IBM Security QRadar Risk Manager
Versão 7.2.5

Guia de Configuração do Adaptador

Nota

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 41.

Informações do produto

Este documento se aplica a IBM QRadar Security Intelligence Platform V7.2.5 e liberações subsequentes, salvo se substituído por uma versão atualizada deste documento.

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.

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 localizar a documentação do produto IBM Security QRadar na web, incluindo 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 Accessing IBM Security Documentation Technical Note (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 Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Declaração de boas práticas de segurança

A segurança do sistema de TI envolve a proteção dos sistemas e de informações por meio de prevenção, detecção e resposta a acesso incorreto de dentro e fora da empresa. O acesso incorreto pode resultar em informações sendo alteradas, destruídas, desapropriadas ou usadas indevidamente ou pode resultar em danos ou uso impróprio dos sistemas, incluindo uso em ataques a outros. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança sozinha pode ser completamente efetiva na prevenção de uso ou acesso impróprios. Sistemas, produtos e serviços IBM são projetados para fazer parte de uma abordagem de segurança abrangente legal, que necessariamente envolverá procedimentos operacionais adicionais, podendo requerer outros sistemas, produtos ou serviços para ser mais eficiente. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU TORNEM SUA EMPRESA IMUNE CONTRA A CONDUTA MAL-INTENCIONADA OU ILEGAL DE QUALQUER PARTE.

Observação:

O uso deste programa pode implicar com várias leis ou regulamentos, incluindo aquelas relacionadas à privacidade, proteção de dados, emprego e comunicação e armazenamento eletrônicos. O IBM Security QRadar pode ser usado apenas para propósitos legais e de maneira legal. O cliente concorda e assume toda a

responsabilidade de usar este programa de acordo com as leis, regulamentos e políticas aplicáveis. O licenciado declara que obteve ou obterá as permissões ou licenças necessárias para permitir o uso do IBM Security QRadar dentro da lei.

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.

Nota: Não é possível importar dispositivos que usam um IP do servidor de gerenciamento, por exemplo, CPSMS e IBM Internet Security Systems GX.

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 todos os modelos, fabricantes e tipos de dispositivos suportados. O QRadar Risk Manager usa os dados para compreender a topologia e a configuração da rede dos 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 utiliza as credenciais do usuário configurado para acessar as configurações do dispositivo e de download.

Processo para integrar dispositivos de rede

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

1. Configure seu dispositivo de rede com acesso apropriado para QRadar Risk Manager.
2. Instale o adaptador apropriado para a seu dispositivo de rede em seu dispositivo do QRadar Risk Manager
3. Use o Configuration Source Management para incluir os dispositivos de rede no QRadar Risk Manager.
4. Defina o método de comunicação (protocolo) requerido para comunicação com os dispositivos de rede.

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

Se QRadar Risk Manager e seus dispositivos de rede não puderem se comunicar, consulte as informações do kit de ferramentas de configuração desconectado no *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:

- BIG-IP
- Check Point 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

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`

   `rpm -Uvh *.rpm`

   Por exemplo:

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

   `rpm -Uvh *.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

Utilize o comando **rpm** para remover um adaptador de 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:
   `rpm -e adapter file`

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

Capítulo 3. Métodos para incluir dispositivos de rede

Use o Configuration Source Management 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 NSM	Incluir dispositivos que são gerenciados por um console Juniper Networks NSM.
Descobrir CPSMS From SiteProtector	Incluir dispositivos que são gerenciados por um Check Point Security Manager Server (CPSMS).
Descobrir	Incluir dispositivos a partir de SiteProtector.

Incluindo um dispositivo de rede

Para incluir um dispositivo de rede para IBM Security QRadar Risk Manager, utilize Configuration Source Management.

Antes de Iniciar

Revise as versões de software suportadas, credenciais e comandos necessários para os dispositivos de rede. Para obter mais informações, consulte Capítulo 4, “Adaptadores suportados”, na página 11.

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 Configuration Source Management.
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. Use um curinga de tipo `10.1.*.*` ou para utilizar 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 do conjunto de credenciais que você criou e digite 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 são solicitadas as credenciais do usuário no modo especialista.
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 Configuration Source Management:

- 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 mais informações sobre a configuração de origens no *IBM Security QRadar Risk Manager User Guide*.

7. No menu de navegação, inclua um dispositivo.
   - Para incluir um dispositivo de rede, clique em **Incluir Dispositivo**.
   - Para incluir vários endereços IP para dispositivos de rede, selecione **Descobrir Dispositivos**.
8. Digite o endereço IP para o dispositivo e selecione o tipo de adaptador, e, em seguida, clique em **Incluir**.

   Um ponto de interrogação azul é exibido na lista de dispositivos para dispositivos que não são submetidos a backup.

9. Selecione o dispositivo que você incluiu na lista de dispositivos, e clique em **Backup**.
10. Repita essas etapas para cada tipo de dispositivo de rede que você deseja incluir.

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 gerenciados por um console Juniper Networks NSM

Utilize o Configuration Source Management para incluir todos os dispositivos de um console do Juniper Networks NSM 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 4, "Adaptadores suportados", na página 11.

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 **Configuration Source Management**.
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. Use um curinga de tipo `10.1.*.*` ou para utilizar 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 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 no serviço da Web do Juniper NSM. 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: Juniper Networks NSM não suporta o SNMP.

7. No menu de navegação, **Descobrir de 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*.

Incluir dispositivos gerenciados por um console CPSMS

Use o Configuration Source Management para incluir todos os dispositivos a partir de um Check Point Security Manager Server (CPSMS) para 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 4, “Adaptadores suportados”, na página 11.

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

É necessário repetir este procedimento para cada CPSMS que você deseja contatar 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 **Configuration Source Management**.
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 de seu dispositivo CPSMS, e 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 o conjunto de credenciais, e clique em **OK**.
   b. Selecione o nome do conjunto de credenciais que você criou e digite um nome de usuário e uma senha válidos para o dispositivo.
7. Digite o nome do SIC de Entidade OPSEC do CPSMS que gerencia os dispositivos de firewall que serão descobertos. Esse valor DEVE ser exato e as mudanças de formato dependem do tipo de dispositivo a partir do qual você está fazendo a descoberta:

Tipo	Nome
Servidor de Gerenciamento	`CN=cp_mgmt,O=<take O value from DN field>`
Gateway para o Servidor de Gerenciamento	`CN=cp_mgmt_<gateway hostname>,O=<take O value from DN field>`

   Por exemplo, quando estiver fazendo uma descoberta a partir do Servidor de Gerenciamento:
   - DN do Aplicativo OPSEC: `CN=cpsms226,O=vm226-CPSMS..bs7ocx`
   - Host do Aplicativo OPSEC: `vm226-CPSMS`

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

   Por exemplo, quando estiver fazendo uma descoberta a partir do Gateway para o Servidor de Gerenciamento:
   - DN do Aplicativo OPSEC: `CN=cpsms230,O=vm226-CPSMS..bs7ocx`
   - Host do Aplicativo OPSEC: `vm230-CPSMS2-GW3`

   O Nome 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 SIC do Objeto de Aplicativo OPSEC que foi 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 **Descobrir Na Check Point SMS**e, em seguida, insira o endereço CPSMS IP.

12. Clique em **OK**.
13. Repita essas etapas para cada dispositivo CPSMS que você deseja incluir.

O que Fazer Depois

Depois de incluir todos os dispositivos necessários, será possível fazer backup de dispositivos e, em seguida, visualizá-las na topologia.

Incluindo dispositivos gerenciados por SiteProtector

Utilize o Configuration Source Management 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 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 Configuration Source Management.
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 SiteProtector , e 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 o conjunto de credenciais, e clique em **OK**.
   b. Selecione o nome do conjunto de credenciais que você criou e digite um nome de usuário e uma senha válidos para o dispositivo.

      Restrição: O nome do usuário e a senha são as mesmas credenciais utilizadas para acessar o banco de dados doSiteProtector 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

Depois de incluir todos os dispositivos necessários, será possível fazer backup de dispositivos e, em seguida, visualizá-las na topologia.

Capítulo 4. Adaptadores suportados

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

A lista de adaptadores suportados e a documentação para eles está crescendo constantemente. Se um adaptador do dispositivo de rede não estiver listado, entre em contato com seu representante de vendas IBM.

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.

Dispositivos SNMP genéricos não têm rotas e, portanto, não transmitem o tráfego.

Parâmetros de credenciais obrigatórios

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

É possível utilizar o Configuration Source Management para configurar credenciais do dispositivo. 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.

Protocolos de conexão

Especifica os protocolos suportados para o dispositivo de rede.

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.

BIG-IP

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

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

Tabela 4. Requisitos de integração para o adaptador BIG-IP

Requisito de integração	**Descrição**
Versões	BIG-IP versão 10 e posterior.
Suporte de dados vizinhos	Suportado
Descoberta SNMP	Corresponde BIG-IP em sysDescr SNMP.
Parâmetros de credenciais obrigatórios	`Nome de usuário` `Senha`
Protocolos de conexão	Telnet SSH

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`

Tabela 4. Requisitos de integração para o adaptador BIG-IP (continuação)

Requisito de integração	Descrição

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 4. Requisitos de integração para o adaptador 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`

Tabela 4. Requisitos de integração para o adaptador BIG-IP (continuação)

Requisito de integração	Descrição

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`

Check Point SecurePlatform Appliances

IBM Security QRadar Risk Manager suporta o adaptador Check Point SecurePlatform Appliances.

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

Tabela 5. Requisitos de integração para o adaptador do Check Point SecurePlatform Appliances

Requisito de integração	Descrição
Versões	Versões R65 e posteriores **Restrição:** Os dispositivos Nokia IPSO não são suportados para backup.
Suporte de dados vizinhos	Não Suportado
Descoberta SNMP	Corresponde NGX em SNMP sysDescr.

Tabela 5. Requisitos de integração para o adaptador do Check Point SecurePlatform Appliances (continuação)

Requisito de integração	Descrição
Parâmetros de credenciais obrigatórios	Nome de usuário Senha Ativar Senha (modo especializado)
Protocolos de conexão	Telnet SSH
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

É possível utilizar o adaptador do Check Point Security Management Server (CPSMS) para descobrir e fazer backup dos nós de extremidade gerenciados pelo CPSMS. Esses nós de extremidade são utilizados para executar o CheckPoint FireWall-1 e a família de produtos VPN-1.

O adaptador CPSMS é baseado na biblioteca CPMI OPSEC SDK da API.

Avançar compatibilidade para conexões CPMI

Conexões CPMI são compatíveis com versões mais recentes. Por exemplo, um aplicativo CPMI que utiliza um NG FP3 OPSEC SDK pode se comunicar com VPN-1 NGX R60.

Compatibilidade com versões anteriores para conexões CPMI

Conexões CPMI não são compatíveis com uma versão anterior. Por exemplo, um aplicativo CPMI que utiliza OPSEC SDK 6.0 não pode se comunicar com nenhuma versão do VPN-1 antes de NGX R60.

Requisitos de configuração para CPSMS

Dois requisitos de configuração devem estar disponíveis para o CPSMS. Esses requisitos estão disponíveis, por padrão, quando o CPSMS é instalado. Entretanto, deve-se garantir que esses requisitos sejam retidos.

O aplicativo cliente CPSMS, cpsms_client, está no adaptador CPSMS. O aplicativo cpsms_client estabelece um método de autenticação assimétrica através de um canal Secure Internal Communication (SIC) com CPSMS. O método assimétrico também é conhecido como o método OPSEC_SSLCA.

O método de autenticação assimétrica é convertido em requisitos de configuração. Deve-se configurar e ativar o Secure Interno de Comunicação (SIC) no servidor de gerenciamento do firewall para permitir que o aplicativo cpsms_client se comunique com o CPSMS.

As portas a seguir 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, auth_port cpmi_server 18190.

Para permitir que o cpsms_client se comunique com o Servidor de Gerenciamento do Ponto de Verificação, o `$CPDIR/conf/sic_policy.conf` na CPSMS deve utilizar a seguinte linha, no mínimo:

```
# OPSEC applications default
ANY ; SAM_clients ; ANY ; sam ; sslca, local, sslca_comp
# sam proxy
ANY ; Modules, DN_Mgmt ; ANY; sam ; sslca
ANY ; ELA_clients ; ANY ; ela ; sslca, local, sslca_comp
ANY ; LEA_clients ; ANY ; lea ; sslca, local, sslca_comp
ANY ; CPMI_clients; ANY ; cpmi ; sslca, local, sslca_comp
```

Cisco CatOS

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

O adaptador do Cisco CatOS coleta as configurações do dispositivo fazendo backup dos dispositivos de rede CatOS que são visualizáveis por QRadar Risk Manager.

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

Tabela 6. Requisitos de Integração para aCisco CatOS do adaptador

Requisito de integração	Descrição
Versões	Dispositivos de chassi da série Catalyst 6500. **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.
Suporte de dados vizinhos	Suportado
Descoberta SNMP	Corresponde CATOS ou Catalyst Operating System no sysDescr SNMP.

Parâmetros de credenciais obrigatórios	`Nome de usuário`
	
	`Senha`
	
	`Ativar Senha`

Protocolos de conexão	Telnet SSH

Tabela 6. 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.

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

Tabela 7. Requisitos de integração para Cisco IOS

Requisito de integração	Descrição
Versões	10.1 e posterior 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.
Suporte de dados vizinhos	Suportado
Descoberta SNMP	Corresponde ISO ou Sistema operacional de internet Cisco no SNMP sysDescr.

Parâmetros de credenciais obrigatórios	`Nome de usuário`
	
	`Senha`
	
	`Ativar Senha`

Protocolos de conexão	Telnet SSH + SCP TFTP

Tabela 7. Requisitos de integração para 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 eigrp neighbors`
	`show diagbus`
	`show diag`
	`show install running`
	`show interfaces`
	`show inventory`
	`show file systems`
	`show mac-address-table dynamic`
	`show module`
	`show mod version`
	`show power`
	`show startup-config`
	`show object-group`
	`show running-config`
	`show snmp`
	`show glbp`
	`show spanning-tree`
	`show standby`
	`set terminal length`
	`show vlan`
	`show vtp status`
	`show version`
	`show vrrp`

Tabela 7. Requisitos de integração para 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 neighbor`
	`show ip protocols`
	`show ipv6 neighbors`
	`show ip ospf interface`
	`show ip route eigrp`

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.

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

Tabela 8. Requisitos de Integração para o adaptador do Cisco Nexus

Requisito de integração	Descrição
Versões	Sem restrições de versão
Suporte de dados vizinhos	Suportado
Descoberta SNMP	Corresponde *Cisco NX-OS* e uma cadeia de qualificação opcional que termina com *Software* no sysDescr SNMP. **Exemplo::** *(Cisco NX\-OS.* Software)*

Parâmetros de credenciais obrigatórios	`Nome de usuário`
	`Senha`
	`Ativar Senha`
	Se você incluir contextos de dispositivo virtual (VDCs) como dispositivos individuais, certifique-se de que as credenciais necessárias possam executar as seguintes ações:
	• Acessar a conta que está ativada para o VDCs.
	• Usar os comandos necessários nesse contexto virtual.

Tabela 8. Requisitos de Integração para o adaptador do Cisco Nexus (continuação)

Requisito de integração	Descrição
Protocolos de conexão	Telnet SSH

Arquivos necessários de terceiros	`adapters-common-2013.03_05-515182.noarch.rpm`
	
	`perl-Net-CIDR-Set-0.11-1.noarch.rpm`
	
	`perl-XML-Twig-3.42-1.noarch.rpm`

Tabela 8. 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	`terminal length 0`
	
	`show version`
	
	`show hostname`
	
	`show vdc`
	
	`snow snmp`
	
	`show module`
	
	`dir` *fs*(*fs* is file systems on the device)
	
	`show interface brief`
	
	`show interface snmp-ifindex`
	
	`show interface` *if* (*if* is all of the interfaces from `show interface brief` with configuration sections)
	
	`show running-config`
	
	`show startup-config`
	
	`show static-route`
	
	`show ip access-lists`
	
	`show object-group`
	
	`show vlan`
	
	`show vtp status`
	
	`show hsrp`
	
	`show vrrp`
	
	`show vtp`
	
	`show glbp`
	
	`show ip arp`
	
	`show mac address-table`
	
	`show ip route`
	
	`show ipv6 route`
	
	`show ipv6 ndp`
	
	`show cdp entry all`
	
	`switchto` *vdc* (para todos os contextos de dispositivos virtuais suportados)

Métodos para incluir VDCs para dispositivos Cisco Nexus

Utilize Configuration Source Management 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 VDCs são incluídos como dispositivos individuais, então cada VDC é exibido como um dispositivo na topologia.

Se VDCs são incluídos como um subdispositivo, eles não são exibidos na topologia. Em vez disso, é possível visualizar o VDCs no Configuration Monitor.

Incluindo VDCs como subdispositivos de seu dispositivoCisco Nexus

Use o Configuration Source Manager para incluir VDCs como subdispositivos de seu dispositivo.Cisco Nexus

Procedimento

1. Utilize o Configuration Source Management 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 Configuration Source Manager para obter as informações de configuração para o seu dispositivo do Nexus

   Para obter informações sobre a configuração do dispositivo, consulte o *IBM Security QRadar Risk Manager User Guide*.
3. Ative os seguintes comandos para o usuário que está especificado nas credenciais:
   - `show vdc` (no contexto admin)
   - `switchto vdc` *x*, em que *x* são os VDCs suportados.

   No Configuration Monitor, 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*.

Incluindo VDCs como dispositivos individuais

Utilize o Configuration Source Management para incluir cada VDC como um dispositivo separado. Ao utilizar 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 Configuration Source Management 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 Configuration Source Management 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 2 permit command terminal
NexusDevice(config-role)# rule 2 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.

O adaptador Cisco Security Appliances coleta as configurações do dispositivo fazendo o backup dos dispositivos da família Cisco. A lista a seguir descreve exemplos dos firewalls Cisco que o adaptador suporta para o Cisco Security Appliances:

- Appliance Security Adaptive independente
- Firewall Service Module (FWSM)
- Um módulo em um chassi Catalyst
- Dispositivo Private Internet Exchange (PIX) Estabelecido.

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

Tabela 9. Requisitos de Integração para o adaptador do Cisco Security Appliances

Requisito de integração	Descrição
Versões	Adaptive Security Appliances (ASA) que usam um sistema operacional Private Internet Exchange (PIX-OS) Roteadores ou comutadores ASA que usam FWSM Roteadores do Cisco IOS 7600 series que usam FWSM. Utilize o adaptador ASA para fazer backup da configuração e do estado dos serviços de cartão do FWSM.
Suporte de dados vizinhos	Suportado
Descoberta SNMP	Corresponde o PIX ou Adaptive Security Appliance ou Firewall Service Module em SNMP sysDescr.

Parâmetros de credenciais obrigatórios	`Nome de usuário`
	
	`Senha`
	
	`Ativar Senha`

Tabela 9. Requisitos de Integração para o adaptador do Cisco Security Appliances (continuação)

Requisito de integração	**Descrição**
Protocolos de conexão	Telnet SSH + SCP

Comandos que o adaptador requer para efetuar login e coletar dados	`change context`
	
	`change context admin-context`
	
	`change context context`
	
	`change system`
	
	`get startup-config`
	
	`show arp`
	
	`show context`
	
	`show interface`

Tabela 9. Requisitos de Integração para o adaptador do Cisco Security Appliances (continuação)

Requisito de integração	Descrição

Comandos que o adaptador requer para efetuar login e coletar dados (continuação)	`show interface detail`
	`show ipv6 interface`
	`show ipv6 neighbor`
	`show mac-address-table`
	`show names`
	`show ospf neighbor`
	`show pager`
	`show route`
	`show running-config`
	`show shun`
	`show version`
	`terminal pager 0`
	`terminal pager 24`
	Where:
	O comando `show pager` deve ser ativado para acessar as contas que usam o QRadar Risk Manager.
	O comando `context` *`context`* de mudança é usado para cada contexto no dispositivo ASA.
	O comando `change system` detecta se o sistema tiver várias configurações de contexto e determina o contexto-admin.
	O comando `change context` é obrigatório se o comando `change system` possui uma configuração de vários contextos ou um contexto configuração admin.
	Os comandos `terminal pager` são utilizados para configurar e reconfigurar o comportamento de paginação.

Fortinet FortiOS

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

O adaptador Fortinet FortiOS interage com o FortiOS através de Telnet ou SSH.

- Endereços baseados em geografia e políticas referenciadas não são suportados pelo QRadar Risk Manager.
- Políticas baseadas em identidade, VPN e 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. Atualmente, apenas as políticas de firewall da Camada 3 são suportadas.

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

Requisito de Integração	**Descrição**
Versão	4.0 MR3
Suporte de dados vizinhos	Não
Descoberta SNMP	Não
Parâmetros de credenciais obrigatórios	Nome de Usuário Senha
Protocolos de conexão	Telnet SSH

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 que tenha acesso de leitura/gravação à 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`
	
	`show full-configuration`
	
	`get router info routing-table static`
	
	`show firewall address`
	
	`get test dnsproxy 6`
	
	`show firewall addrgrp`
	
	`get firewall service predefined <variable>`
	
	`show firewall service custom`
	
	`show firewall service group`
	
	`get system snmp sysinfo`
	
	`show system snmp community`
	
	`show firewall policy`
	
	`show system zone`
	
	`show firewall vip`
	
	`show firewall vipgrp`
	
	`show firewall ippool`
	
	`show firewall central-nat`

ProVision HP Networking

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

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

Tabela 10. Requisitos de integração para o adaptador do ProVision HP Networking

Requisito de integração	**Descrição**
Versões	Comutadores ProVision HP Networking K/KA.11.XX e posterior. **Restrição:** Comutadores HP que estão em um sistema operacional Comware não são suportados por este adaptador.
Suporte de dados vizinhos	Suportado
Descoberta SNMP	Corresponde a números de versão com o formato `HP(.*)Switch(.*)(revisão [A-Z]{1,2}\.(\d+)\.(\d+))` em sysDescr.

Parâmetros de credenciais obrigatórios	`Nome de usuário`
	
	`Senha`
	
	`Ativar Senha`

Protocolos de conexão	SSH

Tabela 10. 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 árvore de amplitude configurada no dispositivo show spanning-tree mst-config show system information show version show vlans show vlans <id> Para cada vlan. show vrrp walkmib

Tabela 10. 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.

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

Tabela 11. Requisitos de integração para o adaptador do Juniper Networks JUNOS

Requisito de integração	Descrição
Versões	Versões 9 e posterior.
Suporte de dados vizinhos	Suportado
Descoberta SNMP	Corresponde ao sysOID SNMP: 1.3.6.1.4.1.2636

Tabela 11. Requisitos de integração para o adaptador do Juniper Networks JUNOS (continuação)

Requisito de integração	Descrição
Parâmetros de credenciais obrigatórios	Nome de usuário Senha
Protocolos de conexão	Telnet SSH + SCP
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 show bgp neighbor show ipv6 neighbors

Juniper Networks NSM

O adaptador IBM Security QRadar Risk Manager suporta o Juniper Networks NSM.

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 contém a configuração e informações sobre o dispositivo para roteadores e comutadores Juniper Networks que são gerenciados pelo console Juniper Networks NSM.

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

Tabela 12. Ambientes suportados pelo adaptador QRadar Risk Manager para o Juniper Networks NSM

Ambiente suportado	**Descrição**
Versões	Aplicativos IDP que são gerenciados pelo NSM
Suporte de dados vizinhos	Não Suportado
Descoberta SNMP	Não Suportado
Parâmetros de credenciais obrigatórios	• `Nome de usuário` • `Senha`
Protocolos de conexão	• 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.

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

Tabela 13. Requisitos de integração para o adaptador do Juniper Networks ScreenOS

Requisito de integração	**Descrição**
Versões	Os firewalls que utilizam um sistema operacional ScreenOS
Suporte de dados vizinhos	Suportado
Descoberta SNMP	Corresponde netscreen ou SSG em sysDescr SNMP.
Parâmetros de credenciais obrigatórios	`Nome de usuário` `Senha`
Protocolos de conexão	Telnet SSH

Tabela 13. Requisitos de integração para o adaptador do Juniper Networks ScreenOS (continuação)

Requisito de integração	Descrição

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`*
	Where:
	zone são os dados da zona retornada a partir 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 utiliza a interface de programação de aplicativo (API) do Rest baseado em XML do PAN-OS para se comunicar com os dispositivos.

Use uma solicitação HTTPS para uma URL enviar um comando para um dispositivo. O formato de comando para a solicitação é `https://deviceIPAddress/api/?type=op&cmd=<command>`

Em que *command* é um conjunto de tags XML ou XPath.

O exemplo a seguir é para um conjunto de tags XML.

```
<show><system><info></info></system></show>
```

O exemplo a seguir é um XPath:

```
/config/predefined/service
```

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

Tabela 14. Requisitos de integração para o adaptador Palo Alto

Requisito de integração	**Descrição**
Versões	PAN-OS versão 4.1.0 e posterior.
Suporte de dados vizinhos	Suportado
Descoberta SNMP	SysDescr corresponde a 'Palo Alto Networks(.*)série firewall' ou sysOid corresponde a 'panPA'

Parâmetros de credenciais obrigatórios	`Nome de usuário`
	
	`Senha`
	
	Utilize o acesso SuperReader para as credenciais.

Protocolos de conexão	HTTPS

Os comandos que são utilizados para a operação de backup	`<show><system><info></info></system></show>`
	
	`<show><config><running></running></config></show>`
	
	`<show><routing><route></route></routing></show>`
	
	`<show><virtual-wire>all</virtual-wire></show>`
	
	`<show><vlan>all</vlan></show>`
	
	`<show><interface>all</interface></show>`
	
	`<show><system><disk-space></disk-space></system></show>`
	
	`<show><system><resources></resources></system></show>`
	
	`/config/predefined/service`

Tabela 14. Requisitos de integração para o adaptador Palo Alto (continuação)

Requisito de integração	Descrição

Os comandos que são utilizados para dados de telemetria e vizinhos	`<show><system><info></info></system></show>`
	
	`<show><interface>all</interface></show>`
	
	`<show><routing><interface></interface></routing></show>`
	
	`<show><counter><interface>all</interface></counter></show>`
	
	`<show><arp>all</arp></show></p><p><show><mac>all</mac></show>`
	
	`<show><routing><route></route></routing></show>`

Os comandos que são utilizados para GetApplication	`<show><config><running></running></config></show>`
	
	`/config/predefined/application`

Sensor Sourcefire 3D

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 Sensor Sourcefire 3D.

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

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.

Tabela 15. Requisitos de integração para o adaptador do Sensor Sourcefire 3D

Requisito de integração	Descrição
Versões	5.2
Suporte de dados vizinhos	Não
Descoberta SNMP	Não

Parâmetros de credenciais obrigatórios	`Nome de usuário`
	
	`Senha`

Protocolos de conexão	SSH

Tabela 15. Requisitos de integração para o adaptador do Sensor Sourcefire 3D (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`

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

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local:

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.

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 contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira 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
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-24

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.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

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.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

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 estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca comercial da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca comercial (® ou ™), estes símbolos indicarão marcas comerciais dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atual de marcas comerciais da IBM está disponível na web em Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Os termos a seguir são marcas comerciais ou marcas registradas de outras empresas:

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

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

Considerações sobre a política de privacidade

Produtos de software IBM, incluindo software como soluções de serviço (“Ofertas de software”), podem usar cookies ou outras tecnologias para coletar informações de uso do produto, para ajudar a melhorar a experiência do usuário final, customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação de identificação pessoal é coletada pelas Ofertas de software. Algumas de nossas Ofertas de software podem ajudá-lo a coletar informações de identificação pessoal. Se esta Oferta de software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

Dependendo das configurações implementadas, esta Oferta de software pode usar cookies de sessão que coletam o ID de sessão de cada usuário para propósitos de gerenciamento e autenticação de sessões. Esses cookies podem ser desativados, mas sua desativação também eliminará a funcionalidade ativada.

Se as configurações implementadas para esta Oferta de software fornecerem a você como cliente a capacidade de coletar informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, você deverá consultar seu próprio conselho jurídico sobre as leis aplicáveis a essa coleta de dados, incluindo requisitos para 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 “Declaração de privacidade de software como serviço e produtos de software IBM” em http://www.ibm.com/software/info/product-privacy.

Índice Remissivo