**.
4. Na janela exibida, altere o nome do arquivo de relatório no campo **Nome**. Por padrão, o nome do arquivo coincide com o nome do modelo de relatório selecionado.
5. Selecione o tipo de arquivo de relatório: XML, HTML ou PDF.
6. Clique no botão **Exportar relatório**.

   O relatório no formato selecionado será baixado para o seu dispositivo (para a pasta padrão do seu dispositivo), ou uma janela padrão **Salvar como** será exibida no navegador para permitir que você salve o arquivo onde quiser.

O relatório é salvo no arquivo.

Como gerar e visualizar um relatório

Para criar e visualizar um relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. Clique no nome do modelo de relatório que deseja usar para criar um relatório.

Um relatório usando o modelo selecionado é gerado e exibido.

Os dados do relatório são exibidos de acordo com a localização definida para o Servidor de Administração.

- Na guia **Resumo**:

  O nome e tipo de relatórios, uma breve descrição e o período de relatórios, assim como as informações sobre o grupo de dispositivos para os quais o relatório é gerado.

  Gráfico que mostra os dados do relatório mais representativos.

  - Tabela consolidada com os indicadores do relatório calculados.

- Na guia **Detalhes**, uma tabela com dados detalhados do relatório é exibida.

Criação de uma tarefa de entrega de relatório

Você pode criar uma tarefa que entregará os relatórios selecionados.

Para criar uma tarefa de entrega de um relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. [Opcional] Marque as caixas de seleção ao lado dos modelos de relatório para os quais deseja criar uma tarefa de entrega de relatório.
3. Clique no botão **Nova tarefa de entrega de relatórios**.
4. O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
5. Na primeira página do assistente, digite o nome da tarefa. O nome padrão é **Entregar relatórios (<N>)**, em que <N> é o número de sequência da tarefa.
6. Na página de configurações da tarefa do assistente, especifique as seguintes configurações:
   a. Modelos de relatório a serem entregues pela tarefa. Caso os tenha selecionado na etapa 2, ignore esta etapa.
   b. O formato do relatório: HTML, XLS ou PDF.
   c. Se os relatórios precisarem ser enviados por e-mail, em conjunto com as configurações de notificação por e-mail.
   d. Se os relatórios precisarem ser salvos em uma pasta, se os relatórios anteriormente salvos nessa pasta precisarem ser sobrescrito e se uma conta específica precisar ser usada para acessar a pasta (para uma pasta compartilhada).
7. Se você deseja modificar outras configurações de tarefa após a criação da tarefa, na página **Concluir a criação da tarefa** do assistente, habilite a opção **Abrir detalhes da tarefa quando a criação for concluída**.
8. Clique no botão **Criar** para criar a tarefa e fechar o assistente.

   A tarefa de entrega de relatório é criada. Se você ativou a opção **Abrir detalhes da tarefa quando a criação for concluída**, a janela de configurações da tarefa é aberta.

:cluir os modelos de relatório

Para excluir um ou vários modelos de relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. Marque as caixas de seleção ao lado dos modelos de relatório que deseja excluir.
3. Clique no botão **Excluir**.
4. Na janela que se abre, clique em **OK** para confirmar a sua seleção.

Os modelos de relatório selecionados são excluídos. Se esses modelos de relatório tiverem sido incluídos nas tarefas de entrega de relatório, eles também serão removidos das tarefas.

Eventos e seleções de eventos

Esta seção fornece informações sobre eventos e seleções de eventos, sobre os tipos de eventos que ocorrem nos componentes do Kaspersky Security Center e sobre como gerenciar o bloqueio de eventos frequentes.

Sobre os eventos do Kaspersky Security Center

O Kaspersky Security Center lhe permite receber informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nestes dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração.

Tipos de eventos

No Kaspersky Security Center, há os seguintes tipos de eventos:

- Eventos gerais. Esses eventos ocorrem em todos os aplicativos Kaspersky gerenciados. Um exemplo de um evento geral é um Surto de vírus. Eventos gerais têm sintaxe e semântica estritamente definidas. Eventos gerais são usados, por exemplo, em relatórios e painéis.
- Eventos gerenciados específicos de aplicativos Kaspersky. Cada aplicativo Kaspersky gerenciado tem o seu próprio conjunto de eventos.

Fontes de eventos

Os eventos podem ser gerados pelos seguintes aplicativos:

- Componentes do Kaspersky Security Center:
  - Servidor de Administração
  - Agente de Rede
  - Servidor MDM do iOS
  - Servidor de dispositivos móveis Exchange

- Aplicativos gerenciados pela Kaspersky

  Para obter detalhes sobre os eventos gerados pelos aplicativos gerenciados pela Kaspersky, consulte a documentação do aplicativo correspondente.

É possível visualizar a lista completa dos eventos que podem ser gerados por um aplicativo na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar a lista de eventos nas propriedades do Servidor de Administração.

Nível de importância dos eventos

Cada evento tem o seu próprio nível de importância. Dependendo das condições da sua ocorrência, a um evento pode ser atribuídos diversos níveis de importância. Há quatro níveis de importância de eventos:

- Um *evento crítico* é um evento que indica a ocorrência de um problema crítico que pode levar à perda de dados, um funcionamento operacional ruim ou um erro crítico.
- Uma *falha funcional* é um evento que indica a ocorrência de um problema sério, erro ou funcionamento incorreto que ocorreu durante a operação do aplicativo ou ao executar um procedimento.
- Um *aviso* é um evento que não necessariamente é sério, mas no entanto indica um problema potencial no futuro. A maior parte de eventos são indicados como avisos se o aplicativo puder ser restaurado sem perda dos dados ou capacidades funcionais após a ocorrência de tais eventos.
- Um evento *de informação* é um evento que ocorre para fins de informar sobre conclusão bem sucedida de uma operação, funcionamento apropriado do aplicativo ou conclusão de um procedimento.

Cada evento tem um prazo de armazenamento definido, durante o qual você pode exibi-lo ou modificá-lo no Kaspersky Security Center. Alguns eventos não são salvos no banco de dados do Servidor de Administração por padrão porque o seu prazo de armazenamento definido é zero. Somente os eventos que serão armazenados no banco de dados do Servidor de Administração por ao menos um dia podem ser exportados aos sistemas externos.

Usar as seleções de eventos

As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. Esses conjuntos de eventos são agrupados de acordo com as seguintes categorias:

Por nível de importância – **Eventos críticos**, **Falhas funcionais**, **Advertências** e **Eventos de informações**

- Por tempo – **Eventos recentes**

Por tipo – **Pedidos de usuário** e **Eventos de auditoria**

Você pode criar e visualizar seleções de eventos definidas pelos usuários baseado nas configurações disponíveis para configuração na interface do Kaspersky Security Center Web Console.

As seleções de eventos estão disponíveis no Kaspersky Security Center Web Console, na seção **Monitoramento e relatórios**, clicando em **Seleções de eventos**.

Por padrão, as seleções de eventos incluem informações dos últimos sete dias.

O Kaspersky Security Center tem um conjunto padrão de seleções de eventos (predefinidas):

Eventos com níveis de importância diferentes:

- **Eventos críticos**

  Falhas funcionais

- **Advertências**

  Mensagens informativas

- **Solicitações de usuário** (eventos de aplicativos gerenciados)
- **Eventos recentes** (na semana passada)
- Eventos de auditoria.

Você também pode criar e configurar seleções adicionais definidos pelo usuário. Em seleções definidas pelos usuários, é possível filtrar eventos pelas propriedades dos dispositivos dos quais se originaram (nomes de dispositivos, conjuntos de IPs e grupos de administração), por tipos de evento e níveis de gravidade, por aplicativo e nome do componente e por intervalo de tempo. Também é possível incluir resultados da tarefa no escopo de pesquisa. Você também pode usar um campo de pesquisa simples em que uma palavra ou várias palavras podem ser digitadas. São exibidos todos os eventos que contêm alguma das palavras digitadas em qualquer lugar nos seus atributos (como nome do evento, descrição, nome do componente).

Para seleções predefinidas e definidas pelos usuários, você pode limitar o número de eventos exibidos ou o número de registros para pesquisar. Ambas as opções afetam o tempo necessário para o Kaspersky Security Center exibir os eventos. Quanto maior for o banco de dados, mais demorado será o processo.

Você pode fazer o seguinte:

Editar propriedades das seleções de eventos

- Gerar seleções de eventos

  Visualizar detalhes das seleções de eventos

- Excluir seleções de eventos
- Excluir eventos do banco de dados do Servidor de Administração

Criar uma seleção de eventos

Para criar uma seleção de eventos:

1. No menu principal, vá para **Monitoramento e relatórios** → **Seleções de eventos**.
2. Clique em **Adicionar**.
3. Na janela **Nova seleção de eventos** que se abre, especifique as configurações da nova seleção de eventos. Faça isso em uma ou mais das seções na janela.
4. Clique em **Salvar** para salvar as alterações.

   A janela de confirmação é exibida.

5. Para visualizar o resultado da seleção de eventos, mantenha a caixa de seleção **Ir para o resultado da seleção** selecionada.

6. Clique em **Salvar** para confirmar a criação da seleção de eventos.

Se você tiver mantido a caixa de seleção **Ir para o resultado da seleção** selecionada, o resultado da seleção de eventos será exibido. Caso contrário, a nova seleção de eventos será exibida na lista de seleção de eventos.

Editar uma seleção de eventos

Para editar uma seleção de eventos:

1. No menu principal, acesse **Monitoramento e relatórios → Seleções de eventos**.
2. Marque a caixa de seleção ao lado da seleção de eventos que deseja editar.
3. Clique no botão **Propriedades**.

   Uma janela de configurações de seleção de eventos é aberta.
4. Edite as propriedades da seleção de eventos.

   Para seleções de eventos predefinidas, você pode editar somente as propriedades nas seguintes guias: **Geral** (exceto o nome de seleção), **Hora** e **Direitos de acesso**.

   Para seleções definidas pelos usuários, você pode editar todas as propriedades.
5. Clique em **Salvar** para salvar as alterações.

A seleção de eventos editada é mostrada na lista.

Visualizando uma lista de uma seleção de eventos

Para visualizar a seleção de eventos:

1. No menu principal, acesse **Monitoramento e relatórios → Seleções de eventos**.
2. Marque a caixa de seleção ao lado da seleção de eventos que deseja iniciar.
3. Execute uma das seguintes ações:

   - Se você quiser configurar a classificação no resultado da seleção de eventos, faça o seguinte:

     a. Clique no botão **Reconfigurar classificação e iniciar**.

     b. Na janela exibida **Reconfigurar classificação para seleção de eventos**, especifique as configurações de classificação.

     c. Clique no nome da seleção.

   - Caso contrário, se você quiser visualizar a lista de eventos e como eles estão classificados no Servidor de Administração, clique no nome da seleção.

O resultado da seleção de eventos é exibido.

Excluir as seleções de eventos

Você pode excluir apenas as seleções de eventos definidas pelo usuário. As seleções de eventos predefinidas não podem ser excluídas.

Para excluir uma ou várias seleções de eventos:

1. No menu principal, acesse **Monitoramento e relatórios** → **Seleções de eventos**.
2. Marque as caixas de seleção ao lado das seleções de eventos que deseja excluir.
3. Clique em **Excluir**.
4. Na janela que se abre, clique em **OK**.

A seleção de eventos é excluída.

Visualização dos detalhes de um evento

Para visualizar detalhes de um evento:

1. Nova seleção de eventos.
2. Clique na hora do evento necessário.

   A janela **Propriedades do evento** se abre.
3. Na janela exibida, você pode fazer o seguinte:

   - Visualizar as informações sobre o evento selecionado
   - Ir ao evento anterior e ao seguir no resultado da seleção de eventos
   - Ir ao dispositivo no qual o evento ocorreu

     Ir ao grupo de administração que inclui o dispositivo no qual o evento ocorreu
   - Para um evento relacionado a uma tarefa, vá às propriedades da tarefa

Exportar eventos para um arquivo

Para exportar eventos para um arquivo:

1. Nova seleção de eventos.
2. Selecione a caixa de seleção junto ao evento necessário.
3. Clique no botão **Exportar para arquivo**.

O evento selecionado é exportado para um arquivo.

Exportando eventos para os sistemas SIEM

Esta seção descreve como configurar a exportação de eventos para os sistemas SIEM.

Cenário: configurando a exportação de eventos para um sistema SIEM

O Kaspersky Security Center permite a configuração por um dos seguintes métodos: exportação para qualquer sistema SIEM que use o formato Syslog, exportação para sistemas QRadar, Splunk, ArcSight SIEM que usam formatos LEEF e CEF ou exportação de eventos para sistemas SIEM diretamente do banco de dados do Kaspersky Security Center. Ao concluir este cenário, o Servidor de Administração envia eventos ao sistema SIEM automaticamente.

Pré-requisitos

Antes de iniciar a exportação de configuração de eventos no Kaspersky Security Center:

- Saiba mais sobre os métodos de exportação de eventos.

  Certifique-se de que tem conhecimento dos os valores das configurações do sistema.

Você pode executar as etapas deste cenário em qualquer ordem.

O processo de exportação de eventos para o sistema SIEM consiste nos seguintes passos:

Configurando o sistema SIEM para receber eventos do Kaspersky Security Center

Instruções: Configurando a exportação de eventos em um sistema SIEM

- **Selecionando os eventos que deseja exportar para o sistema SIEM:**

  Instruções de como proceder:

  - Console de Administração: Marcando eventos de um aplicativo Kaspersky para exportação em formato Syslog, Marcando eventos gerais para exportação em formato Syslog
  - Kaspersky Security Center Web Console: Marcando eventos de um aplicativo Kaspersky para exportação em formato Syslog, Marcando eventos gerais para exportação em formato Syslog

- **Configurando a exportação de eventos para o sistema SIEM usando um dos seguintes métodos:**

  - Usando TCP/IP, UDP ou TLS via protocolos TCP.

- Console de Administração: configurando a exportação de eventos para sistemas SIEM
- Kaspersky Security Center Web Console: configurando a exportação de eventos para sistemas SIEM

- Com o uso da exportação de eventos diretamente do banco de dados do Kaspersky Security Center (um conjunto de visualizações públicas é fornecido no banco de dados do Kaspersky Security Center. É possível encontrar a descrição dessas visualizações públicas no documento klakdb.chm).

Resultados

Após configurar a exportação de eventos para o sistema SIEM, você pode ver os resultados de exportação se tiver selecionado eventos que deseja exportar.

Antes de iniciar

Ao configurar uma exportação automática de eventos no Kaspersky Security Center, você deve especificar algumas das configurações do sistema SIEM. Recomenda-se que você verifique estas configurações com antecedência para preparar-se para configurar o Kaspersky Security Center.

Para configurar com êxito o envio automático de eventos a um sistema SIEM, você deve conhecer as seguintes configurações:

Endereço do servidor do sistema SIEM

O endereço IP do servidor onde o sistema SIEM atualmente usado está instalado. Verifique este valor nas suas configurações de sistema SIEM.

Porta do servidor do sistema SIEM

O número da porta usada para estabelecer a conexão entre o Kaspersky Security Center e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center e nas configurações do receptor do seu sistema SIEM.

Protocolo

Protocolo usado para transferir mensagens do Kaspersky Security Center ao seu sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center e nas configurações do receptor do seu sistema SIEM.

Sobre a exportação de evento

Você pode usar a exportação de evento dentro de sistemas centralizados que tratam de questões de segurança em nível organizacional e técnico, que fornecem serviços de monitoramento da segurança e consolidam informações de diferentes soluções. Estes são sistemas SIEM, que fornecem a análise em tempo real de alertas de segurança e eventos gerados por hardware de rede e aplicativos ou Centros de Operação de Segurança (SOCs).

Estes sistemas recebem dados de muitas fontes, incluindo redes, segurança, servidores, bancos de dados e aplicativos. Os sistemas de SIEM também fornecem a funcionalidade para consolidar os dados monitorados para ajudá-lo a evitar faltar a eventos críticos. Além disso, os sistemas executam a análise automatizada de eventos correlacionados e alertas para notificar os administradores de problemas de segurança imediatos. Um alerta pode ser implementado através de um painel ou pode ser enviado por canais de terceiros, tal como por um e-mail.

O processo de exportar eventos do Kaspersky Security Center para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center) e um receptor do evento (sistema SIEM). Para exportar com sucesso eventos, você deve configurar isso no seu sistema SIEM e no Console de Administração do Kaspersky Security Center. Não importa que lado você configura primeiro. Você pode configurar a transmissão de eventos no Kaspersky Security Center e depois configurar o recebimento de eventos pelo sistema SIEM, ou vice-versa.

Métodos para enviar eventos do Kaspersky Security Center

Há três métodos para enviar eventos do Kaspersky Security Center aos sistemas externos:

Enviando eventos sob o protocolo Syslog à qualquer sistema SIEM

Usando o protocolo Syslog, você pode encaminhar qualquer evento que ocorre no Servidor de Administração do Kaspersky Security Center e em aplicativos Kaspersky que são instalados em dispositivos gerenciados. O protocolo Syslog é um protocolo de registro de mensagem padrão. É possível usá-lo para exportar os eventos para qualquer sistema SIEM.

Para isso, é preciso marcar os eventos que deseja retransmitir ao sistema SIEM. É possível marcar os eventos no console de administração ou no Kaspersky Security Center Web Console. Apenas os eventos marcados serão retransmitidos para o sistema SIEM. Caso não tenha marcado nada, nenhum evento será retransmitido.

- Enviando eventos sobre os protocolos CEF e LEEF para os sistemas QRadar, Splunk e ArcSight

  Você pode usar os protocolos CEF e LEEF para exportar eventos gerais. Ao exportar eventos sobre os protocolos CEF e LEEF, você não tem a capacidade de selecionar eventos específicos para exportar. Em vez disso, todos os eventos gerais são exportados. Diferentemente do protocolo Syslog, os protocolos CEF e LEEF não são universais. CEF e LEEF são destinados para os sistemas SIEM apropriados (QRadar, Splunk e ArcSight). Portanto, quando você escolhe exportar eventos através de um desses protocolos, você usa o analisador necessário no sistema SIEM.

  Para exportar eventos através dos protocolos CEF e LEEF, o recurso Integração com dos sistemas SIEM deve ser ativado no Servidor de Administração usando uma chave de licença ativa ou um código de ativação válido.

- Diretamente do banco de dados do Kaspersky Security Center para qualquer sistema SIEM

  Este método de exportar eventos pode ser usado para receber eventos diretamente das vistas públicas do banco de dados por meio de consultas SQL. Os resultados de uma consulta são salvos em um arquivo XML que pode ser usado como dados de entrada para um sistema externo. Somente os eventos disponíveis nas vistas públicas podem ser exportados diretamente do banco de dados.

Recebimento de eventos pelo sistema SIEM

O sistema SIEM deve receber e corretamente analisar os eventos recebidos do Kaspersky Security Center. Para estes propósitos, você deve configurar apropriadamente o sistema SIEM. A configuração depende do sistema SIEM específico utilizado. No entanto, há um número de etapas gerais na configuração de todos os sistemas SIEM, tal como a configuração do receptor e do analisador.

Sobre a configuração de exportação de eventos em um sistema SIEM

O processo de exportar eventos do Kaspersky Security Center para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center) e um receptor do evento (sistema SIEM). Você deve configurar a exportação de eventos no seu sistema SIEM e no Kaspersky Security Center.

As configurações especificadas no sistema SIEM dependem de qual sistema que você estiver usando. Normalmente, para todos os sistemas SIEM você deve definir um receptor e, opcionalmente, um analisador de mensagem para analisar os eventos recebidos.

Configurar o receptor

Para poder receber eventos enviados pelo Kaspersky Security Center, configure o receptor no seu sistema SIEM. Em geral, as seguintes configurações devem ser especificadas no sistema SIEM:

- **Protocolo para exportar ou tipo de entrada**

  É o protocolo de transferência de mensagem, TCP/IP ou UDP. Este protocolo deve ser o mesmo protocolo que você especificou no Kaspersky Security Center.

  Porta

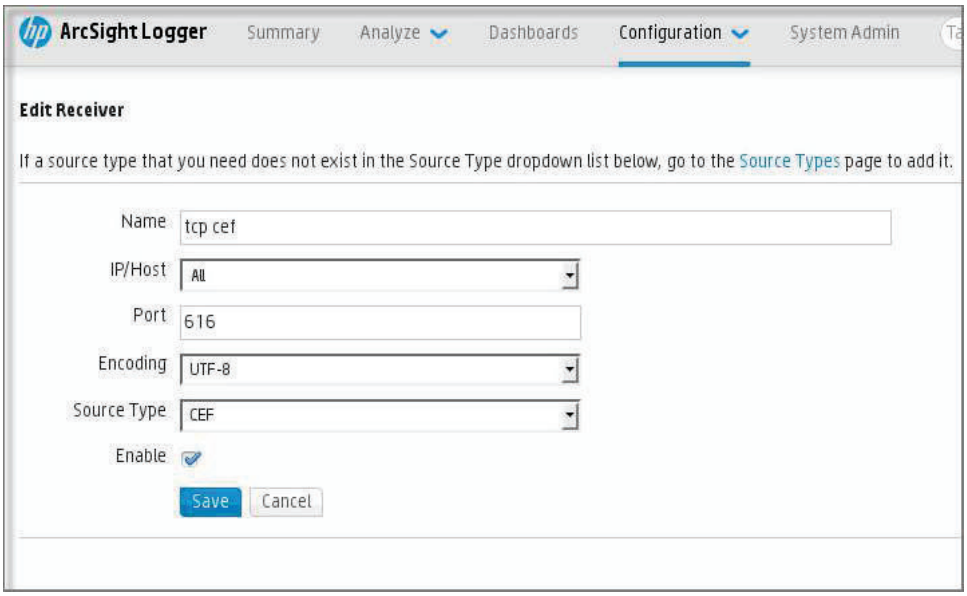
  Número da porta para conectar-se ao Kaspersky Security Center. Esta porta deve ser a mesma que a porta que você especificou no Kaspersky Security Center.

- **Protocolo de mensagem ou tipo de origem**

  O protocolo usado para exportar eventos ao sistema SIEM. Pode ser um dos protocolos padrão: Syslog, CEF ou LEEF. O sistema SIEM seleciona o analisador de mensagem de acordo com o protocolo que você especifica.

Dependendo do sistema SIEM usado, você pode ter que especificar algumas configurações adicionais de receptor.

A figura abaixo mostra tela de configuração de receptor no ArcSight.



Configuração do receptor no ArcSight

Analisador de mensagem

Os eventos exportados são passados aos sistemas SIEM como mensagens. Estas mensagens devem ser apropriadamente analisadas para que as informações nos eventos possam ser usadas pelo sistema SIEM. Os analisadores de mensagem são uma parte do sistema SIEM; eles são usados para dividir o conteúdo da mensagem em campos relevantes, tal como ID do evento, gravidade, descrição, parâmetros e assim por diante. Isto ativa o sistema SIEM para processar eventos recebidos do Kaspersky Security Center para que eles possam ser armazenados no banco de dados do sistema SIEM.

Marcando eventos para exportação para sistemas SIEM em formato Syslog

Esta seção descreve como marcar eventos para exportação adicional para sistemas SIEM no formato Syslog.

Sobre a marcação de eventos para exportação para o sistema SIEM no formato Syslog

Após ativar a exportação automática de eventos, você deve selecionar quais eventos serão exportados ao sistema SIEM externo.

Você pode configurar a exportação de eventos em formato Syslog para um sistema externo com base em uma das seguintes condições:

Marcando eventos gerais. Se você marcar eventos para exportar em uma política, nas configurações de um evento ou no Servidor de Administração, o sistema SIEM receberá os eventos marcados que ocorreram em todos os aplicativos gerenciados pela política específica. Se os eventos exportados foram selecionados na política, você não será capaz de redefini-los para um aplicativo individual gerenciado por esta política.

- Marcando eventos para um aplicativo individual. Se você marcar eventos para exportar para um aplicativo gerenciado instalado em um dispositivo gerenciado, o sistema SIEM somente receberá os eventos que ocorreram neste aplicativo.

Marcando eventos de um aplicativo da Kaspersky para exportação em formato Syslog

Se você desejar exportar eventos que ocorreram em um aplicativo gerenciado específico instalado nos dispositivos gerenciados, marque os eventos para exportação na política do aplicativo. Nesse caso, os eventos marcados são exportados de todos os dispositivos incluídos no escopo da política.

Para marcar eventos para exportação para um aplicativo gerenciado específico:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique na política do aplicativo para o qual você deseja marcar eventos.

   A janela Propriedades da política será aberta.
3. Siga para a seção **Configuração de eventos**.
4. Marque as caixas de seleção ao lado dos eventos que você deseja exportar para um sistema SIEM.
5. Clique no botão **Marcar exportação para o sistema SIEM usando o Syslog**.

   Também é possível marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, que é aberta ao clicar no link do evento.
6. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.
7. Clique no botão **Salvar**.

Os eventos marcados do aplicativo gerenciado estão prontos para serem exportados para um sistema SIEM.

É possível marcar quais eventos exportar para um sistema SIEM para um dispositivo gerenciado específico. Se os eventos exportados anteriormente foram marcados em uma política de aplicativo, não será possível redefinir os eventos marcados para um dispositivo gerenciado.

Para marcar eventos para exportação para um dispositivo gerenciado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
   A lista de dispositivos gerenciados é exibida.
2. Clique no link com o nome do dispositivo desejado na lista de dispositivos gerenciados.

   A janela Propriedades do dispositivo selecionado é exibida.
3. Siga para a seção **Aplicativos**.
4. Clique no link com o nome do aplicativo desejado na lista de aplicativos.
5. Siga para a seção **Configuração de eventos**.
6. Marque as caixas de seleção ao lado dos eventos que deseja exportar para um arquivo.
7. Clique no botão **Marcar exportação para o sistema SIEM usando o Syslog**.

   Além disso, você pode marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, aberta ao se clicar no link do evento.
8. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.

A partir de agora, o Servidor de Administração envia os eventos marcados para o sistema SIEM se a exportação para o sistema SIEM estiver configurada.

Marcando eventos gerais para exportação no formato Syslog

Você pode marcar eventos gerais que o Servidor de Administração exportará para os sistemas SIEM usando o formato Syslog.

Para configurar eventos gerais para um sistema SIEM:

1. Execute uma das seguintes ações:
   - No menu principal, clique no ícone de configurações () ao lado do nome do Servidor de Administração necessário.
   - No menu principal, vá para **Dispositivos** → **Políticas e perfis** e clique no link de uma política.
2. Na janela aberta, vá para **Configuração de eventos**.
3. Clique em **Marcar exportação para o sistema SIEM usando o Syslog**.

   Além disso, você pode marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, aberta ao se clicar no link do evento.
4. O sinal de verificação () aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.

A partir de agora, o Servidor de Administração envia os eventos marcados para o sistema SIEM se a exportação para o sistema SIEM estiver configurada.

Sobre a exportação de eventos usando formatos CEF e LEEF

Você pode usar os formatos CEF e LEEF para exportar eventos gerais, bem como eventos transferidos pelos aplicativos Kaspersky para o Servidor de Administração. O conjunto de eventos exportado é predefinido, e você não pode selecionar os eventos a ser exportados.

Para exportar eventos através dos protocolos CEF e LEEF, o recurso Integração com dos sistemas SIEM deve ser ativado no Servidor de Administração usando uma chave de licença ativa ou um código de ativação válido.

Selecione o formato de exportação com base no sistema SIEM usado. A tabela abaixo mostra os sistemas SIEM e os formatos de exportação correspondentes.

Formatos da exportação de eventos para um sistema SIEM

SIEM system	Formato de exportação
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Formato Estendido de Evento de Log) – Um formato de evento customizado para o IBM Security QRa

codificação de caractere UTF-8. Você pode encontrar as informações detalhadas sobre o protocolo LEEF no IBM Knowledge Center.

- CEF (Formato de Evento Comum) – Um padrão de gerenciamento de registro aberto que aprimora a interoperabilidade da informação relativa a segurança de diferentes dispositivos de segurança e de rede e aplicativos. O CEF lhe permite usar um formato de registro de evento comum para que os dados possam ser facilmente integrados e agregados para a análise por um sistema de gerenciamento corporativo.

A exportação automática significa que o Kaspersky Security Center envie eventos gerais ao sistema SIEM. A exportação automática de eventos inicia imediatamente após você a ativar. Esta seção explica detalhadamente como ativar a exportação automática de eventos.

Sobre a exportação de eventos usando o formato Syslog

Você pode usar o formato Syslog para exportar aos sistemas SIEM os eventos que ocorrem no Servidor de Administração e em outros aplicativos Kaspersky instalados em dispositivos gerenciados.

Syslog é um padrão para o protocolo de registro da mensagem. Isso permite a separação do software que gera mensagens, o sistema que as armazena e o software que os reporta e os analisa. Cada mensagem é legendada com um código de instalação, indicando o tipo de software que gera a mensagem e à mesma é atribuído um nível de gravidade.

O formato Syslog é definido por documentos de Solicitação de Comentários (RFC) publicados pela Internet Engineering Task Force (padrões da Internet). O padrão RFC 5424 é usado para exportar os eventos do Kaspersky Security Center aos sistemas externos.

No Kaspersky Security Center, você pode configurar a exportação dos eventos aos sistemas externos usando o formato Syslog.

O processo de exportação consistem em duas etapas:

1. Ativar a exportação automática do evento. Nesta etapa, o Kaspersky Security Center é configurado para que ele envie eventos ao sistema SIEM. O Kaspersky Security Center começa a enviar eventos imediatamente após você ativar a exportação automática.

2. Selecionar os eventos a ser exportados ao sistema externo. Nesta etapa, você seleciona qual evento exportar ao sistema SIEM.

Configurando o Kaspersky Security Center para exportação de eventos para o sistema SIEM

Este artigo descreve como configurar a exportação de eventos para sistemas SIEM.

Para configurar a exportação para sistemas SIEM no Kaspersky Security Center Web Console:

1. No menu principal, vá para **Configurações do console** → **Integração**.

2. Na guia **Integração**, selecione a seção **SIEM**.

3. Clique no link **Configurações**.

   A seção **Exportar as configurações** é aberta.

4. Especifique as configurações na seção **Exportar as configurações**:

Endereço do servidor do sistema SIEM

O endereço IP do servidor onde o sistema SIEM atualmente usado está instalado. Verifique este valor nas suas configurações de sistema SIEM.

- **Porta do sistema SIEM**

  O número da porta usada para estabelecer a conexão entre o Kaspersky Security Center e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center e nas configurações do receptor do seu sistema SIEM.

- **Protocolo**

Selecione o protocolo a ser usado para transferir mensagens para o sistema SIEM. Você pode selecionar o TCP/IP, UDP ou TLS sobre protocolo TCP.

Especifique as seguintes configurações de TLS se selecionar o protocolo TLS sobre TCP:

- **Autenticação do servidor**

  No campo **Autenticação do servidor**, você pode selecionar os valores de **Certificados confiáveis** ou de **Impressões digitais SHA**:

  - **Certificados confiáveis**. Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação (CA) confiável e carregá-lo para o Kaspersky Security Center. O Kaspersky Security Center verifica se o certificado do servidor do sistema SIEM também é assinado por CAs confiáveis ou não.

    Para adicionar um certificado confiável, clique no botão **Procurar arquivo de certificados CA** e, em seguida, carregue o certificado.

  - **Impressões digitais SHA**. Você pode especificar as impressões digitais SHA-1 dos certificados do sistema SIEM no Kaspersky Security Center. Para adicionar uma impressão digital SHA-1, insira-a no campo **Impressões digital** e, em seguida, clique no botão **Adicionar**.

  Ao usar a configuração **Adicionar autenticação do cliente**, você pode gerar um certificado para autenticar o Kaspersky Security Center. Assim, você usará um certificado autoassinado emitido pelo Kaspersky Security Center. Nesse caso, você pode usar um certificado confiável e uma impressão digital SHA para autenticar o servidor do sistema SIEM.

- **Adicionar nome do assunto/Nome alternativo do assunto**

  Nome do assunto é um nome de domínio para o qual o certificado foi recebido. O Kaspersky Security Center não pode se conectar ao servidor do sistema SIEM se o nome de domínio do servidor do sistema SIEM não corresponder ao nome da entidade do certificado do servidor do sistema SIEM. No entanto, o servidor do sistema SIEM pode alterar seu nome de domínio se o nome tiver sido alterado no certificado. Neste caso, você pode especificar nomes de assuntos no campo **Adicionar nome do assunto/Nome alternativo do assunto**. Se qualquer um dos nomes de assunto especificados corresponder ao nome do assunto do certificado do sistema SIEM, o Kaspersky Security Center valida o certificado do servidor do sistema SIEM.

  Adicionar autenticação do cliente

  Para autenticação de cliente, você pode inserir o seu certificado ou gerá-lo no Kaspersky Security Center.

  Inserir certificado. Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer CA confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

  - **Certificado X.509 PEM**. Carregue um arquivo com um certificado no campo **Arquivo com certificado** e um arquivo com uma chave privada no campo **Arquivo com chave**. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Quando os dois arquivos forem carregados, especifique a senha para decodificar a chave privada no campo **Verificação de senha ou certificado**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

  - **Certificado X.509 PKCS12**. Carregue um único arquivo que contenha um certificado e sua chave privada no campo **Arquivo com certificado**. Quando o arquivo for carregado, especifique a senha para decodificar a chave privada no campo **Verificação de senha ou certificado**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- **Gerar chave**. Você pode gerar um certificado autoassinado no Kaspersky Security Center.
  Como resultado, o Kaspersky Security Center armazena o certificado autoassinado gerado e você pode passar a parte pública do certificado ou a impressão digital SHA1 para o sistema SIEM.

Formato de data

Você pode selecionar os formatos Syslog, CEF ou LEEF, dependendo dos requisitos do sistema SIEM.

Se selecionar o formato Syslog, você deve especificar:

- **Tamanho máximo da mensagem de eventos, em bytes**

  Especifique o tamanho máximo (em bytes) de uma mensagem encaminhada ao sistema SIEM. Cada evento é encaminhado em uma mensagem. Se o comprimento real de uma mensagem exceder o valor especificado, a mensagem é truncada e os dados podem ser perdidos. O tamanho padrão é de 2.048 bytes. Este campo somente está disponível se você selecionou o formato Syslog no campo **Protocolo**.

5. Alterne a opção para a posição **Exportar automaticamente os eventos para o banco de dados do sistema SIEM Ativado**.

6. Clique no botão **Salvar**.

A exportação para o sistema SIEM está configurada.

Exportando eventos diretamente do banco de dados

Você pode recuperar eventos diretamente do banco de dados do Kaspersky Security Center sem ter necessidade de usar a interface Kaspersky Security Center. Você pode consultar as vistas públicas diretamente e recuperar os dados de evento ou criar as suas próprias vistas com base em vistas públicas existentes e endereçá-las para receber os dados de que precisa.

Vistas públicas

Para a sua conveniência, um conjunto de vistas públicas é fornecido no banco de dados do Kaspersky Security Center. Você pode encontrar a descrição destas vistas públicas no documento klakdb.chm.

A vista pública v_akpub_ev_event contém um conjunto de campos que representa os parâmetros de evento no banco de dados. No documento klakdb.chm você também pode encontrar informações sobre vistas públicas que correspondem a outras entidades do Kaspersky Security Center, por exemplo, dispositivos, aplicativos ou usuários. Você pode usar estas informações nas suas consultas.

Esta seção contém instruções para criar uma consulta SQL por meio do utilitário klsql2 e um exemplo de consulta.

Para criar consultas SQL ou vistas do banco de dados, você também pode usar qualquer outro programa para trabalhar com bancos de dados. As informações sobre como exibir os parâmetros para conectar-se ao banco de dados do Kaspersky Security Center, como o nome da instância e o nome do banco de dados, são fornecidas na seção correspondente.

Criar uma consulta SQL usando o utilitário klsql2

a seção descreve como baixar e usar o utilitário klsql2, e como criar uma consulta SQL usando este utilitário

Para usar o utilitário klsql2:

1. Localize o utilitário klsql2 na pasta de instalação do Kaspersky Security Center. Não use versões do utilitário klsql2 destinadas a versões mais antigas do Kaspersky Security Center.
2. Crie o arquivo src.sql em qualquer editor de texto e coloque o arquivo na mesma pasta com o utilitário.
3. No arquivo src.sql, digite a consulta SQL desejada e salve o arquivo.
4. No dispositivo com o Servidor de Administração do Kaspersky Security Center instalado, na linha de comando, digite o seguinte comando para executar a consulta SQL do arquivo src.sql e salvar os resultados no arquivo result.xml:

   ```
   klsql2 -i src.sql -u <nome de usuário> -p <senha> -o result.xml
   ```

   onde `<nome de usuário>` e `<senha>` são as credenciais da conta de usuário que tem acesso ao banco de dados.
5. Caso seja necessário, digite o login e a senha da conta de usuário que tem acesso ao banco de dados.
6. Abra o arquivo result.xml criado recentemente para exibir os resultados da consulta SQL.

É possível editar o arquivo src.sql e criar qualquer consulta SQL para as visualizações públicas. Então, a partir da linha de comando, execute a consulta SQL e salve os resultados em um arquivo.

Exemplo de uma consulta SQL no utilitário klsql2

Esta seção mostra um exemplo de uma consulta SQL, criada por meio do utilitário klsql2.

O exemplo a seguir ilustra a recuperação dos eventos que ocorreram em dispositivos durante os últimos sete dias e exibe os eventos encomendados na hora de sua ocorrência, os eventos mais recentes são exibidos primeiro.

Exemplo:

```
SELECT
e.nId, /* identificador do evento */
e.tmRiseTime, /* hora, em que o evento ocorreu */
e.strEventType, /* nome interno do tipo de evento */
e.wstrEventTypeDisplayName, /* nome exibido do evento */
e.wstrDescription, /* descrição do evento exibida */
e.wstrGroupName, /* nome do grupo, onde o dispositivo está localizado */
h.wstrDisplayName, /* nome exibido do dispositivo, no qual o evento ocorreu */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* endereço IP do dispositivo, no qual
o evento ocorreu */
DE v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Exibir o nome de banco de dados do Kaspersky Security Center

Se você desejar acessar o banco de dados do Kaspersky Security Center por meio das ferramentas de gerenciamento de banco de dados do SQL Server, MySQL ou MariaDB deverá conhecer o nome do banco de dados para conectar-se usando o editor de script SQL.

Para exibir o nome do banco de dados do Kaspersky Security Center:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.
   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Detalhes do banco de dados atual**.

O nome do banco de dados é especificado no campo **Nome do banco de dados**. Use o nome do banco de dados para endereçar o banco de dados nas suas consultas SQL.

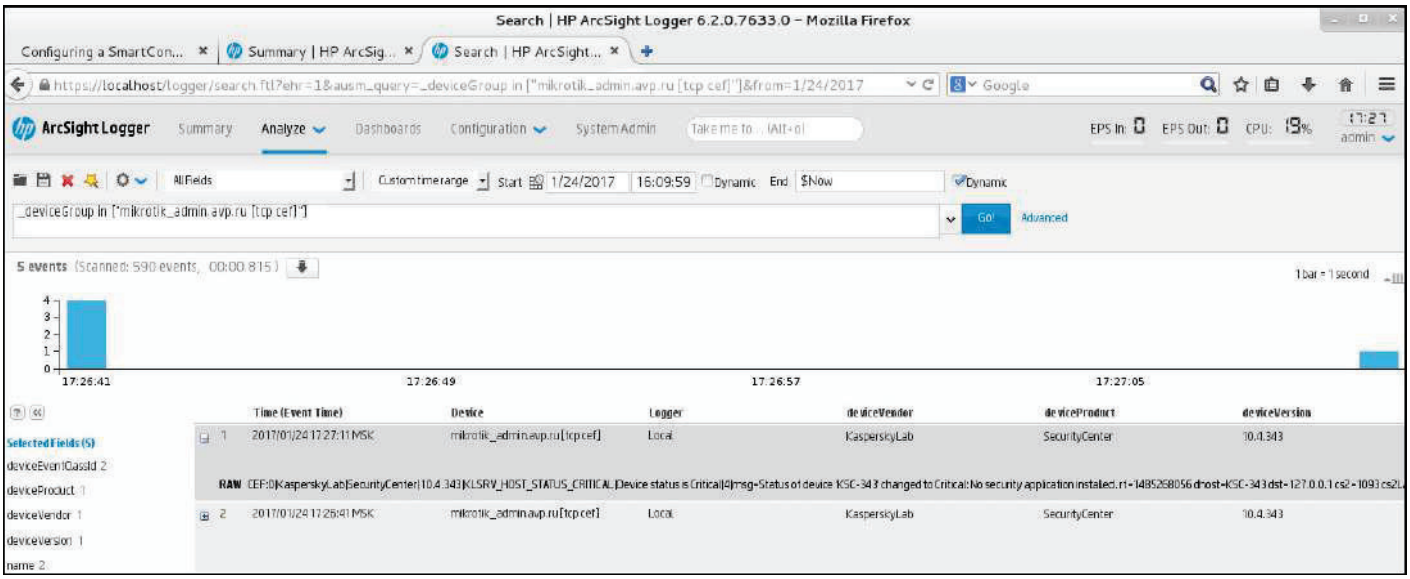
Exibir os resultados da exportação

Você pode controlar para a conclusão bem-sucedida do procedimento de exportação de eventos. Para fazer isto, verifique se as mensagens com eventos exportados são recebidas pelo seu sistema SIEM.

Se os eventos enviados do Kaspersky Security Center forem recebidos e apropriadamente analisados pelo seu sistema SIEM, a configuração nos dois lados foi feita apropriadamente. De outra forma, verifique as configurações que você especificou no Kaspersky Security Center contra a configuração no seu sistema SIEM.

A figura abaixo mostra os eventos exportados ao ArcSight. Por exemplo, o primeiro evento é crítico do Servidor de Administração: "*Status do dispositivo é crítico*".

A representação da exportação de eventos no sistema SIEM varia de acordo com o sistema SIEM que você usa.



Exemplo de eventos

Visualização de um histórico de eventos a partir de um evento

De um evento de criação ou modificação de um objeto que não tem suporte no gerenciamento de revisão, você pode alternar para o histórico de revisões do objeto.

Para visualizar o histórico de revisões de um evento:

1. Nova seleção de eventos.

Sele

3. Clique no botão **Histórico de revisões**.

O histórico de revisões do objeto é aberto.

Excluir os eventos

Para excluir um ou vários eventos:

1. Nova seleção de eventos.
2. Selecione as caixas de seleção junto aos eventos necessários.
3. Clique no botão **Excluir**.

Os eventos selecionados são excluídos e não podem ser restaurados.

Configuração do termo de armazenamento de um evento

O Kaspersky Security Center lhe permite receber informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nestes dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração. Pode ser necessário armazenar alguns eventos por um período maior ou menor do que o especificado pelos valores padrão. Você pode alterar as configurações padrão do período de armazenamento de um evento.

Se não desejar em armazenar alguns eventos no banco de dados do Servidor de Administração, poderá desativar a respectiva configuração na política do Servidor de Administração e na política do aplicativo Kaspersky, ou nas propriedades do Servidor de Administração (apenas para eventos do Servidor de Administração). Isso reduzirá o número de tipos de evento no banco de dados.

Quanto mais longo o prazo de armazenamento de um evento, mais rápido o banco de dados atingirá sua capacidade máxima. No entanto, um prazo de armazenamento mais longo de um evento permite executar tarefas de monitoramento e relatório por um período de tempo maior.

Para definir o prazo de armazenamento de um evento no banco de dados do Servidor de Administração:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Execute uma das seguintes ações:

   Para configurar o termo de armazenamento dos eventos do Agente de Rede ou de um aplicativo Kaspersky gerenciado, clique no nome da política correspondente.

   A janela de página da política será aberta.

   Para configurar os eventos do Servidor de Administração, no menu principal, clique no ícone de Configurações () ao lado do nome do Servidor de Administração necessário.

   Se você possui uma política para o Servidor de Administração, pode clicar no nome dessa política.

   A página de propriedades do Servidor de Administração (ou a página de propriedades da política do Servidor de Administração) é aberta.

3. Selecione a guia **Configuração de eventos**.

   Uma lista de tipos de evento relacionados à seção **Crítico** é exibida.

4. Selecione a seção **Falha funcional**, **Advertência** ou **Informações**.

5. Na lista de tipos de eventos no painel direito, clique no link do evento cujo prazo de armazenamento deseja alterar.

   Na seção **Registro de eventos** da janela, a opção **Armazenar no banco de dados do Servidor de Administração por (dias)** é ativada.

6. Na caixa de edição abaixo desse botão de alternar, insira o número de dias para armazenar o evento.

7. Caso não deseje armazenar um evento no banco de dados do Servidor de Administração, desative a opção **Armazenar no banco de dados do Servidor de Administração por (dias)**.

   Se você configurar eventos do Servidor de Administração na janela de propriedades do Servidor de Administração e se as configurações do evento estiverem bloqueadas na política do Servidor de Administração do Kaspersky Security Center, não será possível redefinir o valor do período de armazenamento para um evento.

8. Clique em **OK**.

   A janela de propriedades da política é fechada.

A partir de agora, quando o Servidor de Administração receber e armazenar os eventos do tipo selecionado, eles terão o prazo de armazenamento alterado. O Servidor de Administração não altera o prazo de armazenamento de eventos recebidos anteriormente.

Eventos dos componentes do Kaspersky Security Center

Cada componente do Kaspersky Security Center tem o seu próprio conjunto de tipos de evento. Esta seção lista tipos de eventos que ocorrem no Servidor de Administração do Kaspersky Security Center, no Agente de Rede, no Servidor de MDM do iOS e em um Servidor de dispositivos móveis do Microsoft Exchange. Os tipos de eventos que ocorrem nos aplicativos Kaspersky não são listados nesta seção.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Estrutura de dados da descrição do tipo de evento

Para cada tipo de evento, seu nome de exibição, o identificador (ID), o código alfabético, a descrição e o termo de armazenamento padrão são fornecidos.

Nome de exibição do tipo de evento. Este texto é exibido no Kaspersky Security Center quando você configura eventos e quando eles ocorrem.

ID do tipo de evento. Este código numérico é usado quando você processa eventos usando ferramentas de terceiros para a análise de eventos.

- **Tipo de evento** (código alfabético). Este código é usado quando você percorre e processa eventos usando vistas públicas fornecidas no banco de dados do Kaspersky Security Center e quando os eventos são exportados para um sistema SIEM.

  Descrição. Este texto contém as situações nas quais um evento ocorre e o que você pode fazer nesses casos.

- **Prazo de armazenamento padrão**. É o número de dias durante os quais o evento é armazenado no banco de dados do Servidor de Administração e é exibido na lista de eventos no Servidor de Administração. Após o término desse período, o evento é excluído. Se o valor do prazo de armazenamento do evento for 0, os eventos são detectados, mas não são exibidos na lista de eventos no Servidor de Administração. Se você configurou para salvar os eventos no log de eventos do sistema operacional, poderá encontrá-los nesse local.
  Você pode alterar o prazo de armazenamento de eventos:

  - Console de Administração: configuração do termo de armazenamento de um evento

    Kaspersky Security Center Web Console: Configurar o termo de armazenamento de um evento

Outros dados podem incluir os seguintes campos:

event_id: número exclusivo do evento no banco de dados, gerado e atribuído automaticamente. Não deve ser confundido com **ID do tipo de evento**.

- **task_id**: a ID da tarefa que causou o evento (se houver)

severity: um dos níveis de gravidade a seguir (na ordem crescente de gravidade):
0) nível de gravidade inválido

1) Informativo

2) Aviso
3) Erro

4) Crítico

Eventos do Servidor de Administração

Esta seção contém informações sobre os eventos relativos ao Servidor de Administração.

Eventos críticos do Servidor de Administração

A tabela abaixo mostra os tipos de eventos do Servidor de Administração do Kaspersky Security Center que têm o nível de importância **Crítico**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Caso a porta seja especificada na janela de propriedades do Servidor de Administração no Console de Administração, o Kaspersky Security Center publicará as métricas e os eventos críticos a serem obtidos pelo Prometheus, um sistema para monitoramento e alerta. O Prometheus obtém as métricas e os eventos críticos e, em seguida, gera os alertas para cada evento.

Eventos críticos do Servidor de Administração

Nome de exibição do	ID de tipo de	Tipo de evento	Descrição	Prazo armazenar

tipo de evento	evento			padrã
O limite da licença foi excedido	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Uma vez por dia o Kaspersky Security Center verifica se a restrição de licenciamento foi excedida. Eventos deste tipo ocorrem quando Servidor de Administração detectar que alguns limites de licenciamento estão excedidos pelos aplicativos da Kaspersky instalados nos dispositivos cliente e se o número de unidades de licenciamento atualmente usadas e cobertas por uma única licença exceder 110% do número total de unidades cobertas pela licença. Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração).	180 dias

			O Kaspersky Security Center determina as regras para gerar eventos quando uma restrição de licenciamento for excedida.	
Surto de vírus	26 (para Proteção Contra Ameaças ao Arquivo)	GNRL_EV_VIRUS_OUTBREAK	Eventos deste tipo ocorrem quando o número de objetos maliciosos detectados em diversos dispositivos gerenciados exceder o limite dentro de um curto período de tempo. Você pode responder ao evento nas seguintes maneiras: ▪ Você pode configurar o limite nas propriedades do Servidor de Administração. Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias
Surto de vírus	27 (para Proteção Contra Ameaças ao Correio)	GNRL_EV_VIRUS_OUTBREAK	Eventos deste tipo ocorrem quando o número de objetos maliciosos detectados em diversos dispositivos gerenciados exceder o limite dentro de um curto período de tempo. Você pode responder ao evento nas seguintes maneiras: Você pode configurar o	180 dias

			propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	
Surto de vírus	28 (para Firewall)	GNRL_EV_VIRUS_OUTBREAK	Eventos deste tipo ocorrem quando o número de objetos maliciosos detectados em diversos dispositivos gerenciados exceder o limite dentro de um curto período de tempo. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias
O dispositivo está sem gerenciamento	4111	KLSRV_HOST_OUT_CONTROL	Eventos deste tipo ocorrem se um dispositivo gerenciado está visível na rede, mas não se conectou ao Servidor de Administração por um período de	180 dias