IBM Security QRadar

Guia de Configuração de Adaptador

Setembro de 2016

Nota

Antes de usar estas informações e o produto que ela suporta, leia as informações em “Avisos” na página 57.

Índice

Introdução ao configurar adaptadores para QRadar Risk Manager

IBM® Security QRadar Risk Manager é um dispositivo que é utilizado para monitorar configurações de dispositivo, simular alterações em seu ambiente de rede e priorizar riscos e vulnerabilidades. O QRadar Risk Manager usa adaptadores para integrar com dispositivos em sua rede.

Público desejado

Os administradores de rede que são responsáveis pela instalação e por configurar os adaptadores devem estar familiarizados com os conceitos de segurança de rede e configurações do dispositivo.

Documentação técnica

Para encontrar a documentação do produto IBM Security QRadar na web, inclusive toda a documentação traduzida, acesse o IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Para obter informações sobre como acessar mais documentação técnica na biblioteca de produtos QRadar, consulte Acessando a documentação do IBM Security QRadar (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Entrando em contato com o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte Nota técnica de suporte e download (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Declaração de boas práticas de segurança

A segurança do sistema de TI envolve a proteção de sistemas e as informações através da prevenção, detecção e resposta para acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mau uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança individual pode ser completamente eficaz na prevenção do acesso ou uso impróprio. AIBM sistemas, produtos e serviços são projetados para fazerem parte de uma abordagem de segurança abrangente legal, que envolverá necessariamente procedimentos operacionais adicionais, podendo requerer outros sistemas, produtos ou serviços para que sejam mais eficientes. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU TORNAM A SUA EMPRESA IMUNE CONTRA CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PESSOA.

Observe que:

O uso desse programa pode implicar em várias leis ou regulamentações, incluindo aquelas relacionadas à privacidade, proteção de dados, emprego, e armazenamento e comunicações eletrônicas. O IBM Security QRadar pode ser usado apenas para

propósitos legais e de maneira legal. O cliente concorda em usar este Programa de acordo com leis, regulamentos e políticas e assume toda a responsabilidade pelo seu cumprimento. O licenciado declara que obterá ou obteve quaisquer consentimentos, permissões ou licenças necessárias para permitir o uso legal do IBM Security QRadar.

Capítulo 1. Visão geral dos Adaptadores

Utilize adaptadores para integrar IBM Security QRadar Risk Manager com seus dispositivos de rede. Ao configurar os adaptadores, o QRadar Risk Manager pode interrogar e importar os parâmetros de configuração de dispositivos de rede, como firewalls, roteadores e comutadores.

Topologia e configuração de rede

QRadar Risk Manager utiliza adaptadores para coletar configurações de rede. Os adaptadores transformam as informações de configuração em um formato unificado para os modelos, fabricantes e tipos de dispositivos suportados. O QRadar Risk Manager usa os dados para entender a topologia e a configuração de rede de seus dispositivos de rede.

Para conectar os dispositivos externos na rede, o QRadar Risk Manager deve ser capaz de acessar os dispositivos. O QRadar Risk Manager usa as credenciais do usuário que são configuradas no QRadar para acessar o dispositivo e fazer download das configurações.

Processo para integrar dispositivos de rede

Para integrar dispositivos de rede com QRadar Risk Manager, siga estas etapas:

1. Configure o dispositivo de rede para ativar a comunicação com o QRadar Risk Manager.
2. Instale o adaptador apropriado para a seu dispositivo de rede em seu dispositivo do QRadar Risk Manager
3. Use o Gerenciamento de origem de configuração para incluir os dispositivos de rede no QRadar Risk Manager.
4. Defina o protocolo de rede que é necessário para a comunicação com seus dispositivos de rede.

   Para obter informações adicionais, consulte *IBM Security QRadar Risk Manager User Guide*.

Tipos de adaptadores

IBM Security QRadar Risk Manager suporta vários tipos de adaptadores.

Os seguintes adaptadores são suportados:

- F5 BIG-IP
- Verificar ponto de SecurePlatform Appliances
- Servidor de gerenciamento de segurança de ponto de verificação
- Cisco Catalyst (CatOS)
- Cisco Internet Operating System (IOS)
- Cisco Nexus
- Cisco Security Appliances
- Fortinet FortiOS
- ProVision HP Networking
- Juniper Networks ScreenOS

- Juniper Networks JUNOS
- Juniper Networks NSM
- Palo Alto
- Sourcefire 3D Sensor
- SNMP genérico
- TippingPoint IPS
- McAfee Sidewinder

Capítulo 2. Instalando adaptadores

Você deve fazer o download dos arquivos do adaptador para seu IBM Security QRadar SIEM Console, e, em seguida, copiá-los para o IBM Security QRadar Risk Manager.

Antes de Iniciar

Depois de estabelecer a conexão inicial, o QRadar SIEM Console é o único dispositivo que pode se comunicar diretamente com o QRadar Risk Manager.

Procedimento

1. Ao usar o SSH, efetue login no seu QRadar SIEM Console como o usuário raiz.
2. Faça o download do arquivo compactado dos adaptadores QRadar Risk Manager do Fix Central (www.ibm.com/support/fixcentral/) para o seu QRadar SIEM Console.
3. Para copiar o arquivo compactado a partir do QRadar SIEM Console para QRadar Risk Manager, digite o comando a seguir:

   `scp adapters.zip root@IP_address:`

   A opção *IP_address* é o endereço IP ou nome do host do QRadar Risk Manager.

   Por exemplo:

   `scp adapters.bundle-2014-10-972165.zip root@100.100.100.100:`
4. No seu dispositivo QRadar Risk Manager, digite a senha para o usuário raiz.
5. Ao usar o SSH a partir do seu QRadar SIEM Console, efetue login no dispositivo QRadar Risk Manager como o usuário raiz.
6. Para desempacotar e instalar os adaptadores, digite os seguintes comandos no diretório-raiz que contém o arquivo compactado:

   `unzip adapters.zip`

   `yum install -y adapters*.rpm`

   Por exemplo:

   `unzip adapters.bundle-2014-10-972165.zip`

   `yum install -y adapters*.rpm`

   Nota:

   Para o QRadar Risk Manager versões anteriores à V.7.2.8, use o comando **rpm**

   Por exemplo:

   `rpm -Uvh adapters*.rpm`
7. Para reiniciar os serviços para o servidor ziptie e concluir a instalação, digite o seguinte comando:

   `service ziptie-server restart`

   Importante: Ao reiniciar os serviços para o servidor do ziptie qualquer dispositivo em andamento a partir de backups de Gerenciamento de Configuração de Origem é interrompido.

Desinstalando um adaptador

Use o comando **yum** para remover um adaptador do IBM Security QRadar Risk Manager.

Procedimento

1. Ao usar o SSH, efetue login no IBM Security QRadar SIEM Console como usuário raiz.
2. Para desinstalar um adaptador, digite o seguinte comando:

   `yum remove -y adapter package`

   Por exemplo, `yum remove -y adapters.cisco.ios-2011_05-205181.noarch`

   Nota:

   Para o QRadar Risk Manager versões anteriores à V.7.2.8, use o comando **rpm**

   Por exemplo:

   `rpm -e adapter file`

   `rpm -e adapters.cisco.ios-2011_05-205181.noarch.rpm`

Capítulo 3. Métodos para incluir dispositivos de rede

Use o Gerenciamento de origem de configuração para incluir os dispositivos de rede no IBM Security QRadar Risk Manager.

A tabela a seguir descreve os métodos que você pode usar para incluir um dispositivo de rede.

Tabela 1. Métodos para incluir um dispositivo de rede no QRadar Risk Manager.

Método	Descrição
Incluir Dispositivo	Incluir um dispositivo.
Descobrir Dispositivos	Incluir vários dispositivos.
Descobrir a partir do NSM	Incluir dispositivos que são gerenciados por um console Juniper Networks NSM.
Descobrir Check Point SMS	Incluir dispositivos que são gerenciados por um Check Point Security Manager Server (CPSMS).
Descobrir a partir de SiteProtector	Incluir dispositivos a partir de SiteProtector.
Descobrir a partir do Defense Center	Inclua dispositivos a partir do Sourcefire Defense Center.

Incluindo um dispositivo de rede

Para incluir um dispositivo de rede para IBM Security QRadar Risk Manager, utilize Gerenciamento de origem de configuração.

Antes de Iniciar

Revise as versões de software suportadas, credenciais e comandos necessários para os dispositivos de rede. Para obter mais informações, consulte Capítulo 5, “Adaptadores suportados”, na página 17.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação **Admin**, clique em **Plug-ins**.
3. Na área de janela Risk Manager, clique em Gerenciamento de origem de configuração.
4. No menu de navegação, clique em **Credenciais**.
5. Na área de janela Grupos de Rede, clique em **Incluir um novo grupo de rede**.
   a. Digite um nome para o grupo de rede e clique em **OK**.
   b. Digite o endereço IP do seu dispositivo, e clique em **Incluir**.

      Você pode digitar um endereço IP, um intervalo de endereços IP, uma sub-rede CIDR ou um curinga.

      Por exemplo, use o formato a seguir para um curinga, digite `10.1.*.*`

      Por exemplo, use o formato a seguir para um CIDR, digite `10.2.1.0/24`.

      Restrição: Não replique os endereços de dispositivo que existem em outros grupos de rede em gerenciamento de Origem de Configuração.

c. Assegure-se de que os endereços incluídos serão exibidos na caixa **Endereço de rede** ao lado da caixa **Incluir endereço**.
d. Repita as duas etapas anteriores para cada endereço IP que deseja incluir.

6. Na área de janela Credenciais, clique em **Incluir um novo conjunto de credencial**.
   a. Digite um nome para o conjunto de credenciais, e clique em **OK**.
   b. Selecione o nome da configuração de credencial que você criar e insira os valores para os parâmetros.

      A seguinte tabela descreve os parâmetros.

Tabela 2. Opções de parâmetro para as credenciais

Parâmetro	Descrição

Nome de usuário	Um nome de usuário válido para efetuar login no adaptador.
	
	Para adaptadores, o nome de usuário e senha que você fornecer requer acesso a vários arquivos, como os seguintes arquivos:
	
	`rule.C`
	
	`objects.C`
	
	`implied_rules.C`
	
	`Standard.PF`

Senha	A senha para o dispositivo.
Ativar Senha	A senha para autenticação de segundo nível. Essa senha é necessária quando as credenciais solicitam as credenciais do usuário que são necessárias para o nível de acesso de modo especializado.
SNMP Get Community	Opcional
Nome de Usuário de Autenticação SNMPv3	Opcional
Senha de Autenticação SNMPv3	Opcional
Senha de Privacidade SNMPv3	Opcional O protocolo que é utilizado para decriptografar os traps SNMPv3.

Restrição: Se o dispositivo de rede atender uma das seguintes condições, você deve configurar os protocolos no Gerenciamento de origem de configuração:

- Seu dispositivo utiliza uma porta não padrão para o protocolo de comunicação.
- Você deseja configurar o protocolo que o IBM Security QRadar Risk Manager utiliza para se comunicar com endereços IP específicos.

Para obter informações adicionais sobre como configurar origens, veja o *IBM Security QRadar Risk Manager User Guide*.

7. No menu de navegação, inclua um único dispositivo ou vários dispositivos.
   - Para incluir um dispositivo de rede, clique em **Incluir Dispositivo**.

- Para incluir vários endereços IP para dispositivos de rede, clique em **Descobrir dispositivos**.

8. Digite o endereço IP para o dispositivo, selecione o tipo de adaptador e, em seguida, clique em **Incluir**.

   Se não tiver sido feito backup do dispositivo, um ponto de interrogação azul aparecerá ao lado do adaptador.
9. Para fazer backup do dispositivo incluído na lista de dispositivos, selecione o dispositivo e, em seguida, clique em **Backup**.
10. Repita essas etapas para cada dispositivo de rede que você incluir na lista de dispositivos.

O que Fazer Depois

Depois de incluir todos os dispositivos necessários, será possível configurar protocolos. Para obter informações adicionais, consulte *IBM Security QRadar Risk Manager User Guide*.

Incluindo dispositivos que são gerenciados por um console NSM

Use o Gerenciamento de origem de configuração para incluir todos os dispositivos de um console Juniper Networks NSM (Network and Security Manager) no IBM Security QRadar Risk Manager.

Antes de Iniciar

Revise as versões de software suportadas, credenciais e comandos necessários para os dispositivos de rede. Para obter mais informações, consulte Capítulo 5, “Adaptadores suportados”, na página 17.

Procedimento

1. No IBM Security QRadar SIEM, clique na guia **Administrador**.
2. No menu de navegação **Admin**, clique em **Plug-ins**.
3. Na área de janela Risk Manager, clique em **Gerenciamento de origem de configuração**.
4. No menu de navegação, clique em **Credenciais**.
5. Na área de janela Grupos de Rede, clique em **Incluir um novo grupo de rede**.
   a. Digite um nome para o grupo de rede e clique em **OK**.
   b. Digite o endereço IP do seu dispositivo, e clique em **Incluir**.

      Você pode digitar um endereço IP, um intervalo de endereços IP, uma sub-rede CIDR ou um curinga.

      Restrição: Não replique os endereços de dispositivo que existem em outros grupos de rede em gerenciamento de Origem de Configuração.
   c. Assegure-se de que os endereços incluídos serão exibidos na caixa **Endereço de rede** ao lado da caixa **Incluir endereço**.
   d. Repita as duas etapas anteriores para cada endereço IP que deseja incluir.
6. Na área de janela Credenciais, clique em **Incluir um novo conjunto de credencial**.
   a. Digite um nome para o conjunto de credenciais, e clique em **OK**.
   b. Selecione o nome do conjunto de credenciais que você criou e digite os valores para os parâmetros.

A seguinte tabela descreve os parâmetros.

Tabela 3. Opções de parâmetros para credenciais de serviços da web do Juniper NSM

Parâmetro	Descrição
Nome de usuário	Um nome de usuário válido para efetuar login nos serviços da web do Juniper NSM (Network and Security Manager). Para os serviços da web do Juniper NSM, este usuário deve poder acessar o servidor Juniper NSM.
Senha	A senha para o dispositivo.
Ativar Senha	Não obrigatório.

Restrição: O Juniper Networks NSM (Network and Security Manager) não suporta SNMP.

7. No menu de navegação, clique em **Descobrir a partir do NSM**.
8. Insira valores para o endereço IP e as credenciais do usuário, clique em **OK** e, em seguida, clique em **GO**.
9. Selecione o dispositivo que você incluiu na lista de dispositivos, e clique em **Backup** e, em seguida, clique em **Sim**.

O que Fazer Depois

Depois de incluir todos os dispositivos necessários, será possível configurar protocolos. Para obter informações adicionais, consulte *IBM Security QRadar Risk Manager User Guide*.

Incluindo dispositivos que são gerenciados por um console CPSMS no QRadar Risk Manager

Use o Gerenciamento de origem de configuração para incluir dispositivos a partir de um Check Point Security Manager Server (CPSMS) no IBM Security QRadar Risk Manager.

Dependendo de sua versão do Check Point Security Manager Server, deve-se escolher um dos métodos de descoberta a seguir para incluir seus dispositivos no QRadar Risk Manager.

Incluindo dispositivos que são gerenciados pelo CPSMS usando OPSEC

Inclua dispositivos que são gerenciados pelo Check Point Security Manager Server versões NGX R60 a R77 no IBM Security QRadar Risk Manager usando OPSEC para descobrir e incluir todos os dispositivos.

Antes de Iniciar

Revise as versões de software suportadas, credenciais e comandos necessários para os dispositivos de rede. Para obter mais informações, consulte Capítulo 5, “Adaptadores suportados”, na página 17.

Deve-se obter o nome SIC da Entidade OPSEC, o nome SIC do Objeto de Aplicativo OPSEC e a senha descartável para a senha do *certificado pull* antes de iniciar este procedimento. Para obter mais informações, consulte sua documentação CPSMS.

Nota: O recurso Importação de Dispositivo não é compatível com os adaptadores CPSMS.

Sobre Esta Tarefa

Repita o procedimento a seguir para cada CPSMS ao qual você desejar se conectar e para iniciar a descoberta de seus firewalls gerenciados.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação **Admin**, clique em **Plug-ins**.
3. Na área de janela Risk Manager, clique em **Gerenciamento de origem de configuração**.
4. No menu de navegação, clique em **Credenciais**.
5. Na área de janela Grupos de Rede, clique em **Incluir um novo grupo de rede**.
   a. Digite um nome para o grupo de rede e, em seguida, clique em **OK**.
   b. Digite o endereço IP de seu dispositivo CPSMS e, em seguida, clique em **Incluir**.

      Restrição: Não replique os endereços de dispositivo que existem em outros grupos de rede em gerenciamento de Origem de Configuração.
   c. Assegure-se de que os endereços incluídos serão exibidos na caixa **Endereço de rede** ao lado da caixa **Incluir endereço**.
6. Na área de janela Credenciais, clique em **Incluir um novo conjunto de credencial**.
   a. Digite um nome para a configuração de credencial e, em seguida, clique em **OK**.
   b. Selecione o nome da configuração de credencial que você criou e, em seguida, digite um nome de usuário e uma senha válidos para o dispositivo.
7. Digite o nome SIC da Entidade OPSEC do CPSMS que gerencia os dispositivos de firewall a serem descobertos. Esse valor deve ser exato porque o formato depende do tipo de dispositivo a partir do qual a descoberta é proveniente. Use a tabela a seguir como uma referência para formatos de nome SIC da Entidade OPSEC.

Tipo	Nome
Servidor de gerenciamento	`CN=cp_mgmt,O=<tome o valor O do campo DN>`
Gateway para o servidor de gerenciamento	`CN=cp_mgmt_<nome do host do gateway>,O=<tome o valor O do campo DN>`

   Por exemplo, quando estiver descobrindo a partir do Servidor de gerenciamento:
   - DN do aplicativo OPSEC: `CN=cpsms226,O=vm226-CPSMS..bs7ocx`
   - Host de aplicativos OPSEC: `vm226-CPSMS`

   O Nome do SIC da Entidade é `CN=cp_mgmt,O=vm226-CPSMS..bs7ocx`

Por exemplo, quando estiver descobrindo a partir do Gateway para o servidor de gerenciamento:

- DN do aplicativo OPSEC: `CN=cpsms230,O=vm226-CPSMS..bs7ocx`
- Host de aplicativos OPSEC: `vm230-CPSMS2-GW3`

O Nome do SIC da Entidade é `CN=cp_mgmt_vm230-CPSMS2-GW3,O=vm226-CPSMS..bs7ocx`

8. Use o aplicativo Check Point SmartDashboard para inserir o nome do SIC do Objeto de Aplicativo OPSEC criado no CPSMS.

   Por exemplo: `CN=cpsms230,O=vm226-CPSMS.bs7ocx`
9. Obter o certificado SSL OPSEC
   a. Clique em **Obter Certificado**.
   b. No campo **Autoridade de Certificação IP**, digite o endereço IP.
   c. No campo **Senha de Certificado Pull**, digite a senha descartável para o Aplicativo OPSEC.
   d. Clique em **OK**.
10. Clique em **OK**.
11. Clique em **Protocolos** e verifique se o protocolo **CPSMS** está selecionado.

    A porta padrão para o protocolo CPSMS é 18190.
12. Clique em **Descobrir no Check Point OPSEC** e, em seguida, insira o endereço IP do CPSMS.
13. Clique em **OK**.
14. Repita essas etapas para cada dispositivo CPSMS que você deseja incluir.

O que Fazer Depois

Ao incluir todos os dispositivos necessários, faça backup dos dispositivos e visualize-os na topologia.

Incluindo dispositivos que são gerenciados pelo CPSMS usando HTTPS

Inclua dispositivos que são gerenciados pelo Check Point Security Manager Server versão R80 no IBM Security QRadar Risk Manager usando o protocolo HTTPS para descobrir e incluir os dispositivos.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação **Admin**, clique em **Plug-ins**.
3. Na área de janela Risk Manager, clique em **Gerenciamento de origem de configuração**.
4. No menu de navegação, clique em **Credenciais**.
5. Na área de janela Grupos de Rede, clique em **Incluir um novo grupo de rede**.
   a. Digite um nome para o grupo de rede e, em seguida, clique em **OK**.
   b. Digite o endereço IP do seu dispositivo Check Point e, em seguida, clique em **Incluir**.
   c. Assegure-se de que o endereço seja exibido na caixa **Endereço de rede**.
6. Na área de janela Credenciais, clique em **Incluir um novo conjunto de credencial**.
   a. Digite um nome para a configuração de credencial e, em seguida, clique em **OK**.

b. Selecione o nome da configuração de credencial que você criou e, em seguida, digite um nome de usuário e uma senha válidos para o dispositivo.

7. Clique em **OK**.
8. Clique em **Protocolos** e verifique se o protocolo **HTTPS** está selecionado.
9. Clique em **Descobrir no Check Point HTTPS** e, em seguida, insira o endereço IP do Check Point.
10. Clique em **OK**.

O que Fazer Depois

Após incluir todos os dispositivos necessários, faça backup dos dispositivos e visualize-os na topologia.

Incluindo dispositivos que são gerenciados pelo SiteProtector

Utilize o Gerenciamento de origem de configuração para incluir dispositivos a partir de SiteProtector para IBM Security QRadar Risk Manager.

Antes de Iniciar

Os adaptadores IBM Internet Security Systems GX e IBM Security SiteProtector System devem ser instalados antes de ser possível incluir dispositivos.

O protocolo do Microsoft SQL deve estar ativado para usar a porta 1433 do Microsoft SQL Server.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação **Admin**, clique em **Plug-ins**.
3. Na área de janela Risk Manager, clique em Gerenciamento de origem de configuração.
4. No menu de navegação, clique em **Credenciais**.
5. Na área de janela Grupos de Rede, clique em **Incluir um novo grupo de rede**.
   a. Digite um nome para o grupo de rede e, em seguida, clique em **OK**.
   b. Digite o endereço IP de seu dispositivo SiteProtector e, em seguida, clique em **Incluir**.
   c. Assegure-se de que os endereços incluídos serão exibidos na caixa **Endereço de rede** ao lado da caixa **Incluir endereço**.
6. Na área de janela Credenciais, clique em **Incluir um novo conjunto de credencial**.
   a. Digite um nome para a configuração de credencial e, em seguida, clique em **OK**.
   b. Selecione o nome da configuração de credencial que você criou e, em seguida, digite um nome de usuário e uma senha válidos para o dispositivo.

      Restrição: O nome do usuário e a senha são as mesmas credenciais que aquelas usadas para acessar o banco de dados do SiteProtector Microsoft SQL Server.
7. Clique em **OK**.

8. Clique em **Descobrir SiteProtector De** e, em seguida, insira o endereço IP SiteProtector.
9. Clique em **OK**.

O que Fazer Depois

Quando incluir todos os dispositivos necessários, faça backup dos dispositivos e visualize-os na topologia.

Capítulo 4. Resolução de problemas de descoberta e backup de dispositivo

Corrija problemas com a descoberta e o backup de dispositivo. É possível consultar os detalhes para logs e mensagens de erro e aviso para ajudar a solucionar problemas.

Falha de Backup de Dispositivo

Verifique as credenciais de login do dispositivo.

1. Na guia **Administrador**, clique em **Configuration Source Management**.
2. Verifique se as credenciais para acessar o dispositivo de destino estão corretas.
3. Teste as credenciais no dispositivo de destino.

Visualizar erros de backup de dispositivo

Para ver erros de backup, execute as etapas a seguir:

1. Na guia **Administrador**, clique em **Configuration Source Management**.
2. Clique em um dispositivo e, em seguida, clique em **Visualizar erro**.

Esta tabela lista o identificador de mensagem de erro, a descrição da mensagem e a ação de resolução de problemas sugerida.

Tabela 4. Erros de backup de dispositivo

Erros de backup	Descrição do Erro	Etapa de resolução de problemas sugerida
UNEXPECTED_RESPONSE	A tentativa de conexão atingiu o tempo limite	Verifique se você está usando o adaptador correto.
INVALID_CREDENTIALS	As credenciais estão incorretas	Verifique as credenciais em **Configuration Source Management**.
SSH_ERROR	Connection error	Verifique se o dispositivo está funcionando e está conectado à sua rede. Use outros protocolos de conexão de rede e as ferramentas de resolução de problemas para verificar se o dispositivo é acessível. Verifique se o protocolo de conexão SSH é permitido e se está configurado corretamente.
TELNET_ERROR	Connection error	Verifique se o dispositivo está funcionando e está conectado à sua rede. Use outros protocolos de conexão de rede e as ferramentas de resolução de problemas para verificar se o dispositivo é acessível. Verifique se o protocolo de conexão Telnet é permitido e se está configurado corretamente.

Tabela 4. Erros de backup de dispositivo (continuação)

Erros de backup	Descrição do Erro	Etapa de resolução de problemas sugerida
SNMP_ERROR	Connection error	Verifique se o dispositivo está funcionando e está conectado à sua rede. Use outros protocolos de conexão de rede e as ferramentas de resolução de problemas para verificar se o dispositivo é acessível. Verifique se o SNMP é permitido e se está configurado corretamente.
TOO_MANY_USERS	O número de usuários que estão configurados para acessar esse dispositivo foi excedido.	Verifique o número máximo de usuários que têm permissão para acessar o dispositivo, efetuando logon no dispositivo e verificando a configuração para o número máximo de usuários que podem acessar o dispositivo ao mesmo tempo.
DEVICE_MEMORY_ERROR	Erros de configuração do dispositivo	Verifique se o dispositivo está funcionando corretamente. Acesse o dispositivo e verifique a configuração e verifique os logs em busca de erros. Use a documentação do dispositivo para ajudar a solucionar os erros.
NVRAM_CORRUPTION_ERROR	Problemas de acesso ao dispositivo	Em **Configuration Source Management**, verifique o nível de acesso do nome do usuário que está configurado para acessar o dispositivo.
INSUFFICIENT_PRIVILEGE	O usuário que está configurado para acessar o dispositivo tem privilégio insuficiente	Em **Configuration Source Management**, verifique o nível de acesso do nome do usuário que está configurado para acessar o dispositivo.
DEVICE_ISSUE	Erro no dispositivo	Selecione o dispositivo em **Configuration Source Management** e clique em **Visualizar erro** para ver mais detalhes.

O backup é concluído com aviso de análise

Para visualizar mais detalhes sobre o aviso, execute as etapas a seguir:

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de configuração**.
3. Clique em **Ver log** para o dispositivo selecionado na tabela **Lista de dispositivos**.

Você tem as versões mais recentes do adaptador?

Para verificar suas versões do adaptador, efetue login como raiz no dispositivo QRadar Risk Manager e, em seguida, digite o comando a seguir:

```
yum list adapter\*
```

É possível procurar informações de data nos nomes dos adaptadores para ajudar a determinar as datas de liberação.

Para fazer download do pacote configurável do adaptador mais recente, execute as etapas a seguir:

1. Acesse o IBM Fix Central (https://www.ibm.com/support/fixcentral/).
2. No campo **Seletor de produto**, digite `Risk Manager` para filtrar sua seleção.
3. Clique em IBM Security QRadar Risk Manager.
4. Na lista **Versão instalada**, selecione a versão que está instalada em seu sistema.
5. Na lista **Plataforma**, selecione o sistema operacional que está instalado em seu sistema e, em seguida, clique em **Continuar**.
6. Clique em **Procurar correções** e, em seguida, clique em **Continuar**.
7. Para fazer download do pacote configurável do adaptador mais recente, clique no link do pacote configurável do adaptador na parte superior da lista **Adaptador**.

Você tem o backup de dispositivo mais recente?

Para verificar se você tem um backup recente, execute estas etapas:

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de configuração**.
3. Clique duas vezes no dispositivo na tabela **Lista de dispositivos**.
4. Na barra de ferramentas, clique em **Histórico**. A configuração mais recente que foi importada é exibida.

Se você não achar que tem a configuração mais recente, verifique executando o backup novamente.

Erro ao importar configurações de seus dispositivos

Um arquivo CSV formatado incorretamente pode fazer com que um backup de dispositivo falhe. Execute estas etapas para verificar o arquivo CSV:

1. Revise o arquivo CSV para corrigir quaisquer erros.
2. Reimporte as configurações do dispositivo usando o arquivo CSV atualizado.

Falha ao descobrir dispositivos no Check Point SMS (OPSEC)

Siga todas as etapas na seção "Incluindo dispositivos que são gerenciados por um console do CPSMS" do *IBM Security QRadar Risk Manager Adapter Configuration Guide*, especialmente as etapas 7 e 8 em que os campos do OPSEC devem ser exatos.

Tarefas relacionadas:

"Incluindo dispositivos que são gerenciados pelo CPSMS usando OPSEC" na página 8
Inclua dispositivos que são gerenciados pelo Check Point Security Manager Server versões NGX R60 a R77 no IBM Security QRadar Risk Manager usando OPSEC para descobrir e incluir todos os dispositivos.

Capítulo 5. Adaptadores suportados

IBM Security QRadar Risk Manager integra-se com muitos fabricantes e vendedores de produtos de segurança.

As informações a seguir são fornecidas para cada adaptador suportado:

Versões suportadas

Especifica o nome do produto e a versão suportada.

Suporta dados vizinhos

Especifica se dados vizinhos são suportados para este adaptador. Se o seu dispositivo suporta os dados, então os dados vizinhos serão obtidos a partir de um dispositivo utilizando Simple Network Management Protocol (SNMP)e uma interface da linha de comandos (CLI).

Descoberta SNMP

Especifica se o dispositivo permite a descoberta utilizando SNMP.

Os dispositivos devem suportar o MIB-2 padrão para que a descoberta SNMP ocorra e a configuração do SNMP do dispositivo deve ser suportada e configurada corretamente.

Parâmetros de credenciais obrigatórios

Especifica os requisitos de acesso necessários para o QRadar Risk Manager e o dispositivo para conectar.

Assegure-se de que as credenciais do dispositivo, configuradas em QRadar Risk Manager e no dispositivo, sejam as mesmas.

Se um parâmetro não for necessário, esse campo poderá ser deixado em branco.

Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.

Protocolos de conexão

Especifica os protocolos suportados para o dispositivo de rede.

Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.

Comandos necessários

Especifica a lista de comandos que o adaptador requer para efetuar login e coletar dados.

Para executar os comandos listados no adaptador, as credenciais que são fornecidas em QRadar Risk Manager devem ter os privilégios apropriados.

Arquivos coletados

Especifica a lista de arquivos que o adaptador deve ser capaz de acessar. Para acessar esses arquivos, as credenciais apropriadas devem ser configuradas para o adaptador.

Verificar ponto de SecurePlatform Appliances

IBM Security QRadar Risk Manager suporta o adaptador Verificar ponto de SecurePlatform Appliances.

Os recursos a seguir estão disponíveis com o adaptador Verificar ponto de SecurePlatform Appliances:

- NAT dinâmico
- NAT estático
- Descoberta SNMP
- Roteamento estático
- Protocolos de conexão Telnet e SSH

A tabela a seguir descreve os requisitos de integração para o adaptador do Verificar ponto de SecurePlatform Appliances.

Tabela 5. Requisitos de integração para o adaptador do Verificar ponto de SecurePlatform Appliances

Requisito de integração	Descrição
Versões	R65 a R77.30 **Restrição:** Os dispositivos Nokia IPSO não são suportados para backup.
Descoberta SNMP	Corresponde NGX em SNMP sysDescr.
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha** **Ativar Senha** (modo especializado)
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **Telnet** **SSH**

Tabela 5. Requisitos de integração para o adaptador do Verificar ponto de SecurePlatform Appliances (continuação)

Requisito de integração	Descrição

Comandos que o adaptador requer para efetuar login e coletar dados	`nome do host`
	`dmidecode`
	`ver`
	`uptime`
	`dmesg`
	`route -n`
	`show users`
	`ifconfig -a`
	`echo $FWDIR`

Arquivos coletados	`rules.C`
	`objects.C`
	`implied_rules.C`
	`Standard.pf`
	`snmpd.com`

Adaptador do Check Point Security Management Server

Use o adaptador Check Point para descobrir e fazer backup de nós de extremidade que são gerenciados pelo Security Management Server (CPSMS).

Escolha um dos adaptadores a seguir para descobrir e fazer backup de nós de extremidade que são gerenciados pelo CPSMS.

Adaptador do Check Point Security Management Server OPSEC

Use o adaptador do Check Point Security Management Server OPSEC para descobrir e fazer backup de nós de extremidade que são gerenciados pelo CPSMS versões NGX R60 a R77.

Os recursos a seguir estão disponíveis com o adaptador do Check Point Security Management Server OPSEC:

- Protocolo OPSEC
- NAT dinâmico
- NAT estático
- Roteamento Estático

O adaptador CPSMS é construído sobre o OPSEC SDK 6.0, que suporta produtos Check Point que são configurados para usar certificados assinados usando somente SHA-1.

A tabela a seguir descreve os requisitos de integração para o adaptador CPSMS.

Tabela 6. Requisitos de integração para o adaptador CPSMS

Requisito de integração	Descrição
Versões	NGX R60 a R77
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use as credenciais que são configuradas a partir de 'Incluindo dispositivos gerenciados por um console CPSMS'.
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**CPSMS**
Requisitos de Configuração	Para permitir que `cpsms_client` se comunique com o Check Point Management Server, o `$CPDIR/conf/sic_policy.conf` no CPSMS deve incluir a linha a seguir: `# OPSEC applications defaultANY ; SAM_clients ; ANY ; sam ; sslca, local, sslca_comp# sam proxyANY ; Modules, DN_Mgmt ; ANY; sam ; sslcaANY ; ELA_clients ; ANY ; ela ; sslca, local, sslca_compANY ; LEA_clients ; ANY ; lea ; sslca, local, sslca_compANY ; CPMI_clients; ANY ; cpmi ; sslca, local, sslca_comp`
Portas necessárias	As portas a seguir são usadas pelo QRadar Risk Manager e devem ser abertas no CPSMS: Porta 18190 para o serviço da Interface de Gerenciamento do Ponto de Verificação (ou CPMI) Porta 18210 para o Serviço de Certificado Pull de CA Interno do Ponto de Verificação (ou FW1_ica_pull) Se não for possível utilizar 18190 como uma porta de atendimento para o CPMI, então o número da porta do adaptador do CPSMS deve ser semelhante ao valor listado no arquivo `$FWDIR/conf/fwopsec.conf` para CPMI no CPSMS. Por exemplo, `cpmi_server auth_port 18190`.

Adaptador do Check Point Security Management Server HTTPS

Use o adaptador do Check Point Security Management Server HTTPS para descobrir e fazer backup de nós de extremidade que são conectados a blades de firewall que são gerenciados pelo Security Management Server versão R80.

Os recursos a seguir estão disponíveis com o adaptador do Check Point Security Management Server HTTPS:

- NAT estático
- Roteamento Estático
- Protocolo de conexão HTTPS

Os recursos a seguir não são suportados pelo adaptador do Check Point Security Management Server:

- Objetos dinâmicos (objetos de rede)
- Zonas de segurança (objetos de rede)
- Objetos RPC (serviços)
- Objetos DCE-RPC (serviços)
- Serviços ICMP (serviços)
- Objetos GTP (serviços)
- Objetos TCP compostos (serviços)
- Objetos TCP do Citrix (serviços)
- Outros serviços (serviços)
- Objetos de usuário
- Objetos de horário
- Negação de critérios da política de controle de acesso

Nota:

Se você fizer upgrade para o Check Point Security Management Server R80 de uma versão anterior do Check Point SMS, deverá redescobrir seus dispositivos usando o método de descoberta **Descobrir do Check Point HTTPS**, mesmo se os seus dispositivos forem registrados pelo **Gerenciamento de origem de configuração**.

A tabela a seguir descreve os requisitos de integração para o adaptador do Check Point Security Management Server.

Tabela 7. Requisitos de integração para o adaptador do Check Point Security Management Server

Requisito de integração	**Descrição**
Versões	R80
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**. **Nota:** Deve-se incluir credenciais para o Check Point Security Management Server antes de configurar a descoberta de dispositivo.	**Nome de usuário** **Senha**

Tabela 7. Requisitos de integração para o adaptador do Check Point Security Management Server (continuação)

Requisito de integração	Descrição
Configuração da descoberta de dispositivo Para configurar a descoberta de dispositivo no QRadar, efetue login como administrador e use o **Gerenciamento de origem de configuração** na guia **Administrador**. Para configurar o método de descoberta, clique em **Descobrir no Check Point HTTPS**, insira o endereço IP do Check Point Security Management Server e, em seguida, clique em **OK**.	Descobrir no Check Point HTTPS
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	HTTPS
Requisitos do nível de acesso de usuário	Todos com acesso de leitura/gravação

Terminais da API solicitados	Use o formato a seguir para emitir os comandos listados para os dispositivos:
	
	`https://<managemenet server>:<port>/web_api/<command>`
	
	`show-simple-gateways`
	
	`show-hosts`
	
	`show-networks`
	
	`show-address-ranges`
	
	`show-groups`
	
	`show-groups-with-exclusion`
	
	`show-services-tcp`
	
	`show-services-udp`
	
	`show-service-groups`
	
	`show-packages`
	
	`show-access-rulebase`
	
	`show-nat-rulebase`
	
	`run-script`
	
	`show-task`

Cisco CatOS

IBM Security QRadar Risk Manager suporta o adaptador Cisco Catalyst (CatOS).

O adaptador Cisco CatOS coleta configurações de dispositivo fazendo backup dos dispositivos de rede CatOS que o QRadar Risk Manager pode acessar.

Os recursos a seguir estão disponíveis com o adaptador Cisco CatOS:

- Suporte de dados vizinhos
- Descoberta SNMP
- Roteamento Estático
- Protocolos de conexão Telnet e SSH

A tabela a seguir descreve os requisitos de integração para o adaptador do Cisco CatOS.

Tabela 8. Requisitos de Integração para aCisco CatOS do adaptador

Requisito de integração	**Descrição**
Versões	Dispositivos de chassi da série Catalyst 6500. 4.2 6,4 **Restrição:** O adaptador para CatOS faz backup apenas da estrutura da porta de comutação essencial. O backup dos adaptadores do Multilayer Switch Feature Card (MSFC) CatOS é feito pelos adaptadores do Cisco IOS. Os adaptadores do Firewall Services Module (FWSM) CatOs são submetidos a backup por adaptadores Cisco ASA.
Descoberta SNMP	Corresponde CATOS ou Catalyst Operating System no sysDescr SNMP.
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha** **Ativar Senha**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **Telnet** **SSH**

Tabela 8. Requisitos de Integração para aCisco CatOS do adaptador (continuação)

Requisito de integração	Descrição

Comandos que o adaptador requer para efetuar login e coletar dados	`show version`
	`whichboot`
	`show module`
	`show mod ver`
	`show system`
	`show flash devices`
	`show flash ...`
	`show snmp ifalias`
	`show port ifindex`
	`show interface`
	`show port`
	`show spantree`
	`show ip route`
	`show vlan`
	`show vtp domain`
	`show arp`
	`show cdp`
	`show cam dynamic`
	`show port status`
	`show counters`

Cisco IOS

IBM Security QRadar Risk Manager suporta a Cisco Internet Operating System (IOS)do adaptador.

O adaptador do Cisco IOS coleta configurações de dispositivo fazendo backup de comutações e roteadores de rede baseados em IOS.

Os recursos a seguir estão disponíveis com o adaptador Cisco IOS:

- Suporte de dados vizinhos
- NAT dinâmico
- NAT estático
- Descoberta SNMP
- Roteamento Estático
- Roteamento dinâmico EIGRP e OSPF
- Tunelamento P2P/VPN
- Protocolos de conexão Telnet e SSH

A tabela a seguir descreve os requisitos de integração para Cisco IOS.

Tabela 9. Requisitos de integração para o Cisco IOS

Requisito de integração	Descrição
Versões	IOS 12.0 a 15.1 para roteadores e comutadores Cisco Catalyst 6500 comuta com MSFC. Utilize o adaptador Cisco IOS para fazer backup da configuração e do estado dos serviços placa de MSFC. Se um roteador de série Cisco IOS 7600 possui um FWSM, utilize o adaptador Cisco ASA para fazer backup do FWSM.
Nível de acesso de usuário	Um usuário com o nível de privilégio executável de comando para cada comando que o adaptador requer para efetuar login e coletar dados. Por exemplo, é possível configurar um usuário de nível de privilégio customizado 10 que use a autenticação de banco de dados local. O exemplo a seguir configura todos os comandos `show ip` para o nível de privilégio 10. `privilege exec level 10 show ip`
Descoberta SNMP	Corresponde ISO ou Sistema operacional de internet Cisco no SNMP sysDescr.
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha** **Ativar nome do usuário** (Opcional) Use esse campo se o usuário precisar inserir um nível de privilégio específico ao efetuar login no dispositivo. Use o formato `level-<n>`, em que *n* é um nível de privilégio [0-15]. Por exemplo, para inserir o nível de privilégio 10, insira o comando a seguir: `level-10` Isso resulta no envio do comando **`enable 10`** para o dispositivo Cisco. **Ativar senha** (Opcional)
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **Telnet** **SSH**

Tabela 9. Requisitos de integração para o Cisco IOS (continuação)

Requisito de integração	Descrição

Comandos que o adaptador requer para efetuar login e coletar dados	`show access-lists`
	`show cdp neighbors detail`
	`show diag`
	`show diagbus`
	`show file systems`
	`show glbp`
	`show install running`
	`show interfaces`
	`show inventory`
	`show ip route ospf`
	`show mac address-table dynamic`
	`show module`
	`show mod version`
	`show object-group`
	`show power`
	`show snmp`
	`show spanning-tree`
	`show standby`
	`show startup-config`
	`show version`
	`show vlan`
	`show vrrp`
	`show vtp status`

Tabela 9. Requisitos de integração para o Cisco IOS (continuação)

Requisito de integração	Descrição

`show ip` comandos que o adaptador requer para efetuar login e coletar dados	`show ip arp`
	`show ip bgp neighbors`
	`show ip eigrp interface`
	`show ip eigrp neighbors`
	`show ip eigrp topology`
	`show ip ospf`
	`show ip ospf interface`
	`show ip ospf neighbor`
	`show ip protocols`
	`show ip route eigrp`
	`terminal length 0`

Cisco Nexus

Para integrar IBM Security QRadar Risk Manager com a sua rede de dispositivos, certifique-se de que consiga revisar os requisitos para o adaptador do Cisco Nexus.

Os recursos a seguir estão disponíveis com o adaptador Cisco Nexus:

- Suporte de dados vizinhos
- Descoberta SNMP
- Roteamento dinâmico EIGRP e OSPF
- Roteamento Estático
- Protocolos de conexão Telnet e SSH

A tabela a seguir descreve os requisitos de integração para o adaptador do Cisco Nexus.

Tabela 10. Requisitos de Integração para o adaptador do Cisco Nexus

Requisito de integração	Descrição
Versões e níveis de sistema operacional suportados	Nexus 5548: nível de sistema operacional 6.0 Nexus série 7000: nível de sistema operacional 6.2 Nexus série 9000: nível de sistema operacional 6.1
Descoberta SNMP	Corresponde *Cisco NX-OS* e uma cadeia de qualificação opcional que termina com *Software* no sysDescr SNMP. **Exemplo::** *(Cisco NX\-OS.* Software)*

Tabela 10. Requisitos de Integração para o adaptador do Cisco Nexus (continuação)

Requisito de integração	Descrição
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha** **Ativar Senha** **Se você incluir Virtual Device Contexts (VDCs) como dispositivos individuais, assegure-se de que as credenciais necessárias permitam as ações a seguir:** Acessar a conta que está ativada para o VDCs. Usar os comandos necessários nesse contexto virtual.
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **Telnet** **SSH**

Tabela 10. Requisitos de Integração para o adaptador do Cisco Nexus (continuação)

Requisito de integração	Descrição

Comandos que o adaptador requer para efetuar login e coletar dados	`show hostname`
	
	`show version`
	
	`show vdc`
	
	`show vdc current-vdc`
	
	`switchto vdc <vdc>` em que *vdc* é um `vdc` ativo que é listado ao inserir o comando `show vdc`.
	
	`show snmp`
	
	`dir <filesystem>` em que *filesystem* é `bootflash`, `slot0`, `volatile`, `log`, `logflash` ou `system`.
	
	`show running-config`
	
	`show startup-config`
	
	`show module`
	
	`show interface brief`
	
	`show interface snmp-ifindex`
	
	`show ip access-lists`
	
	`show vlan`
	
	`show vtp status`
	
	`show spanning-tree summary`
	
	`show object-group`
	
	`show interface <interface>` em que *interface* é qualquer interface listada ao inserir o comando `show running-config`.
	
	`show hsrp`
	
	`show vrrp`
	
	`show vtp`
	
	`show glbp`
	
	`show ip eigrp`
	
	`show ip route eigrp`
	
	`show ip ospf`
	
	`show ip route ospf`
	
	`show ip rip`
	
	`show ip route rip`

Tabela 10. Requisitos de Integração para o adaptador do Cisco Nexus (continuação)

Requisito de integração	Descrição

Comandos de telemetria	`terminal length 0`
	
	`show hostname`
	
	`show vdc`
	
	`switchto vdc <vdc>` em que *vdc* é um `vdc` ativo que é listado ao inserir o comando `show vdc`.
	
	`show cdp entry all`
	
	`show interface brief`
	
	`show ip arp`
	
	`show mac address-table`
	
	`show ip route`

Métodos para incluir VDCs para dispositivos Cisco Nexus

Utilize Gerenciamento de origem de configuração para incluir dispositivos de rede Nexus e Virtual Device Contexts (VDC) para IBM Security QRadar SIEM. Há duas formas de incluir diversos VDCs no IBM Security QRadar Risk Manager.

É possível incluir VDCs como subdispositivos do dispositivo Nexus ou como dispositivos individuais.

Visualizar Virtual Device Contexts

Se você incluir VDCs como dispositivos individuais, cada VDC será exibido como um dispositivo na topologia.

Se incluir VDCs como subdispositivos, eles não serão exibidos na topologia. É possível visualizar os VDCs na janela Monitor de configuração.

Incluindo VDCs como subdispositivos de seu dispositivo Cisco Nexus

Use o Gerenciamento de origem de configuração para incluir VDCs como subdispositivos de seu dispositivo Cisco Nexus.

Procedimento

1. Ative os seguintes comandos para o usuário que está especificado nas credenciais:
   - `show vdc` (contexto de administrador)
   - `switchto vdc x`, em que *x* é o VDC suportado.

   Em Monitor de configuração, é possível visualizar o dispositivo Nexus na topologia e os subdispositivos VDC. Para obter informações sobre a visualização de dispositivos, consulte o *IBM Security QRadar Risk Manager User Guide*.
2. Use o Gerenciamento de origem de configuração para incluir o endereço IP de *contexto de administrador* do dispositivo Nexus.

Para obter mais informações, consulte “Incluindo um dispositivo de rede” na página 5.

Incluindo VDCs como dispositivos individuais

Use o Gerenciador de origem de configuração para incluir cada VDC (Virtual Device Context) como um dispositivo separado. Ao usar esse método, o dispositivo Nexus e os VDCs são exibidos na topologia.

Ao visualizar o dispositivo Cisco Nexus e os VDCs na topologia, a contenção do chassi é representada separadamente.

Procedimento

1. Utilize o Gerenciamento de origem de configuração para incluir o endereço IP adm. de cada VDC.

   Para obter mais informações, consulte “Incluindo um dispositivo de rede” na página 5.
2. Utilize o Gerenciamento de origem de configuração para obter as informações de configuração para suas VDCs.
3. No dispositivo Cisco Nexus, utilize o Cisco Nexus CLI para desativar o comando **switchto vdc** para o nome do usuário que está associado ao adaptador.

   Exemplo:: Se o nome de usuário para um dispositivo for Cisco Nexus *qrmuser*, digite os seguintes comandos:

```
 NexusDevice(config)# role name qrmuser
NexusDevice(config-role)# rule 1 deny command switchto vdc
NexusDevice(config-role)# rule 2 permit command show *
NexusDevice(config-role)# rule 3 permit command terminal
NexusDevice(config-role)# rule 4 permit command dir
```

Cisco Security Appliances

Para integrar IBM Security QRadar Risk Manager com a sua rede de dispositivos, assegure que você reveja os requisitos para a Cisco Security Appliances do adaptador.

Os recursos a seguir estão disponíveis com o adaptador Cisco Security Appliances:

- Suporte de dados vizinhos
- NAT estático
- Descoberta SNMP
- Roteamento dinâmico EIGRP e OSPF
- Roteamento Estático
- Tunelamento IPSEC
- Protocolos de conexão Telnet e SSH

O adaptador Cisco Security Appliances coleta as configurações do dispositivo fazendo o backup dos dispositivos da família Cisco. O adaptador Cisco Security Appliances suporta os firewalls a seguir:

- Cisco Adaptive Security Appliances (ASA) 5500 series
- Firewall Service Module (FWSM)
- Módulo em um chassi de Catalisador
- Dispositivo Private Internet Exchange (PIX) Estabelecido.

Nota: Os contextos transparentes do Cisco ASA não podem ser colocados na topologia do QRadar Risk Manager e não é possível executar procuras de caminho nesses contextos transparentes.

A tabela a seguir descreve os requisitos de integração para o adaptador do Cisco Security Appliances.

Tabela 11. Requisitos de Integração para o adaptador do Cisco Security Appliances

Requisito de integração	Descrição
Versões	ASA: 8.2, 8.4 a 9.1.7 PIX: 6.1, 6.3 FWSM: 3.1, 3.2

Nível mínimo de acesso de usuário	nível de privilégio 5
	
	É possível fazer backup de dispositivos com o nível de acesso de nível de privilégio 5. Por exemplo, é possível configurar um usuário de nível 5 que use autenticação de banco de dados local, executando os comandos a seguir:
	
	`aaa authorization command LOCAL`
	
	`aaa authentication enable console LOCAL`
	
	`privilege cmd level 5 mode exec command terminal`
	
	`privilege cmd level 5 mode exec command changeto` (somente *multicontexto*)
	
	`privilege show level 5 mode exec command running-config`
	
	`privilege show level 5 mode exec command startup-config`
	
	`privilege show level 5 mode exec command version`
	
	`privilege show level 5 mode exec command shun`
	
	`privilege show level 5 mode exec command names`
	
	`privilege show level 5 mode exec command interface`
	
	`privilege show level 5 mode exec command pager`
	
	`privilege show level 5 mode exec command arp`
	
	`privilege show level 5 mode exec command route`
	
	`privilege show level 5 mode exec command context`
	
	`privilege show level 5 mode exec command mac-address-table`

Descoberta SNMP	Corresponde o PIX ou Adaptive Security Appliance ou Firewall Service Module em SNMP sysDescr.

Tabela 11. Requisitos de Integração para o adaptador do Cisco Security Appliances (continuação)

Requisito de integração	Descrição
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha** **Ativar Senha**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **Telnet** **SSH** **SCP**

Tabela 11. Requisitos de Integração para o adaptador do Cisco Security Appliances (continuação)

Requisito de integração	Descrição

Comandos necessários que o adaptador requer para efetuar login e coletar dados	`changeto context <context>`
	
	`changeto system`
	
	`show running-config`
	
	`show startup-config`
	
	`show arp`
	
	`show context`
	
	`show interface`
	
	`show mac-address-table`
	
	`show names`
	
	`show ospf neighbor`
	
	`show route`
	
	`show shun`
	
	`show version`
	
	`terminal pager 0`
	
	`show interface detail`
	
	`show crypto ipsec sa`
	
	`show eigrp topology`
	
	`show eigrp neighbors`
	
	`show firewall`
	
	O comando `changeto context <context>` é usado para cada contexto no dispositivo ASA.
	
	O comando `changeto system` detecta se o sistema tem configurações *multicontexto* e determina o *contexto de administrador*.
	
	O comando `changeto context` será necessário se o comando `changeto system` tiver uma configuração *multicontexto* ou um contexto de *configuração de administrador*.
	
	O comando `terminal pager` é usado para desligar o comportamento de paginação.

F5 BIG-IP

IBM Security QRadar Risk Manager suporta o adaptador F5 BIG-IP.

Os recursos a seguir estão disponíveis com o adaptador F5 BIG-IP:

- Suporte de dados vizinhos
- NAT dinâmico
- NAT estático
- Descoberta SNMP
- Roteamento Estático
- Protocolos de conexão Telnet e SSH

Os dispositivos de balanceador de carga F5 BIG-IP que executam o Local Traffic Manager (LTM) são suportados.

No dispositivo F5 BIG-IP, deve-se configurar a função **Administrador** para o nome do usuário que o QRadar Risk Manager usa para backup e configurar o **Shell avançado** para o **Acesso ao terminal**.

A tabela a seguir descreve os requisitos de integração para o adaptador F5 BIG-IP.

Tabela 12. Requisitos de integração para o adaptador F5 BIG-IP

Requisito de integração	Descrição
Versões	10.1.1 11.4.1
Descoberta SNMP	Corresponde ao F5 BIG-IP no sysDescr SNMP
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**SSH**

Tabela 12. Requisitos de integração para o adaptador F5 BIG-IP (continuação)

Requisito de integração	Descrição
Comandos que o adaptador requer para efetuar login e coletar dados	nome do arquivo gato dmesg uptime route -n ip addr list snmpwalk -c public localhost 1.3.6.1.4.1.3375.2.1.2.4.3.2.1.1 snmpwalk -c public localhost 1.3.6.1.4.1.3375.2.1.2.4.3.2.1.2
Comandos que o adaptador requer para efetuar login e coletar dados bigpipe	bigpipe global bigpipe system hostname bigpipe platform bigpipe version show bigpipe db packetfilter bigpipe db packetfilter.defaultaction bigpipe packet filter list bigpipe nat list all bigpipe vlan show all bigpipe vlangroup list all bigpipe vlangroup bigpipe interface show all bigpipe interface all media speed bigpipe trunk all interfaces bigpipe stp show all bigpipe route all list all bigpipe mgmt show all bigpipe mgmt route show all bigpipe pool bigpipe self bigpipe virtual list all bigpipe snat list all bigpipe snatpool list all
Comandos que o adaptador requer para efetuar login e coletar dados	b db snat.anyipprotocol

Tabela 12. Requisitos de integração para o adaptador F5 BIG-IP (continuação)

Requisito de integração	Descrição

Comandos que o adaptador requer para efetuar login e coletar dados tmsh	`tmsh -q list sys global-settings hostname`
	`tmsh -q show sys version`
	`tmsh -q show sys hardware`
	`tmsh -q list sys snmp sys-contact`
	`tmsh -q show sys memory`
	`tmsh -q list /net interface all-properties`
	`tmsh -q list net trunk`
	`tmsh -q list /sys db packetfilter`
	`tmsh -q list /sys db packetfilter.defaultaction`
	`tmsh -q list /net packet-filter`
	`tmsh -q list /net vlan all-properties`
	`tmsh -q show /net vlan`
	`tmsh -q list /net vlan-group all all-properties`
	`tmsh -q list net tunnels`

Comandos que o adaptador requer para efetuar login e coletar dados tmsh (continuação)	`tmsh -q show /net vlan-group`
	`tmsh -q list ltm virtual`
	`tmsh -q list ltm nat`
	`tmsh -q list ltm snatpool`
	`tmsh -q list ltm snat`
	`tmsh -q list sys db snat.anyipprotocol`
	`tmsh -q list net stp-globals all-properties`
	`tmsh -q list net stp priority`
	`tmsh -q list net stp all-properties`
	`tmsh -q list net route`
	`tmsh -q list sys management-ip`
	`tmsh -q list sys management-route`
	`tmsh -q list ltm pool`
	`tmsh -q list net self`
	`tmsh -q list net ipsec`

Arquivos coletados	`/config/bigip.license`
	`/config/snmp/snmpd.conf`
	`/etc/passwd`

Fortinet FortiOS

O adaptador IBM Security QRadar Risk Manager para Fortinet FortiOS suporta dispositivos Fortinet FortiGate que executam o sistema operacional Fortinet (FortiOS).

Os recursos a seguir estão disponíveis com o adaptador Fortinet FortiOS:

- NAT estático
- Roteamento Estático
- Protocolos de conexão Telnet e SSH

O adaptador Fortinet FortiOS interage com o FortiOS através de Telnet ou SSH. A lista a seguir descreve algumas limitações do QRadar Risk Manager e do adaptador Fortinet FortiOS:

- Endereços baseados em geografia e políticas referenciadas não são suportados pelo QRadar Risk Manager.
- As políticas baseadas na identidade, de VPN e de Internet Protocol Security não são suportadas pelo QRadar Risk Manager.
- Políticas que usam os perfis Unified Threat Management (UTM) não são suportadas pelo adaptador Fortinet FortiOS. Somente as políticas de firewall da Camada 3 são suportadas.
- Rotas de políticas não são suportadas.
- Os domínios virtuais com os links virtuais que têm endereços IP parciais ou que não têm endereço IP não são suportados.

Os requisitos de integração para o adaptador Fortinet FortiOS são descritos na tabela a seguir:

Tabela 13. Requisitos de integração para o adaptador Fortinet FortiOS

Requisito de Integração	**Descrição**
Versão	4.0 MR3 à 5.2.4
Descoberta SNMP	Não
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **Telnet** **SSH**
Requisitos do nível de acesso de usuário	Acesso de leitura/gravação para firewalls Fortinet que têm VDOMs ativados Acesso somente leitura para firewalls Fortinet que não têm VDOMs ativados

Tabela 13. Requisitos de integração para o adaptador Fortinet FortiOS (continuação)

Requisito de Integração	Descrição

Comandos que o adaptador requer para efetuar login e coletar dados	`config system console`
	
	`set output standard`
	Nota: Os comandos `config system console` e `set output standard` requerem um usuário com acesso de leitura/gravação para a configuração do sistema. Se você usar um usuário somente leitura com paginação ativada ao fazer backup de um dispositivo Fortigate, o desempenho será afetado significativamente.
	
	`show system interface`
	
	`get hardware nic <variable>`
	
	`get system status`
	
	`get system performance status`
	
	`get router info routing-table static`
	
	`get test dnsproxy 6`
	
	`show firewall addrgrp`
	
	`show firewall address`
	
	`show full-configuration`
	
	`get firewall service predefined <variable>`
	
	`show firewall service custom`
	
	`show firewall service group`
	
	`show firewall policy`
	
	`show system zone`
	
	`show firewall vip`
	
	`show firewall vipgrp`
	
	`show firewall ippool`

Comandos para usar com VDOMs	`config global` para inserir o modo de configuração global `config vdom; edit <vdom-name>` para alternar entre VDOMs

Adaptador SNMP genérico

O IBM Security QRadar Risk Manager suporta dispositivos que executam um agente do SNMP com o adaptador SNMP genérico.

Esse adaptador interage com o agente do SNMP usando as consultas SNMP.

Os identificadores de objeto (OIDs) estão contidos no MIB-2 do SNMP e é possível esperar todos os agentes do SNMP exporem esses OIDs.

A seguir estão as limitações do adaptador:

- Coleta somente informações da interface básica e do sistema básico. As regras e as informações de roteamento não são coletadas.
- Mesmo que exibido na UI do **Gerenciamento de origem de configuração**, com SNMPv3, o adaptador não suporta a criptografia AES.
- O adaptador não suporta a criptografia AES com SNMPv3, mesmo que possa parecer suportá-la na janela Gerenciamento de origem de configuração.

Os requisitos de integração para o adaptador SNMP genérico são descritos na tabela a seguir:

Requisito de Integração	**Descrição**
Versão	SNMPv1, SNMPv2c, SNMPv3
Suporte de dados vizinhos	Não
Descoberta SNMP	Não
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	O SNMPv1 e SNMPv2c requerem **SNMP Get Community** O SNMPv3 requer **Nome de Usuário de Autenticação SNMPv3** O SNMPv3 pode ter uma das credenciais a seguir: **Senha de Autenticação SNMPv3** **Senha de Privacidade SNMPv3**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **SNMPv1** **SNMPv2c** **SNMPv3 usando MD5** **SHA com DES**

Requisito de Integração	Descrição
Comandos que o adaptador requer para efetuar login e coletar dados	Comandos SNMP Get .1.3.6.1.2.1.1.1.0 .1.3.6.1.2.1.1.2.0 .1.3.6.1.2.1.1.3.0 .1.3.6.1.2.1.1.4.0 .1.3.6.1.2.1.1.5.0 .1.3.6.1.2.1.1.6.0 Comandos SNMP Walk .1.3.6.1.2.1.2.2.1.2 .1.3.6.1.2.1.2.2.1.3 .1.3.6.1.2.1.2.2.1.4 .1.3.6.1.2.1.2.2.1.5 .1.3.6.1.2.1.2.2.1.6 .1.3.6.1.2.1.2.2.1.7 .1.3.6.1.2.1.4.20

ProVision HP Networking

O IBM Security QRadar Risk Manager suporta o adaptador HP Networking ProVision.

Os recursos a seguir estão disponíveis com o adaptador HP Networking ProVision:

- Suporte de dados vizinhos
- Descoberta SNMP
- Roteamento dinâmico RIP
- Protocolos de conexão Telnet e SSH

A tabela a seguir descreve os requisitos de integração para o adaptador ProVision HP Networking.

Tabela 14. Requisitos de integração para o adaptador do ProVision HP Networking

Requisito de integração	Descrição
Versões	Comutadores HP Networking ProVision K/KA.15.X **Restrição:** Os comutadores HP que executam um sistema operacional Comware não são suportados por esse adaptador.
Descoberta SNMP	Corresponde a números de versão com o formato `HP(.*)Switch(.*)(revisão [A-Z]{1,2}\.(\d+)\.(\d+))` em sysDescr.

Tabela 14. Requisitos de integração para o adaptador do ProVision HP Networking (continuação)

Requisito de integração	Descrição
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha** **Ativar Senha**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**SSH**

Tabela 14. Requisitos de integração para o adaptador do ProVision HP Networking (continuação)

Requisito de integração	Descrição
Comandos de operação de backup emitidos pelo adaptador para o dispositivo	dmesgshow system power-supply getmib show access-list vlan <*vlan id*> show access-list show access-list <*name or number*> show access-list ports <*port number*> show config show filter show filter <*id*> show running-config show interfaces brief show interfaces <*interface id*> Para cada interface. show jumbos show trunks show lacp show module show snmp-server show spanning-tree show spanning-tree config show spanning-tree instance <*id or list*> (para cada spanning-tree que estiver configurado no dispositivo) show spanning-tree mst-config show system information show version show vlans show vlans <*id*> (para cada vlan) show vrrp walkmib

Tabela 14. Requisitos de integração para o adaptador do ProVision HP Networking (continuação)

Requisito de integração	Descrição

Comandos de operação de backup `show ip` que são emitidos pelo adaptador para o dispositivo	`show ip`
	`show ip route`
	`show ip odpf`
	`show ip odpf redistribute`
	`show ip rip`
	`show ip rip redistribute`

telemetria e comandos de dados vizinho	`getmib`
	`show arp`
	`show cdp neighbors`
	`show cdp neighbors detail <port number>`
	`show interfaces brief`
	`show interface`
	`show ip route`
	`show lldp info remote-device`
	`show lldp info remote-device <port number>`
	`show mac-address or show mac address`
	`show system information`
	`show vlans`
	`show vlans custom id state ipaddr ipmask`
	`walkmib`

Juniper Networks JUNOS

Para integrar IBM Security QRadar Risk Manager com a sua rede de dispositivos, certifique-se de que consiga revisar os requisitos para o adaptador do Juniper Networks JUNOS.

Os recursos a seguir estão disponíveis com o adaptador Juniper Networks JUNOS:

- Suporte de dados vizinhos
- Descoberta SNMP
- Roteamento dinâmico OSPF
- Roteamento Estático
- Protocolos de conexão Telnet e SSH

A tabela a seguir descreve os requisitos de integração para o adaptador do Juniper Networks JUNOS.

Tabela 15. Requisitos de integração para o adaptador do Juniper Networks JUNOS

Requisito de integração	**Descrição**
Versões	10.4 11.2 a 12.3 13.2
Descoberta SNMP	Corresponde ao sysOID SNMP: 1.3.6.1.4.1.2636
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **Telnet** **SSH** **SCP**

Tabela 15. Requisitos de integração para o adaptador do Juniper Networks JUNOS (continuação)

Requisito de integração	Descrição

Comandos que o adaptador requer para efetuar login e coletar dados	`show version`
	`show system uptime`
	`show chassis hardware`
	`show chassis firmware`
	`show chassis mac-address`
	`show chassis routing-engine`
	`show configuration snmp`
	`show snmp mib walk system configure`
	`show configuration firewall`
	`show configuration firewall family inet6`
	`show configuration security`
	`show configuration security zones`
	`show interfaces`
	`show interfaces filters`
	`show ospf interface detail`
	`show bgp neighbor`
	`show configuration routing-option`
	`show arp no-resolve`
	`show ospf neighbor`
	`show rip neighbor`

Juniper Networks NSM

O adaptador IBM Security QRadar Risk Manager suporta o Juniper Networks NSM (Network and Security Manager).

Você pode utilizar o QRadar Risk Manager para fazer backup de um único dispositivo Juniper Networks ou obter informações sobre o dispositivo a partir de um console Juniper Networks NSM.

O console Juniper Networks NSM (Network and Security Manager) contém a configuração e as informações sobre o dispositivo para roteadores e comutadores Juniper Networks que são gerenciados pelo console Juniper Networks NSM.

É possível usar os protocolos de conexão HTTPS e SOAP com o Juniper Networks NSM.

A tabela a seguir descreve os ambientes suportados para Juniper Networks NSM.

Tabela 16. Ambientes suportados pelo adaptador QRadar Risk Manager para o Juniper Networks NSM

Ambiente suportado	Descrição
Versões	Dispositivos IDP que são gerenciados pelo NSM (Network and Security Manager)
Descoberta SNMP	Não Suportado
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **SOAP** **HTTP**

Juniper Networks ScreenOS

Para integrar IBM Security QRadar Risk Manager com a sua rede de dispositivos, certifique-se de que consiga revisar os requisitos para o adaptador do Juniper Networks ScreenOS.

Os recursos a seguir estão disponíveis com o adaptador Juniper Networks ScreenOS:

- Suporte de dados vizinhos
- NAT dinâmico
- NAT estático
- Descoberta SNMP
- Roteamento Estático
- Protocolos de conexão Telnet e SSH

A tabela a seguir descreve os requisitos de integração para o adaptador do Juniper Networks ScreenOS.

Tabela 17. Requisitos de Integração para o adaptador do Juniper Networks ScreenOS

Requisito de integração	Descrição
Versões	5.4 6.2
Descoberta SNMP	Corresponde netscreen ou SSG em sysDescr SNMP.
Parâmetros de credenciais obrigatórios	**Nome de usuário** **Senha**

Tabela 17. Requisitos de Integração para o adaptador do Juniper Networks ScreenOS (continuação)

Requisito de integração	Descrição
Protocolos de conexão suportados	Use qualquer um dos protocolos de conexão suportados a seguir: **Telnet** **SSH**

Comandos que o adaptador requer para efetuar login e coletar dados	`set console page 0`
	`get system`
	`get config`
	`get snmp`
	`get memory`
	`get file info`
	`get file`
	`get service`
	`get group address`*`zone group`*
	`get address`

Comandos que o adaptador requer para efetuar login e coletar dados (continuação)	`get service group`
	`get service group` *`variable`*
	`get interface`
	`get interface`*`variable`*
	`get policy all`
	`get policy id`*`variable`*
	`get admin user`
	`get route`
	`get arp`
	`get mac-learn`
	`get counter statistics interface` *`variable`*
	Em que *zone* são os dados de zona retornados do comando `get config`.
	group são os dados de grupo retornados a partir do comando `get config`.
	variable é uma lista de dados retornados a partir de um comando `get service group`, `get interface` ou `get policy id`.

Palo Alto

IBM Security QRadar Risk Manager suporta o adaptador Palo Alto. O adaptador Palo Alto usa a API REST baseada em XML do PAN-OS para se comunicar com os dispositivos de firewall Palo Alto.

Os recursos a seguir estão disponíveis com o adaptador Palo Alto:

- Suporte de dados vizinhos
- NAT dinâmico
- NAT estático
- Descoberta SNMP
- Tunelamento de IPSEC/VPN
- Applications
- Usuário/Grupos
- Protocolo de conexão HTTPS

Nota:

O adaptador Palo Alto não suporta políticas compartilhadas que são enviadas por push a dispositivos por um sistema de gerenciamento de segurança de rede Palo Alto Panorama.

A tabela a seguir descreve os requisitos de integração para o adaptador Palo Alto.

Tabela 18. Requisitos de integração para o adaptador Palo Alto

Requisito de integração	**Descrição**
Versões	PAN-OS Versões 5.0 a 7.0
Nível mínimo de acesso de usuário	Superusuário (acesso total) necessário para dispositivos PA que têm Listas de Bloqueios Dinâmicos para executar comandos de nível de sistema. Superusuário (somente leitura) para todos os outros dispositivos PA.
Descoberta SNMP	SysDescr corresponde a 'Palo Alto Networks(.*)série firewall' ou sysOid corresponde a 'panPA'
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**HTTPS**

Tabela 18. Requisitos de integração para o adaptador Palo Alto (continuação)

Requisito de integração	Descrição
Comandos necessários a serem usados para a operação de backup.	/api/?type=op&cmd=<show><system><info></info></system>/show> /api/?type=op&cmd=<show><config><running></running></config></show> /api/?type=op&cmd=<show><interface>all</interface></show>
Comandos opcionais a serem usados para a operação de backup.	/api/?type=op&cmd=<show><system><resources></resources></system></show> /api/?type=op&cmd=/config/predefined/service /api/?type=op&cmd=<request><system><external-list><show><name>$listName</name>< /show></external-list></system></request> em que *$listName* é uma variável nesse comando, que é executado várias vezes. /api/?type=op&cmd=<show><object><dynamic-address-group><all></all></dynamic-address-group></object></show> /api/?type=config&action=get&xpath=/config/predefined/application
Comandos necessários a serem usados para dados de telemetria e vizinhos.	/api/?type=op&cmd=<show><system><info></info></system></show> /api/?type=op&cmd=<show><interface>all</interface></show> /api/?type=op&cmd=<show><routing><interface></interface></routing></show>
Comandos opcionais a serem usados para dados de telemetria e vizinhos.	/api/?type=op&cmd=<show><counter><interface>all</interface></counter></show> /api/?type=op&cmd=<show><arp>all</arp></show> <show><mac>all</mac></show> /api/?type=op&cmd=<show><arp>all</arp></show> /api/?type=op&cmd=<show><routing><route></route></routing></show>
Comandos necessários a serem usados para o GetApplication.	/api/?type=config&action=get&xpath=/config/predefined/application

Sidewinder

O IBM Security QRadar Risk Manager suporta dispositivos McAfee Enterprise Firewall (Sidewinder) que executam o SecureOS.

Os recursos a seguir estão disponíveis com o adaptador Sidewinder:

- NAT estático
- Roteamento Estático
- Protocolos de conexão Telnet e SSH

O adaptador Sidewinder interage com o sistema operacional McAfee (SecureOS) baseado na CLI sobre Telnet ou SSH.

O adaptador Sidewinder possui as limitações a seguir:

- Somente as políticas de firewall da Camada 3 são suportadas porque as políticas da Camada 7 que usam as defesas do aplicativo Sidewinder não são suportadas.
- As políticas baseadas em Identidade, baseadas em geografia e IPv6 são descartadas, porque essas políticas não são suportadas pelo QRadar Risk Manager.

Os requisitos de integração para o adaptador Sidewinder são descritos na tabela a seguir:

Tabela 19. Adaptador Sidewinder

Requisito de Integração	**Descrição**
Versões suportadas	8.3.2
Nível mínimo de acesso de usuário	administrativo O nível de acesso de usuário administrador é necessário para recuperar informações de serviços predefinidos do banco de dados usando o comando **`cf appdb list verbose=on`**.
Descoberta SNMP	Não
Parâmetros de credenciais obrigatórios	**Nome de usuário** **Senha**
Protocolos de conexão suportados	Use qualquer um dos protocolos de conexão suportados a seguir: **SSH** **Telnet**

Tabela 19. Adaptador Sidewinder (continuação)

Requisito de Integração	Descrição

Comandos que o adaptador requer para efetuar login e coletar dados	`nome do host`
	`uname -r`
	`uptime`
	`cf license q`
	`cf route status`
	`cf ipaddr q`
	`cf iprange q`
	`cf subnet q`
	`cf domain q`
	Use `"dig $address +noall +answer"` para cada saída de domínio de: `cf domain q`
	`cf host q`
	`cf netmap q`
	`cf netgroup q`
	`cf appdb list verbose=on`
	`cf application q`
	`cf appgroup q`
	`cf policy q`
	`cf interface q`
	`cf zone q`

Sourcefire 3 D Sensor

Para integrar IBM Security QRadar Risk Manager com a sua rede de dispositivos, certifique-se de que consiga revisar os requisitos para o adaptador do Sourcefire 3 D Sensor.

Os recursos a seguir estão disponíveis com o adaptador Sourcefire 3 D Sensor:

- IPS
- Protocolo de conexão SSH

Limitações:

- Políticas de intrusão anexadas a regras de controle de acesso individuais não são usadas pelo QRadar Risk Manager. Apenas a política de intrusão padrão é suportada.
- NAT e VPN não são suportados.

A tabela a seguir descreve os requisitos de integração para o adaptador do Sourcefire 3 D Sensor.

Tabela 20. Requisitos de Integração para o adaptador do Sourcefire 3 D Sensor

Requisito de integração	**Descrição**
Versões	5.2
Sensores 3D suportados (dispositivos Série 2)	3D500 3D1000 3D2000 3D2100 3D2500 3D3500 3D4500 3D6500 3D9900
Descoberta SNMP	Não
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**Nome de usuário** **Senha**
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	**SSH**

Tabela 20. Requisitos de Integração para o adaptador do Sourcefire 3 D Sensor (continuação)

Requisito de integração	Descrição
Comandos que o adaptador requer para efetuar login e coletar dados	show version show memory show network show interfaces expert sudo su df nome do host ip addr route cat find head mysql

Adaptador IPS TippingPoint

O IBM Security QRadar Risk Manager suporta dispositivos IPS (sistema de prevenção de intrusão) TippingPoint que executam o TOS e que estão sob controle do SMS.

Os recursos a seguir estão disponíveis com o adaptador TippingPoint IPS:

- IPS
- Protocolos de conexão Telnet, SSH+HTTPS

Esse adaptador requer interação com os dispositivos a seguir:

- IPS diretamente usando o sistema operacional TippingPoint (TOS) sobre Telnet ou SSH.
- TippingPoint Secure Management Server (SMS) por meio da API de serviços da web sobre HTTPS.

Uma conexão com o TippingPoint SMS é necessária para obter as assinaturas mais recentes do Digital Vaccines, que são gerenciadas pelo SMS.

Esse adaptador funciona somente com dispositivos IPS sob controle do SMS. Os serviços da web do SMS devem ser ativados para um backup bem-sucedido.

Essa lista descreve as limitações do adaptador TippingPoint:

- O QRadar Risk Manager não processa endereços IP de origem ou destino em regras ou filtros do IPS. Os recursos do TippingPoint a seguir não são suportados:
  - Filtros de gerenciamento de tráfego
  - Exceções e restrições de perfil ou filtro
  - Filtros definidos pelo usuário
- Filtros do IPS sem um CVE associado não são modelados porque o IPS não pode ser mapeado para nenhuma vulnerabilidade do QRadar.

Os requisitos de integração para o adaptador TippingPoint são descritos na tabela a seguir:

Tabela 21. Adaptador IPS TippingPoint

Requisito de Integração	**Descrição**
Versões Suportadas	TOS 3.6 e SMS 4.2
Nível mínimo de acesso de usuário	IPS: Operador SMS: Operador (customizado) Um usuário que pertence a um grupo com uma função *operador customizado*, que tem a opção `Acessar serviços da web do SMS` ativada.
Descoberta SNMP	Não
Parâmetros de credenciais obrigatórios Para incluir credenciais no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Insira as seguintes credenciais: **Nome do usuário**: *<IPS CLI username>* **Senha**: *<IPS CLI password>* **Ativar nome do usuário**: *<SMS username>* **Ativar senha**: *<SMS password>*
Protocolos de conexão suportados Para incluir protocolos no QRadar, efetue login como um administrador e use **Gerenciamento de origem de configuração** na guia **Administrador**.	Use qualquer um dos protocolos de conexão suportados a seguir: **Telnet** para a CLI do IPS **SSH** para a CLI do IPS **HTTPS** para SMS

Comandos que o adaptador requer para efetuar login e coletar dados	`show config`
	
	`show version`
	
	`show interface`
	
	`show host`
	
	`show sms`
	
	`show filter $filterNumber` (para cada assinatura localizada no Digital Vaccine)

Comandos de API enviados para o SMS para recuperar as assinaturas mais recentes	`https://<sms_server>/dbAccess/tptDBServlet?method=DataDictionary&table=SIGNATURE&format=xml`

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual
Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Quaisquer referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais nesses websites não fazem parte dos materiais deste produto IBM e o uso desses websites é de total responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Av. Pasteur, 138/146 - Botafogo
Rio de Janeiro, RJ
Estados Unidos

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Os dados de desempenho e os exemplos dos clientes citados são apresentados para fins ilustrativos apenas. Resultados reais de desempenho podem variar dependendo de configurações específicas e condições operacionais.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

As declarações relacionadas a direção ou intenção futuros da IBM estão sujeitas a alteração ou retirada sem aviso prévio e representam metas e objetivos apenas.

Os preços da IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso prévio. Os preços do revendedor podem variar.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer semelhança com empresas ou pessoas reais é mera coincidência.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas comerciais da International Business Machines Corp., registradas em muitas jurisdições no mundo inteiro. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou outras empresas. Uma lista atual das marcas comerciais da IBM está disponível na web em "Informações de marca comercial e copyright" em www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT e o logotipo Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos, outros países ou ambos.

Termos e condições para a documentação do produto

Permissões para o uso dessas publicações são concedidas de acordo com os seguintes termos e condições.

Aplicabilidade

Esses termos e condições estão completando quaisquer termos para uso do website IBM.

Uso pessoal

Você pode reproduzir estas publicações para seu uso pessoal, não comercial, desde que todos os avisos do proprietário sejam preservados. Você não pode distribuir, exibir ou fazer trabalho derivado dessas publicações, ou qualquer parte delas, sem o consentimento expresso da IBM.

Uso Comercial

É possível reproduzir, distribuir e exibir essas publicações unicamente dentro de sua empresa, contanto que todos os avisos do proprietário sejam preservados. Não é permitido criar trabalhos derivados destas publicações, ou reproduzir, distribuir ou exibir estas publicações ou qualquer porção das mesmas fora de sua empresa, sem o consentimento expresso da IBM.

Direitas

Exceto conforme expressamente concedido nessa permissão, nenhuma outra permissão, licença ou direito é concedido, seja expresso ou implícito, às publicações ou quaisquer informações, dados, software ou outra propriedade intelectual contida neste.

A IBM reserva-se o direito de retirar as permissões concedidas neste documento sempre que, a seu critério, o uso das publicações for prejudicial ao seu interesse ou, conforme determinado pela IBM, as instruções acima não estiverem sendo seguidas da maneira adequada.

O Cliente não pode fazer download, exportar ou reexportar estas informações, exceto se elas estiverem totalmente em conformidade com todas as leis e regulamentações aplicáveis, incluindo todas as leis e regulamentações de exportação dos Estados Unidos.

A IBM NÃO SE RESPONSABILIZA PELO CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE

ENCONTRAM" E SEM GARANTIA DE QUALQUER TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E DE ADEQUAÇÃO PARA UM PROPÓSITO ESPECÍFICO.

Declaração de privacidade on-line da IBM

Os produtos do software IBM, incluindo as soluções de software como serviço, (“Ofertas de software”) podem usar cookies ou outras tecnologias para coletar informações do uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar interações com o usuário final ou para outros propósitos. Em muitas casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoalmente identificáveis. Se esta Oferta de Software usar cookies para coletar informações pessoais identificáveis, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

Dependendo das configurações implementadas, essa Oferta de Software poderá usar cookies de sessão que coletam o ID da sessão de cada usuário para fins de gerenciamento de sessões e autenticação. Estes cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas para esta Oferta de Software fornecerem a capacidade de coletar, como cliente, informações pessoalmente identificáveis dos usuários finais por meio de cookies e outras tecnologias, deve-se consultar seu próprio conselho jurídico a respeito das leis aplicáveis a essa coleta de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de privacidade da IBM em http://www.ibm.com/privacy e a Declaração de privacidade online da IBM em http://www.ibm.com/privacy/details, a seção intitulada “Cookies, web beacons e outras tecnologias” e a “Declaração de privacidade de software como serviço e de produtos de software IBM” em http://www.ibm.com/software/info/product-privacy.

Impresso no Brasil