IBM Security QRadar
Versão 7.2.5

Guia de Instalação do FIPS 140-2

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 31.

Informações do produto

Este documento aplica-se ao IBM QRadar Security Intelligence Platform V7.2.5 e às liberações subsequentes, a não ser que seja substituído por uma versão atualizada.

Índice

Introdução às instalações do FIPS do QRadar

O Guia de Instalação do FIPS do IBM® Security QRadar fornece informações sobre a instalação e ativação do modo VERIFIED em sistemas QRadar.

Para obter informações sobre produtos de segurança do IBM que são certificados pelo FIPS, consulte os documentos de Política de segurança do IBM Security FIPS 140. Localize esses documentos no website do National Institute of Standards and Technology (NIST), na seção Module Validation Lists: NIST (http://csrc.nist.gov/groups/STM/cmvp/index.html).

Para instalar ou recuperar um sistema de alta disponibilidade (HA), consulte o *IBM Security QRadar High Availability Guide*.

Público-alvo

Esse guia é destinado a usuários ou administradores de operações criptográficas que são responsáveis por instalar, manter e configurar sistemas QRadar ativados para FIPS. Ao ativar o modo VERIFIED, você cria uma função de usuário administrador para serviços gerais de segurança e uma função de usuário criptográfico para operações criptográficas.

Documentação técnica

Para localizar a documentação do produto do 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 Acessando o 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 contatar o suporte ao cliente, consulte o 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 proteger sistemas e informações por meio de prevenção, detecção e resposta ao acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em informações que são alteradas, destruídas, desapropriadas ou usadas indevidamente ou pode resultar em dano ou uso indevido dos sistemas, inclusive para uso em ataques a outros. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum único produto, serviço ou medida de segurança pode ser completamente efetivo na prevenção de uso ou acesso incorreto. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança legal abrangente, que envolverá necessariamente procedimentos operacionais adicionais e poderá requerer que outros sistemas, produtos ou serviços sejam mais efetivos. A IBM

NÃO GARANTE QUE QUAISQUER SISTEMAS, PRODUTOS OU SERVIÇOS SÃO IMUNES, OU DEIXARÃO SUA EMPRESA IMUNE, DE CONDUTAS ILEGAIS OU MALICIOSAS DE QUALQUER PARTE.

Observação:

O uso deste Programa pode envolver diversas leis ou regulamentos, Incluindo aqueles relacionados a privacidade, proteção de dados, empregabilidade, e comunicações eletrônicas e armazenamento. O IBM Security QRadar pode ser usado somente para propósitos legais e de forma legal. O cliente concorda em usar este programa conforme as leis aplicáveis, regulamentos e políticas e assume todas as responsabilidades para obedecê-las. O licenciado declara que irá obter ou obteve quaisquer consentimentos, permissões ou licenças necessárias para habilitar o uso legal do IBM Security QRadar.

Capítulo 1. Visão Geral de Implementação do QRadar

É possível instalar o IBM Security QRadar em um único servidor para pequenas empresas ou em vários servidores para ambientes corporativos grandes.

Visão geral do FIPS

O IBM Security QRadar usa os provedores de criptografia aprovados pelo FIPS 140-2 para criptografia. O Cryptographic Security Kernel aprovado é Q1 Labs, Q1 Labs, uma empresa IBM ou IBM Corp.

Os certificados estão listados no: *website do NIST* (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm).

Siga essas diretrizes para seu dispositivo FIPS do QRadar:

- Use firmware certificado pelo FIPS.
- Deve-se ativar o modo VERIFIED após a instalação e configuração iniciais do dispositivo.
- Deve-se ativar o modo VERIFIED em qualquer dispositivo restaurado para as configurações padrão de fábrica (desconfigurado).

Versão do software QRadar para conformidade com o FIPS

Deve-se instalar uma versão do IBM Security QRadar em conformidade com o FIPS. Para 7.2.5, esta versão é 7.2.5.20160829181208

Faça o download do QRadar ISO a partir do IBM Fix Central.

Restrições do dispositivo

Algumas restrições se aplicam a dispositivos FIPS do IBM Security QRadar.

Essas restrições se aplicam ao dispositivo FIPS do QRadar:

- Não é possível usar o SSH usando a conta do usuário raiz para efetuar login em um dispositivo que tem o modo VERIFIED ativado. Somente a conta do usuário crypto ou contas do usuário admin podem usar SSH para efetuar login em um dispositivo QRadar ativado para FIPS.
- Não é possível instalar esse dispositivo como uma máquina virtual (VM)
- Não é possível instalar correções de software em dispositivos QRadar, a menos que a atualização seja certificada pelo FIPS.
- Não é possível desativar o modo VERIFIED no QRadar usando seu navegador. A conta do usuário criptográfico é a única função que tem permissões para desativar o modo VERIFIED.
- Não selecione MD5 ou DES quando configurar respostas de SNMP, porque essas opções não são compatíveis com o FIPS. Se essas opções forem escolhidas quando o dispositivo estiver no modo VERIFIED, o dispositivo não executará a resposta. Uma mensagem de erro que indica que a resposta é inválida é criada no log do sistema.
- A Alta disponibilidade (HA) não é suportada em dispositivos FIPS.

Chaves de Ativação e Chaves de Licença

Ao instalar dispositivos do IBM Security QRadar, você deve digitar uma chave de ativação. Depois de instalar, você deve aplicar suas chaves de licença. Para evitar digitar a chave errada no processo de instalação, é importante entender a diferença entre as chaves.

Chave de Ativação

A chave de ativação é uma sequência alfanumérica de 24 dígitos, com 4 partes, que você recebe da IBM. Todas as instalações dos produtos QRadar utilizam o mesmo software. No entanto, a chave de ativação especifica quais módulos de software aplicar para cada tipo de dispositivo. Por exemplo, utilize a chave de ativação do IBM Security QRadar QFlow Collector para instalar apenas os módulos do QRadar QFlow Collector.

É possível obter a chave de ativação a partir dos locais a seguir:

- Se você tiver comprado um dispositivo que venha com o software QRadar pré-instalado, a chave de ativação estará incluída em um documento no CD anexado.
- Se você adquiriu o software QRadar ou o download do dispositivo virtual, uma lista de chaves de ativação será incluída no documento de *Introdução*. A *Introdução* é anexada ao e-mail de confirmação.

Chave de licença

O sistema inclui uma chave de licença temporária que fornece a você acesso ao software QRadar por cinco semanas. Depois de instalar o software e antes da chave de licença padrão expirar, você deverá incluir suas licenças adquiridas.

A tabela a seguir descreve as restrições para a chave de licença padrão:

Tabela 1. Restrições para a Chave de Licença Padrão para Instalações do QRadar SIEM

Uso	**Limite**
Limite de origem de log ativo	750
Limite de eventos por segundo	5000
Fluxos por intervalo	200000
Limite de usuários	10
Limite de objeto de rede	300

Tabela 2. Restrições para a Chave de Licença Padrão para Instalações do QRadar Log Manager

Uso	**Limite**
Limite de origem de log ativo	750
Limite de eventos por segundo	5000
Limite de usuários	10
Limite de objeto de rede	300

Quando você adquire um produto QRadar, um e-mail que contém a chave de licença permanente é enviado a partir da IBM. Essas chaves de licença estendem os recursos de seu tipo de dispositivo e definem parâmetros operacionais do sistema. Você deve aplicar as chaves de licença antes da expiração de sua licença padrão.

Tarefas relacionadas:

Capítulo 2, “Instalando um QRadar Console ou Host Gerenciado”, na página 15
Instale o Console IBM Security QRadar ou um host gerenciado no dispositivo QRadar ou em seu próprio dispositivo.

Módulo de Gerenciamento Integrado

Utilize o Módulo de Gerenciamento Integrado, que está no painel traseiro de cada tipo de dispositivo, para gerenciar os conectores seriais e Ethernet.

É possível configurar o Módulo de Gerenciamento Integrado para compartilhar uma porta Ethernet com a interface de gerenciamento do produto IBM Security QRadar. No entanto, para reduzir o risco de perder a conexão quando o dispositivo é reiniciado, configure Módulo de Gerenciamento Integrado no modo dedicado.

Para configurar o Módulo de Gerenciamento Integrado, você deve acessar as configurações do BIOS do sistema pressionando F1 quando a tela inicial da IBM é exibida. Para obter mais informações sobre a configuração do Módulo de Gerenciamento Integrado, consulte *Integrated Management Module User's Guide* no CD que é fornecido com o dispositivo.

Conceitos relacionados:

“Acessórios de Hardware e Software de Desktop de Pré-requisito para Instalações do QRadar” na página 4
Antes de instalar os produtos IBM Security QRadar, assegure-se de ter acesso aos acessórios de hardware e ao software de desktop necessários.

Componentes do QRadar

IBM Security QRadar consolida os dados do evento a partir de origens de log que são utilizadas pelos dispositivos e aplicativos em sua rede.

Importante: Versões de software para todos os dispositivos IBM Security QRadar em uma implementação devem ser a mesma versão e nível de correção. Implementações que utilizam versões diferentes do software não são suportadas.

As implementações do QRadar podem incluir os seguintes componentes:

QRadar QFlow Collector
Coleta passivamente fluxos de tráfego da rede por meio de portas de período ou grampos de rede. O IBM Security QRadar QFlow Collector também suporta a coleção de fontes de dados baseadas em fluxo externo, como NetFlow.

É possível instalar um QRadar QFlow Collector em seu próprio hardware ou utilizar um dos dispositivos QRadar QFlow Collector.

Restrição: O componente está disponível somente para implementações do QRadar SIEM.

QRadar Console
Fornece a interface com o usuário do produto QRadar. A interface fornece eventos em tempo real e visualizações do fluxo, relatórios, ofensas, informações de ativos e funções administrativas.

Em implementações distribuídas do QRadar, utilize o QRadar Console para gerenciar hosts que incluem outros componentes.

Magistrate
Um serviço em execução no QRadar Console, o Magistrate fornece os componentes de processamento centrais. É possível incluir um componente do Magistrate para cada implementação. O Magistrate fornece visualizações, relatórios, alertas e análise de tráfego de rede e eventos de segurança.

O componente do Magistrate processa eventos com relação às regras customizadas. Se um evento corresponder a uma regra, o componente do Magistrate gerará a resposta que está configurada na regra customizada.

Por exemplo, a regra customizada pode indicar que quando um evento corresponde à regra, uma ofensa é criada. Se não houver correspondência para uma regra customizada, o componente do Magistrate utiliza as regras padrão para processar o evento. Uma ofensa é um alerta processado usando diversas entradas, eventos individuais e eventos que são combinados com o comportamento analisado e vulnerabilidades. O componente do Magistrate prioriza as ofensas e designa um valor de magnitude, que é baseado em diversos fatores, incluindo o número de eventos, a gravidade, relevância e credibilidade.

QRadar Coletor de Eventos
Reúne eventos de origens de log locais e remotas. Normaliza eventos da origem do log brutos. Durante esse processo, o componente do Magistrate examina o evento a partir da origem de log e mapeia o evento para um QRadar Identifier (QID). Em seguida, o Coletor de Eventos empacota eventos idênticos para conservar o uso do sistema e envia as informações para o Processador de Eventos.

QRadar Processador de Eventos
Processa eventos que são coletados a partir de um ou mais componentes do Coletor de Eventos. O Processador de Eventos correlaciona as informações de produtos QRadar e distribui as informações para a área apropriada, dependendo do tipo de evento.

O Processador de Eventos também inclui informações que são reunidas pelos produtos QRadar para indicar alterações comportamentais ou violações de política para o evento. Ao concluir, o Processador de Eventos envia os eventos para o componente do Magistrate.

Para obter mais informações sobre cada componente, consulte *Guia de Administração*.

Acessórios de Hardware e Software de Desktop de Pré-requisito para Instalações do QRadar

Antes de instalar os produtos IBM Security QRadar, assegure-se de ter acesso aos acessórios de hardware e ao software de desktop necessários.

Acessórios de Hardware

Assegure-se de ter acesso aos componentes de hardware a seguir:

- Monitor e teclado ou console serial
- Uninterrupted Power Supply (UPS) para todos os sistemas que armazenam dados, como o QRadar Console, componentes do Processador de Eventos ou componentes do QRadar QFlow Collector
- Cabo de modem nulo, se desejar conectar o sistema a um console serial

Importante: Os produtos QRadar suportam implementações Redundant Array of Independent Disks (RAID) baseadas em hardware, mas não suportam instalações RAID baseadas em software.

Requisitos de Software de Desktop

Assegure-se de que os aplicativos a seguir estejam instalados em todos os sistemas de desktop usados para acessar a interface com o usuário do produto QRadar:

- Java™ Runtime Environment (JRE) versão 1.7 ou IBM 64-bit Runtime Environment for Java V7.0
- Adobe Flash versão 10.x

Tarefas relacionadas:

Capítulo 2, "Instalando um QRadar Console ou Host Gerenciado", na página 15
Instale o Console IBM Security QRadar ou um host gerenciado no dispositivo QRadar ou em seu próprio dispositivo.

Instalando os rótulos tamper-proof para segurança física

Os rótulos Tamper-proof são necessários para a segurança física do FIPS e devem ser instalados antes da colocação do dispositivo no rack de servidor.

Sobre Esta Tarefa

Se seu dispositivo não incluiu rótulos para segurança física do FIPS ou não continha um número suficiente de rótulos, é necessário entrar em contato com o representante de vendas para receber rótulos adicionais.

Quarenta rótulos tamper-proof estão incluídos com seu dispositivo FIPS do IBM Security QRadar. Esses rótulos são numerados com um código de 7 dígitos para seu dispositivo.

Importante: Assegure-se de que o local esteja livre de poeira ou resíduos antes de instalar um rótulo tamper-proof.

Procedimento

1. Instale 12 rótulos tamper nos botões de ejeção do lado esquerdo da transportadora de disco rígido. Três rótulos tamper são necessários para proteger cada banco de 3 discos rígidos. Não cubra aberturas perfuradas na transportadora do disco rígido e no chassi do servidor com os rótulos tamper.

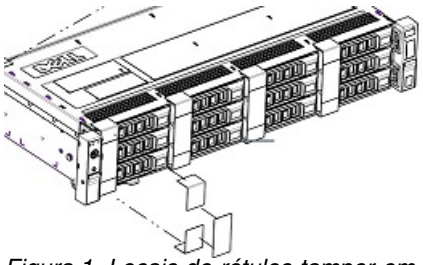

Figura 1. Locais de rótulos tamper em discos rígidos

2. Instale dois rótulos tamper nos cantos superior direito e esquerdo do servidor na superfície superior, próximo da frente do servidor. Assegure-se de que o rótulo ligue o vão entre o painel frontal e a superfície superior do chassi do servidor.

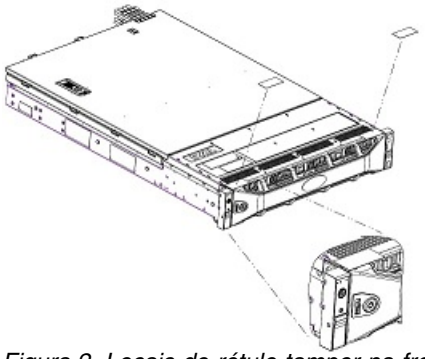

Figura 2. Locais do rótulo tamper na frente do dispositivo

3. Para instalar os rótulos tamper necessários na parte superior do dispositivo, conclua as etapas a seguir:
   a. Instale um rótulo tamper no lado direito e esquerdo do dispositivo, ligando o vão entre o chassi do servidor e a tampa superior removível. Assegure-se de que o rótulo ligue o vão nas superfícies laterais e cubra a superfície superior do servidor.
   b. Instale um rótulo tamper no lado direito e esquerdo do dispositivo na traseira do servidor. Assegure-se de que o rótulo ligue o vão entre o chassi do servidor e a tampa de acesso superior removível.

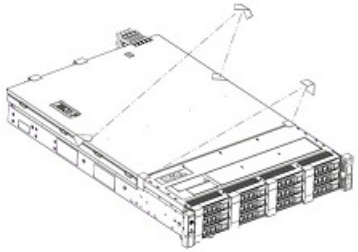

Figura 3. Locais de rótulo tamper na parte superior do dispositivo

4. Para instalar os rótulos tamper necessários na parte posterior do dispositivo, conclua as etapas a seguir:
   a. Instale dois rótulos tamper para cobrir os vãos entre o chassi do servidor, a fonte de alimentação removível e os recursos de tampa de preenchimento.
   b. Instale dois rótulos tamper sobre as hachuras de liberação da placa PCIE.

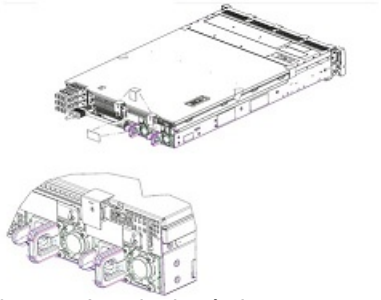

Figura 4. Locais de rótulo tamper na traseira do dispositivo

Navegadores da web suportados

Para que os recursos em produtos IBM Security QRadar funcionem corretamente, deve-se usar um navegador da web suportado.

Ao acessar o sistema QRadar, um nome de usuário e uma senha são solicitados. O nome de usuário e a senha devem ser configurados com antecedência pelo administrador.

A tabela a seguir lista as versões suportadas dos navegadores da web.

Tabela 3. Navegadores da web suportados para produtos QRadar

Navegador da web	Versões suportadas
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer de 32 bits e 64 bits, com o modo de documento e o modo de navegador ativados	9.0 10.0
Google Chrome	A versão atual a partir da data de liberação da versão do IBM Security QRadar que tiver instalada.

Ativando o modo de documento e o modo de navegador no Internet Explorer

Se você usar o Microsoft Internet Explorer para acessar os produtos IBM Security QRadar, devem-se ativar o modo de navegador e o modo de documento.

Procedimento

1. Em seu navegador da web Internet Explorer, pressione F12 para abrir a janela Ferramentas de desenvolvedor.
2. Clique em **modo de navegador** e selecione a versão de seu navegador da web.
3. Clique em **Modo de documento**.
   - Para o Internet Explorer V9.0, selecione **Padrões do Internet Explorer 9**.
   - Para o Internet Explorer V10.0, selecione **Padrões do Internet Explorer 10**.

Conceitos relacionados:

"Acessórios de Hardware e Software de Desktop de Pré-requisito para Instalações do QRadar" na página 4
Antes de instalar os produtos IBM Security QRadar, assegure-se de ter acesso aos acessórios de hardware e ao software de desktop necessários.

Instalações da unidade flash USB

É possível instalar o software IBM Security QRadar com uma unidade flash USB.

As instalações de unidade flash USB são instalações de produto integral. Não é possível usar uma unidade flash USB para fazer upgrade ou aplicar correções de produto. Para obter mais informações sobre a aplicação de fix packs, consulte as Notas sobre a liberação do fix pack.

Versões suportadas

Os seguintes dispositivos ou sistemas operacionais podem ser usados para criar uma unidade flash USB inicializável:

- Um dispositivo QRadar v7.2.1 ou posterior
- Um sistema Linux instalado com o Red Hat Enterprise Linux 6.5
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 2008
- Microsoft Windows 2008R2

Visão geral da instalação

Siga este procedimento para instalar o software QRadar a partir de uma unidade flash USB:

1. Crie uma unidade flash USB inicializável.
2. Instale o software no seu dispositivo QRadar.
3. Instale quaisquer liberações de manutenção de produto ou fix packs.

   Consulte as Notas sobre a liberação para instruções de instalação de fix packs e liberações de manutenção.

Criando uma unidade flash USB inicializável com um dispositivo QRadar

É possível usar um dispositivo IBM Security QRadar V7.2.1 ou posterior para criar uma unidade flash USB inicializável que possa ser usada para instalar o software QRadar.

Antes de Iniciar

Antes de criar uma unidade flash USB inicializável a partir de um dispositivo QRadar, deve-se ter acesso aos seguintes itens:

- Uma unidade flash USB de 2 GB
- Um arquivo de imagem ISO QRadar V7.2.1 ou posterior
- Um dispositivo QRadar físico

Se o seu dispositivo QRadar não tiver conectividade com a Internet, é possível fazer o download do arquivo de imagem ISO QRadar para um computador desktop ou outro dispositivo QRadar com acesso à Internet. Então é possível copiar o arquivo ISO para o dispositivo QRadar, no qual você instala o software.

Ao criar uma unidade flash USB inicializável, os conteúdos da unidade flash serão excluídos.

Procedimento

1. Faça o download do arquivo de imagem ISO do QRadar.
   a. Acesse o website de Suporte IBM (www.ibm.com/support).
   b. Localize o arquivo ISO IBM Security QRadar que corresponde à versão do dispositivo QRadar.
   c. Copie o arquivo de imagem ISO para um diretório `/tmp` no seu dispositivo QRadar.
2. Usando SSH, efetue login no seu sistema QRadar como usuário raiz.

3. Insira a unidade flash USB na porta USB no seu sistema QRadar.

   Pode levar até 30 segundos para o sistema reconhecer a unidade flash USB.
4. Digite o seguinte comando para montar a imagem ISO:

   ```
   mount -o loop /tmp/<nome da imagem ISO>.iso /media/cdrom
   ```
5. Digite o seguinte comando para copiar o script de criação USB do ISO montado para o diretório /tmp.

   ```
   cp /media/cdrom/post/create-usb-key.py /tmp/
   ```
6. Digite o seguinte comando para iniciar o script de criação de USB:

   ```
   /tmp/create-usb-key.py
   ```
7. Pressione Enter.
8. Pressione 1 e digite o caminho para o arquivo ISO. Por exemplo,

   ```
   /tmp/<nome da imagem iso>.iso
   ```
9. Pressione 2 e selecione a unidade que contém sua unidade flash USB.
10. Pressione 3 para criar sua chave USB.

    O processo de gravar a imagem ISO na sua unidade flash USB requer vários minutos para ser concluído. Quando o ISO for gravado na unidade flash USB, uma mensagem de confirmação será exibida.
11. Pressione q para sair do script da chave USB.
12. Remova a unidade flash USB do seu sistema QRadar.
13. Para liberar espaço, remova o arquivo de imagem ISO do sistema de arquivos /tmp.

O que Fazer Depois

Se a conexão ao dispositivo for serial, consulte Configurando uma unidade flash para dispositivos apenas seriais.

Se a conexão com o dispositivo for por teclado e mouse (VGA), consulte Instalando QRadar com uma unidade flash USB.

Criando uma unidade flash USB com Microsoft Windows

É possível usar um sistema de desktop ou notebook Microsoft Windows para criar uma unidade flash USB que possa ser usada para instalar o software QRadar.

Antes de Iniciar

Antes de criar uma unidade flash USB inicializável com um sistema Microsoft Windows, deve-se ter acesso aos seguintes itens:

- Uma unidade flash USB de 2 GB
- Um sistema de desktop ou notebook com os seguintes sistemas operacionais:
  - Windows 7
  - Windows Vista
  - Windows 2008
  - Windows 2008R2

Deve-se fazer o download dos seguintes arquivos do website de Suporte IBM (www.ibm.com/support).

- QRadar V7.2.1 ou posterior, arquivo de imagem ISO do Red Hat de 64 bits
- Ferramenta Create-USB-Install-Key (CUIK).

Deve-se fazer o download dos seguintes arquivos da Internet.

- PeaZip Portable 4.8.1
- SYSLINUX 4.06

Dica: Pesquise na web `Peazip Portable v4.8.1` e `Syslinux` para localizar os arquivos para download.

Ao criar uma unidade flash USB inicializável, os conteúdos da unidade flash serão excluídos.

Procedimento

1. Extraia a ferramenta Create-USB-Install-Key (CUIK) para o diretório `c:\cuik`.
2. Copie os arquivos `.zip` para PeaZip Portable 4.8.1 e SYSLINUX 4.06 para a pasta `cuik\deps`.

   Por exemplo, `c:\cuik\deps\peazip_portable-4.8.1.WINDOWS.zip` e `c:\cuik\deps\syslinux-4.06.zip`.

   Não é preciso extrair os arquivos `.zip`. Os arquivos somente precisam estar disponíveis no diretório `cuik/deps`.
3. Insira a unidade flash USB na porta USB no seu computador.
4. Verifique se a unidade flash USB está listada por letra da unidade e acessível no Microsoft Windows.
5. Clique com o botão direito em `c:\cuik\cuik.exe`, selecione **Executar como administrador** e pressione **Enter**.
6. Pressione `1`, selecione o arquivo QRadar ISO e clique em **Abrir**.
7. Pressione `2` e selecione o número que corresponde à letra da unidade designada à sua unidade flash USB.
8. Pressione `3` para criar a unidade flash USB.
9. Pressione **Enter** para confirmar que você está ciente de que os conteúdos da unidade flash USB serão excluídos.
10. Digite `create` para criar uma unidade flash USB inicializável a partir da imagem ISO. Este processo pode levar vários minutos.
11. Pressione **Enter** e digite `q` para sair da ferramenta Create_USB_Install_Key.
12. Ejete com segurança a unidade flash USB do seu computador.

O que Fazer Depois

Se a conexão ao dispositivo for serial, consulte Configurando uma unidade flash para dispositivos apenas seriais.

Se a conexão com o dispositivo for por teclado e mouse (VGA), consulte Instalando QRadar com uma unidade flash USB.

Criando uma unidade flash USB inicializável com Red Hat Linux

É possível usar um sistema de desktop ou notebook Linux com Red Hat v6.3 para criar uma unidade flash USB inicializável que possa ser usada para instalar o software IBM Security QRadar.

Antes de Iniciar

Antes de criar uma unidade flash USB inicializável com um sistema Linux, deve-se ter acesso aos seguintes itens:

- Uma unidade flash USB de 2 GB
- Um arquivo de imagem ISO QRadar V7.2.1 ou posterior
- Um sistema Linux que tenha os seguintes softwares instalados:
  - Red Hat 6.5
  - Python 6.2 ou posterior

Ao criar uma unidade flash USB inicializável, os conteúdos da unidade flash serão excluídos.

Procedimento

1. Faça o download do arquivo de imagem ISO do QRadar.
   a. Acesse o website de Suporte IBM (www.ibm.com/support).
   b. Localize o arquivo ISO IBM Security QRadar.
   c. Copie o arquivo de imagem ISO para um diretório `/tmp` no seu dispositivo QRadar.
2. Atualize seu sistema baseado em Linux para incluir esses pacotes.
   - syslinux
   - mtools
   - dosfstools
   - parted

   Para informações sobre o gerenciador de pacote específico para seu sistema Linux, consulte a documentação do fornecedor.
3. Efetue login no sistema QRadar como usuário raiz.
4. Insira a unidade flash USB na porta USB dianteira no seu sistema.

   Pode levar até 30 segundos para o sistema reconhecer a unidade flash USB.
5. Digite o seguinte comando para montar a imagem ISO:

   ```
   mount -o loop /tmp/<nome da imagem ISO>.iso /media/cdrom
   ```
6. Digite o seguinte comando para copiar o script de criação USB do ISO montado para o diretório `/tmp`.

   ```
   cp /media/cdrom/post/create-usb-key.py /tmp/
   ```
7. Digite o seguinte comando para iniciar o script de criação de USB:

   ```
   /tmp/create-usb-key.py
   ```
8. Pressione `Enter`.
9. Pressione 1 e digite o caminho para o arquivo ISO. Por exemplo,

   ```
   /tmp/Rhe664QRadar7_2_4_<build>.iso
   ```
10. Pressione 2 e selecione a unidade que contém sua unidade flash USB.
11. Pressione 3 para criar sua chave USB.

    O processo de gravar a imagem ISO na sua unidade flash USB requer vários minutos para ser concluído. Quando o ISO for gravado na unidade flash USB, uma mensagem de confirmação será exibida.
12. Pressione `q` para sair do script da chave USB.
13. Remova a unidade flash USB do seu sistema.

O que Fazer Depois

Se a conexão ao dispositivo for serial, consulte Configurando uma unidade flash para dispositivos apenas seriais.

Se a conexão com o dispositivo for por teclado e mouse (VGA), consulte Instalando QRadar com uma unidade flash USB.

Configurando uma unidade flash USB para dispositivos apenas seriais

Deve-se concluir uma etapa de configuração extra antes de poder usar a unidade flash USB inicializável para instalar o software QRadar em dispositivos apenas seriais.

Sobre Esta Tarefa

Esse procedimento não será necessário se você tiver um teclado e um mouse conectados ao dispositivo.

Procedimento

1. Insira a unidade flash USB inicializável na porta USB do dispositivo.
2. Na unidade flash USB, localize o arquivo `syslinux.cfg`.
3. Edite o arquivo de configuração syslinux para alterar a instalação padrão de `default linux` para `default serial`.
4. Salve as alterações no arquivo de configuração syslinux.

O que Fazer Depois

Agora você está pronto para instalar o QRadar com a unidade flash USB.

Instalando um QRadar com uma unidade flash USB

Siga este procedimento para instalar o QRadar a partir de uma unidade flash USB inicializável.

Antes de Iniciar

Deve-se criar uma unidade flash USB inicializável antes de poder usá-la para instalar o software QRadar.

Sobre Esta Tarefa

Este procedimento fornece orientação geral sobre como usar uma unidade flash USB inicializável para instalar o software QRadar.

O processo de instalação completo é documentado no Guia de Instalação do produto.

Procedimento

1. Instale todo o hardware necessário.
2. Selecione uma das opções a seguir:
   - Conecte um notebook à porta serial na parte de trás do dispositivo.
   - Conecte um teclado e monitor a suas respectivas portas.

3. Insira a unidade flash USB inicializável na porta USB do dispositivo.
4. Reinicie o dispositivo.

   A maioria dos dispositivos pode inicializar a partir de uma unidade flash USB por padrão. Se você estiver instalando um software QRadar no seu próprio hardware, pode precisar configurar a ordem de inicialização do dispositivo para priorizar USB.

   Depois da inicialização do dispositivo, a unidade flash USB preparará o dispositivo para instalação. Esse processo pode levar até uma hora para ser concluído.
5. Quando o menu **Red Hat Enterprise Linux** for exibido, selecione uma das seguintes opções:
   - Se você tiver conectado um teclado e um monitor, selecione **Instalar ou fazer upgrade usando o console VGA**.
   - Se você tiver conectado um notebook com uma conexão serial, selecione **Instalar ou atualizar usando o console Serial**.
6. Digite `SETUP` para iniciar a instalação.
7. Quando o aviso de login for exibido, digite `root` para efetuar login no sistema como usuário raiz.

   O nome de usuário faz distinção entre maiúsculas e minúsculas.
8. Pressione **Enter** e siga os avisos para instalar o QRadar.

   O processo de instalação completo é documentado no Guia de Instalação do produto.

Fazendo upgrade do dispositivo compatível com FIPS para o QRadar V7.2.5

Fazendo upgrade de um dispositivo compatível com FIPS a partir de uma liberação anterior do IBM Security QRadar para o QRadar V7.2.5 para ter os recursos mais recentes.

Antes de Iniciar

Faça download das correções de software a seguir a partir do Fix Central (http://www.ibm.com/support/fixcentral).

- `7.1.0-QRADAR-QRSIEM-495292`
- `7.1.0-QRADAR-QRSIEM-599086`
- `7.2.2-QRADAR-QRSIEM-891276`
- `7.2.4-QRADAR-QRSIEM-983526`
- `QRadar FIPS 7.2.5.20160829181208`
- `qradar-fips-upgrade-7.2.5-3.el6.x86_64.rpm`

Procedimento

1. Use o SSH para efetuar login no QRadar como um usuário criptografado.
2. Desative o modo FIPS em cada host usando o comando a seguir:

   ```
   disable_fips
   ```
3. Em cada host do QRadar, instale o RPM da atualização do FIPS usando o comando a seguir:

   ```
   rpm -ivh qradar-fips-upgrade-7.2.5-3.el6.x86_64.rpm
   ```
4. Após a instalação do RPM ser concluída, reinicie cada host.

5. No console do QRadar, aplique as correções de software a seguir na ordem listada, usando a opção `All` para atualizar todos os hosts.
   a. `7.1.0-QRADAR-QRSIEM-495292`
   b. `7.1.0-QRADAR-QRSIEM-599086`
   c. `7.2.2-QRADAR-QRSIEM-891276`
   d. `7.2.4-QRADAR-QRSIEM-983526`
6. Reinicie cada host do QRadar.
7. No console do QRadar, aplique a correção de software `7.2.5.20160829181208` e, em seguida, reinicie cada host.
8. Para concluir o upgrade, digite o comando a seguir em cada host:
   ```
   complete-fips-upgrade
   ```
9. Após o upgrade ser concluído, digite **Sim** no prompt e, em seguida, reinicie cada host.
10. Em cada host gerenciado, ative o modo VERIFIED inserindo o comando a seguir:
    ```
    /opt/qradar/fips/setup/fips_setup.py --enable
    ```

O que Fazer Depois

Desative as atualizações automáticas em seus dispositivos FIPS. Para obter informações adicionais, consulte "Desativando atualizações automáticas" na página 17.

Instalando uma versão anterior do software QRadar

Instale uma versão anterior do software IBM Security QRadar se sua implementação requer recursos que são oferecidos somente em uma versão anterior. Por exemplo, a versão do QRadar certificada por FIPS é sempre uma versão anterior à liberação mais recente.

Antes de Iniciar

Faça download do QRadar ISO necessário a partir de www.ibm.com/support/fixcentral (http://www-933.ibm.com/support/fixcentral).

Procedimento

1. Copie o ISO para uma unidade flash USB ou grave-o em um disco digital versátil (DVD).

   Importante: É possível instalar o QRadar em um sistema remoto, mas assegure-se de usar um protocolo que suporta o comando `FLATTEN`, tal como iDRAC. O SSH não suporta o comando `FLATTEN`.
2. Selecione a unidade flash USB ou o DVD como a opção de inicialização para o dispositivo no qual deseja instalar o QRadar.
3. Ligue o dispositivo.
4. Digite `FLATTEN` para instalar o software no ISO. Para obter informações adicionais, consulte Capítulo 2, "Instalando um QRadar Console ou Host Gerenciado", na página 15.

Capítulo 2. Instalando um QRadar Console ou Host Gerenciado

Instale o Console IBM Security QRadar ou um host gerenciado no dispositivo QRadar ou em seu próprio dispositivo.

Versões de software para todos os dispositivos IBM Security QRadar em uma implementação devem ser a mesma versão e nível de correção. Implementações que utilizam versões diferentes do software não são suportadas.

Antes de Iniciar

Assegure que os requisitos a seguir sejam atendidos:

- O hardware requerido está instalado.
- Um teclado e um monitor são conectados usando a conexão VGA.
- A chave de ativação está disponível.

Procedimento

1. Digite `setup` para continuar e efetuar login como raiz.
2. Aceite o Contrato de licença do usuário final (EULA).

   Dica: Pressione a tecla Barra de Espaço para avançar através do documento.
3. Quando for solicitada a chave de ativação, digite a sequência alfanumérica de 24 dígitos, com 4 partes, que você recebeu da IBM.

   A letra I e o número 1 (um) são tratados da mesma forma. A letra O e o número 0 (zero) também são tratados da mesma forma.
4. para o tipo de configuração, selecione **normal**, modelo corporativo e configure o horário.
5. Selecione o tipo de endereço IP:
   - Selecione **Sim** para configurar automaticamente o QRadar para IPv6.
   - Selecione **Não** para configurar um endereço IP manualmente do QRadar para IPv4 ou IPv6.
6. Selecione a configuração de interface ligada, se necessário.
7. Selecione a interface gerenciada.
8. No assistente, insira um nome completo do domínio no campo **Nome do host**.
9. No campo **Endereço IP**, insira um endereço IP estático ou use o endereço IP designado.

   Importante: Se você estiver configurando esse host como um host primário para um cluster de alta disponibilidade (HA) e selecionar **Sim** para configuração automática, deverá registrar o endereço IP gerado automaticamente. O endereço IP gerado é inserido durante a configuração de alta disponibilidade.

   Para obter mais informações, consulte o *Guia de alta disponibilidade do IBM Security QRadar*.
10. Se você não tiver um servidor de email, insira `localhost` no campo **Nome do servidor de email**.
11. Clique em **Concluir**.

12. No campo **Senha raiz**, crie uma senha que cumpra os seguintes critérios:
    - Conter pelo menos 5 caracteres
    - Não conter espaços
    - Pode incluir os seguintes caracteres especiais: @, #, ^ e *.
13. Siga as instruções no assistente de instalação para concluir a instalação.

    O processo de instalação pode demorar vários minutos.
14. Aplique sua chave de licença.
    a. Efetue login no QRadar:

       `https://IP_Address_QRadar`

       O nome de usuário padrão é `admin`. A senha é a senha da conta do usuário raiz.
    b. Clique em login.
    c. Clique na guia **Administrador**.
    d. Na área de janela de navegação, clique em **Configuração do Sistema**.
    e. Clique no ícone **Gerenciamento de Sistema e de Licença**.
    f. Na caixa de listagem **Exibir**, selecione **Licenças** e faça upload de chave de licença.
    g. Selecione a licença não alocada e clique em **Alocar Sistema para Licença**.
    h. Na lista de licenças, selecione uma licença e clique em **Alocar Licença para Sistema**.
15. Se desejar incluir hosts gerenciados, use o editor de implementação. Para obter mais informações sobre o editor de implementação, consulte o *Guia de administração do IBM Security QRadar SIEM*.

Ativando o modo VERIFIED

Use a interface da linha de comandos para ativar o modo VERIFIED ou FIPS em seu dispositivo IBM Security QRadar.

Sobre Esta Tarefa

Após ativar o modo VERIFIED em um dispositivo QRadar, o acesso à interface da linha de comandos é restrito à função administrativa ou a contas do usuário criptografadas. Essas contas são criadas ao ativar o modo VERIFIED para QRadar. O acesso ao SSH é restrito às contas do usuário FIPS admin e crypto.

Deve-se ativar o modo VERIFIED em hosts gerenciados primeiro e, depois, no Console do QRadar.

Procedimento

1. Use SSH para efetuar login no QRadar como o usuário raiz.
2. Digite o comando a seguir:

   ```
   /opt/qradar/fips/setup/fips_setup.py --enable
   ```

   Se arquivos criptográficos necessários estiverem ausentes, a saída o alertará sobre os arquivos ausentes.
3. Digite `Sim` para ativar o modo VERIFIED.
4. Insira uma senha para a conta do usuário crypto. A senha deve atender aos seguintes critérios:
   - conter pelo menos 6 caracteres.
   - incluir um caractere especial, como um ponto, vírgula, `$, !, %, ^ ou *`.

5. Insira novamente a senha crypto para confirmar.
6. Insira uma senha para a conta do usuário admin. A senha deve atender aos seguintes critérios:
   - conter pelo menos 6 caracteres.
   - incluir um caractere especial, como um ponto, vírgula, `$, !, %, ^` ou `*`.
7. Insira novamente a senha admin para confirmar.
8. Digite `reboot` para reiniciar o dispositivo QRadar.

   Quando o dispositivo reiniciar os serviços, o modo FIPS será ativado.

   Repita esse processo para ativar o modo FIPS em cada host gerenciado adicional em sua implementação. O Console do QRadar é o dispositivo final ativado no modo FIPS.

O que Fazer Depois

Desative as atualizações automáticas em seus dispositivos FIPS. Para obter informações adicionais, consulte "Desativando atualizações automáticas".

Desativando atualizações automáticas

Para evitar que o sistema instale automaticamente atualizações de software, é necessário desativar as atualizações de software no Console do IBM Security QRadar.

Sobre Esta Tarefa

A especificação FIPS requer a instalação de software certificado e testado pelo FIPS. No entanto, as atualizações de Módulos de Suporte de Dispositivo (DSMs), de protocolos e de scanner são permitidas.

O Console do QRadar é responsável por fazer download e fornecer atualizações para hosts gerenciados em sua implementação. É necessário concluir esse procedimento somente em seu Console.

Procedimento

1. Abra o navegador da web.
2. Efetue login no QRadar:

   `https://<IP address>`

   Nome de usuário: `admin`

   Senha: `<root password>`

   Em que *<IP address>* é o endereço IP do Console do QRadar.
3. Clique em **Efetuar login no QRadar**.

   Uma chave de licença padrão fornece acesso ao QRadar por cinco semanas. Para obter informações adicionais sobre como atualizar sua chave de licença, consulte o Guia de administração do *IBM Security QRadar*.
4. Clique na guia **Administrador**.
5. No menu de navegação, clique em **Configuração do sistema**.
6. Clique no ícone **Atualização automática**.
7. No menu de navegação, clique em **Alterar configurações**.
8. Na caixa de listagem **Atualizações principais**, selecione **Desativar**.
9. Na caixa de listagem **Atualizações secundárias**, selecione **Desativar**.

10. Clique em **Salvar**.

    O processo de instalação está concluído. Agora você está pronto para usar o dispositivo QRadar com o FIPS ativado.

Capítulo 3. Comandos shell do FIPS

É possível usar o SSH para conectar-se a um dispositivo FIPS do IBM Security QRadar como o usuário crypto ou admin que tem permissões especiais de conta.

Usando comandos shell de conta crypto

É possível usar contas do usuário crypto e os comandos que são aplicados a essa conta para executar tarefas administrativas e manter dispositivos FIPS.

Sobre Esta Tarefa

A conta do usuário crypto é fornecida para responsáveis pela segurança em sua organização. Um usuário criptográfico pode desativar o modo VERIFIED em um dispositivo IBM Security QRadar.

As contas do usuário criptográfico podem ativar o modo VERIFIED, verificar o modo de Módulo em um dispositivo ou desativar o modo VERIFIED usando comandos shell. Os usuários crypto também têm permissão de todos os comandos fornecidos para usuários admin para manutenção do QRadar.

Procedimento

1. Use SSH para efetuar login no QRadar como o usuário crypto FIPS.
   Nome de usuário: `crypto`
   Senha: *<password>*
2. Insira um dos seguintes comandos admin:

Tabela 4. Comandos crypto FIPS suportados

Comando	Descrição
commit	Aplica mudanças feitas em um arquivo de sistema do sistema ativado para FIPS. O comando commit inclui as seguintes opções: • **--list** - A opção list exibe os arquivos do sistema que foram alterados pelo usuário crypto. • **--changes <*file*>** - Exibe uma lista de diferenças no arquivo feita por um administrador de um dispositivo ativado para FIPS. • **--check** - Verifica a lista de arquivos que têm permissão para mudanças. • **--allowed** - Exibe uma lista de arquivos do sistema que têm mudanças permitidas por um administrador de um dispositivo ativado para FIPS. • **--force** - Permite que um administrador force uma mudança de arquivo para arquivos na lista permitida. Os arquivos que não estão na lista de arquivos permitida são ignorados. • **--revert <file>** - Descarta mudanças feitas em um arquivo especificado.
deploy	Inicia uma implementação completa em um dispositivo ativado para FIPS. Esse comando reinicia serviços em seu dispositivo. A coleta de eventos e fluxos ficará interrompida até a conclusão do processo de implementação.
disable_verified_mode	Desativa o modo VERIFIED em um dispositivo. Esse processo reinicia vários serviços e requer uma reinicialização do dispositivo.
fips_self_check	Exibe o status do sistema operacional, os arquivos RPM necessários, as configurações de log e o modo de Módulo na linha de comandos.
get_logs	Coleta dados do sistema para seu dispositivo FIPS.
mod_log4j	Modifica origens de log usando a interface da linha de comandos de um dispositivo ativado para FIPS.
reboot	Reinicia um dispositivo ativado para FIPS.
service <service name> <start | stop | restart>	Altera o status de um serviço no dispositivo do QRadar. Para obter uma lista de serviços que podem ser reiniciados pelo usuário crypto, digite **service --list**.

Tabela 4. Comandos crypto FIPS suportados (continuação)

Comando	Descrição
shell	Acessa um shell da linha de comandos para visualizar e editar arquivos.
shutdown	Desliga um dispositivo ativado para FIPS.
help	Exibe a interface da ajuda para um comando FIPS admin ou crypto específico. **<*command*>** é qualquer comando de usuário crypto nessa tabela.
exit	Efetua logout da conta do usuário crypto.

Usando comandos shell de conta admin

É possível usar as contas do usuário admin e os comandos shell para tarefas administrativas e tarefas de manutenção.

Sobre Esta Tarefa

Conceda a função de usuário admin somente a administradores para manter e suportar os dispositivos FIPS em sua organização.

As contas do usuário administrador não podem desativar o modo VERIFIED, verificar o modo de Módulo ou ativar o modo VERIFIED. Os usuários admin podem usar um conjunto específico de opções da linha de comandos para manter um sistema ativado para FIPS.

Procedimento

1. Use SSH para efetuar login no IBM Security QRadar como o usuário admin FIPS.
2. Insira um dos seguintes comandos admin:

Tabela 5. Comandos admin FIPS suportados

Comando	Descrição
commit	Aplica mudanças feitas nos arquivos do sistema de seu sistema ativado para FIPS. O comando commit inclui as seguintes opções: • `--list` - Exibe os arquivos do sistema que são alterados pelo usuário admin. • `changes <file>` - Exibe uma lista de diferenças no arquivo feitas por um administrador de um dispositivo ativado para FIPS. • `--check` - Verifica a lista de arquivos que têm permissão para mudanças. • `--allowed` - Exibe uma lista de arquivos do sistema que têm mudanças permitidas por um administrador de um dispositivo ativado para FIPS. • `--force` - Força uma mudança no arquivo para arquivos na lista permitida. Os arquivos que não estão na lista de arquivos permitida são ignorados. • `--revert <file>` - Descarta mudanças feitas em um arquivo especificado.
deploy	Inicia uma implementação completa em um dispositivo ativado para FIPS.
get_logs	Coleta dados do sistema para seu dispositivo FIPS.
mod_log4j	Modifica origens de log usando a interface da linha de comandos de um dispositivo ativado para FIPS.
reboot	Reinicia um dispositivo ativado para FIPS.
shell	Acessa um shell da linha de comandos para visualizar e editar arquivos.
shutdown	Desliga um dispositivo ativado para FIPS.
help	Exibe uma lista de comandos que estão disponíveis para um usuário admin.
exit	Efetua logout da conta do usuário admin.

Capítulo 4. Casos de uso do FIPS

Tarefas comuns que um usuário crypto ou admin podem ter que executar em dispositivos ativados para FIPS, como usar a linha de comandos para verificar a ativação, reiniciar um serviço e incluir um host gerenciado.

Autoverificação do FIPS

É possível usar a interface da linha de comandos para verificar se o FIPS está ativado em seu dispositivo.

Procedimento

1. Use SSH para efetuar login no IBM Security QRadar como o usuário `crypto`.
2. Digite `fips_self_check`.

   A saída exibe o status de seu dispositivo FIPS.

   ```
   Verifying Operating System ... (OK)
   Verifying installed RPMs: - kernel ... (OK) - dracut-fips ... (OK) -
   libgcrypt... (OK) - openssl ... (OK) - nss ... (OK) - fipscheck-lib ...
   (OK)
   Verifying Ariel Log Hashing Setting ... (OK)
   Modo de módulo: VERIFIED
   ```

Desativando o modo VERIFIED

É possível usar a interface da linha de comandos e a conta do usuário criptográfico para desativar o modo VERIFIED em um dispositivo IBM Security QRadar.

Sobre Esta Tarefa

O modo VERIFIED deve estar desativado na ordem a seguir:

1. Hosts gerenciados
2. QRadar Console

Procedimento

1. Use SSH para efetuar login no dispositivo FIPS do QRadar como um usuário `crypto`.
2. Insira o seguinte comando:

   ```
   disable_verified_mode
   ```

3. Digite **Sim** para desativar do modo VERIFIED.
4. Digite **reboot** para reiniciar o dispositivo QRadar.

   Após o dispositivo reiniciar os serviços, o modo VERIFIED será desativado. Para desativar o modo VERIFIED, repita esse processo em cada dispositivo adicional incluído no Console como um host gerenciado.

Reiniciando um serviço quando o modo VERIFIED está ativado

Use SSH para reiniciar, parar ou iniciar um serviço quando o modo VERIFIED estiver ativado com as instruções a seguir.

Procedimento

1. Use SSH para efetuar login no IBM Security QRadar como o usuário `crypto` FIPS.
2. Digite `service --list`.
3. Digite `service <service name> <start | stop | restart>`.

   Exemplo: No exemplo a seguir, o servidor Tomcat é reiniciado.

   ```
   service tomcat restart
   ```
4. Digite `exit` para efetuar logout da interface da linha de comandos shell.

Editando um arquivo de configuração com o modo VERIFIED ativado

É possível editar o arquivo de mapeamento do aplicativo para assegurar que o tráfego seja classificado de forma apropriada na interface com o usuário do IBM Security QRadar. As entradas extras incluídas no arquivo de mapeamento substituem os IDs do aplicativo padrão.

Sobre Esta Tarefa

Esse caso de uso destina-se a mostrar a um administrador como editar um ID do aplicativo padrão quando o modo VERIFIED está ativado.

Procedimento

1. Use SSH para efetuar login no QRadar como o usuário `admin` ou `crypto` FIPS.
2. Digite `shell`.
3. Insira `edit <file name>` para iniciar a edição de um arquivo de configuração do sistema.

   Exemplo: No exemplo a seguir, apps.conf é editado.

   ```
   edit /store/configservices/staging/globalconfig/apps.conf
   ```
4. Salve suas mudanças.
5. Digite `exit` para sair do shell de comando.
6. Digite `commit --changes <file name>` para visualizar as mudanças feitas no arquivo de configuração.

   Exemplo: No exemplo a seguir, as mudanças no arquivo apps.conf são visualizadas.

   ```
   changes /store/configservices/staging/globalconfig/apps.conf
   ```
7. Digite `commit` para aplicar as mudanças no arquivo de configuração ao dispositivo ativado para FIPS.

   O arquivo é atualizado em seu dispositivo FIPS quando aparece a seguinte mensagem.

   ```
   Mudanças confirmadas para /store/configservices/staging/globalconfig/
   apps.conf \
   ```

Incluindo um host gerenciado em uma implementação de FIPS

Para incluir um novo host gerenciado na implementação do FIPS, deve-se desativar o modo VERIFIED em sua implementação, incluir o host gerenciado e ativar novamente o modo VERIFIED.

Procedimento

1. Efetue login como o usuário criptográfico e desative o modo VERIFIED em todos os dispositivos em sua implementação, digitando o comando a seguir:

   ```
   disable_verified_mode
   ```

   Deve-se desativar o modo VERIFIED na ordem a seguir:

   - Hosts gerenciados
   - IBM Security QRadar Console
2. Efetue login na interface com o usuário do Console do QRadar como o usuário `admin`.
3. Na guia **Admin**, clique em **Editor de implementação**.
4. No menu, selecione **Ações > Incluir um host gerenciado**.
5. Clique em **Avançar**.
6. Insira valores para os parâmetros.

   Se você selecionou a caixa de seleção **O host é baseado em NAT**, a página Definir configurações do NAT será exibida.
7. Para selecionar uma rede NAT, insira valores para os seguintes parâmetros:

   - **Inserir IP público do servidor ou dispositivo a ser incluído** - O host gerenciado usa o endereço IP público para comunicar-se com hosts gerenciados em redes diferentes que usam o NAT.
   - **Selecionar rede baseada em NAT** - Na caixa de listagem, selecione a rede que deseja que seja usada por esse host gerenciado.

   Se o host gerenciado estiver na mesma sub-rede que o Console, selecione o console da rede baseada em NAT.

   Se o host gerenciado não estiver na mesma sub-rede que o Console, selecione o host gerenciado da rede baseada em NAT.

   Nota: Para obter informações sobre como gerenciar redes baseadas em NAT, consulte o Guia de administração do *QRadar*.
8. Clique em **Avançar**.
9. Clique em **Concluir**.

   Uma mensagem do sistema informa que o editor de implementação está incluindo o host gerenciado. Quando esse processo estiver concluído, você retornará à guia **Admin**.
10. No menu da guia **Admin**, clique em **Implementar Mudanças**.
11. Use SSH para efetuar login no dispositivo do QRadar como o usuário `crypto`.
    a. Digite o comando a seguir para ativar novamente o modo VERIFIED:

       ```
       /opt/qradar/fips/setup/fips_setup.py --enable
       ```

       Deve-se ativar novamente o modo VERIFIED na ordem a seguir:

       - Hosts gerenciados
       - QRadar Console

    b. Insira **Sim** para ativar novamente o modo VERIFIED.
    c. Digite `reboot` para reiniciar o dispositivo QRadar.

       Após o dispositivo reiniciar os serviços, o modo VERIFIED é ativado. A configuração está concluída.

Capítulo 5. Gerenciamento de Configurações de Rede

Utilize o `script qchange_netsetup` para alterar as configurações de rede de seu sistema IBM Security QRadar. As definições de rede configuráveis incluem nome do host, endereço IP, máscara de rede, gateway, endereços DNS, endereço IP público e servidor de e-mail.

Caso deva desativar o modo VERIFIED, consulte "Desativando o modo VERIFIED" na página 23 na página 23.

Alterando as Configurações de Rede em um Sistema Multifuncional

É possível alterar as configurações de rede em seu sistema multifuncional. Um sistema multifuncional tem todos os componentes do IBM Security QRadar que estão instalados em um sistema.

Antes de Iniciar

- Você deve ter uma conexão local para seu QRadar Console.
- Confirme que não há mudanças não implementadas.
- Se você estiver mudando o nome do host do endereço IP de uma caixa na implementação, deverá removê-lo da implementação.
- Se esse sistema fizer parte de um par HA, primeiro você deverá desativar o HA antes de mudar quaisquer configurações de rede.
- Se o sistema que você deseja mudar é o console, você deverá remover todos os hosts na implementação antes de continuar.

Procedimento

1. Efetue login como o usuário raiz.
2. Digite o comando a seguir:

   ```
   qchange_netsetup
   ```
3. Siga as instruções no assistente para concluir a configuração.

   A tabela a seguir contém descrições e notas para ajudar a configurar as configurações de rede.

Tabela 6. Descrição de Configurações de Rede para um QRadar Console Multifuncional

Configuração de Rede	Descrição
Nome do host	Nome completo do domínio
Endereço do servidor do DNS secundário	Opcional
Endereço IP público para redes que utilizam Conversão de Endereço de Rede (NAT)	Opcional Utilizado para acessar o servidor, geralmente a partir de uma rede diferente ou da Internet. Configurado usando os serviços de Conversão de Endereço de Rede (NAT) em suas configurações de rede ou firewall em sua rede. (O NAT converte um endereço IP em uma rede em um endereço IP diferente em outra rede).

Tabela 6. Descrição de Configurações de Rede para um QRadar Console Multifuncional (continuação)

Configuração de Rede	Descrição
Nome do servidor de e-mail	Se você não tiver um servidor de e-mail, utilize `localhost`.

Uma série de mensagens é exibida conforme o QRadar processa as alterações solicitadas. Após as alterações solicitadas serem processadas, o sistema do QRadar é encerrado e reiniciado automaticamente.

Alternando as configurações de rede de um QRadar Console em uma implementação de múltiplos sistemas

Para alterar as configurações de rede em uma implementação multissistema do IBM Security QRadar, remova todos os hosts gerenciados, altere as configurações de rede, inclua os hosts gerenciados novamente e, então, redesigne o componente.

Antes de Iniciar

- Você deve ter uma conexão local para seu QRadar Console.

Procedimento

1. Para remover hosts gerenciados, efetue login no QRadar:

   `https://IP_Address_QRadar`

   O **Username** é `admin`.

   a. Clique na guia **Administrador**.
   b. Clique no ícone do **Editor de implementação**.
   c. Na janela Editor de Implementação, clique na guia **Visualização do Sistema**.
   d. Para cada host gerenciado em sua implementação, clique com o botão direito do mouse no host gerenciado e selecione **Remover Host**.
   e. Na guia **Administrador**, clique em **Implementar Mudanças**.
2. Digite o seguinte comando: `qchange_netsetup`.
3. Siga as instruções no assistente para concluir a configuração.

   A tabela a seguir contém descrições e notas para ajudar a configurar as configurações de rede.

Tabela 7. Descrição de configurações de rede para uma implementação do QRadar Console de múltiplos sistemas.

Configuração de Rede	Descrição
Nome do host	Nome completo do domínio
Endereço do servidor do DNS secundário	Opcional

Tabela 7. Descrição de configurações de rede para uma implementação do QRadar Console de múltiplos sistemas (continuação).

Configuração de Rede	Descrição
Endereço IP público para redes que utilizam Conversão de Endereço de Rede (NAT)	Opcional Utilizado para acessar o servidor, geralmente a partir de uma rede diferente ou da Internet. Configurado usando os serviços de Conversão de Endereço de Rede (NAT) em suas configurações de rede ou firewall em sua rede. (O NAT converte um endereço IP em uma rede em um endereço IP diferente em outra rede).
Nome do servidor de e-mail	Se você não tiver um servidor de e-mail, utilize `localhost`.

Depois de configurar os parâmetros de instalação, uma série de mensagens é exibida. O processo de instalação pode demorar vários minutos.

4. Para incluir novamente e redesignar os hosts gerenciados, efetue login no QRadar.

   `https://IP_Address_QRadar`

   O **Username** é `admin`.

   a. Clique na guia **Administrador**.
   b. Clique no ícone do **Editor de implementação**.
   c. Na janela Editor de Implementação, clique na guia **Visualização do Sistema**.
   d. Clique em **Ações** > **Incluir um host gerenciado**.
   e. Siga as instruções no assistente para incluir um host.

      Selecione a opção **Host é NAT** para configurar um endereço IP público para o servidor. Esse endereço IP é um endereço IP secundário que é utilizado para acessar o servidor, geralmente a partir de uma rede diferente ou da Internet. O endereço IP público é geralmente configurado utilizando os serviços de Conversão de Endereço de Rede (NAT) em suas configurações de rede ou firewall em sua rede. O NAT converte um endereço IP em uma rede em um endereço IP diferente em outra rede

5. Redesigne todos os componentes que não são sejam seu QRadar Console para seus hosts gerenciados.

   a. Na janela Editor de Implementação, clique na guia **Visualização de Eventos** e selecione o componente que você deseja redesignar para o host gerenciado.
   b. Clique em **Ações** > **Designar**.
   c. Na lista **Selecione uma lista de hosts**, selecione o host que você deseja redesignar para este componente.
   d. Na guia **Administrador**, clique em **Implementar Mudanças**.

Atualizando Configurações de Rede Após uma Substituição de NIC

Se você substituir sua placa-mãe integrada ou NICs (placas da interface de rede) independentes, deverá atualizar suas configurações de rede do IBM Security QRadar para assegurar que o hardware permaneça operacional.

Sobre Esta Tarefa

O arquivo de configurações de rede contém um par de linhas para cada NIC que está instalado e um par de linhas para cada NIC que foi removido. Você deve remover as linhas para o NIC que você removeu e, em seguida, renomear o NIC que você instalou.

Seu arquivo de configurações de rede pode ser parecido com o seguinte exemplo, em que *NAME="eth0"* é o NIC que foi substituído e *NAME="eth4"* é o NIC que foi instalado.

```
 # PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"
```

Procedimento

1. Utilize o SSH para efetuar login no produto IBM Security QRadar como o usuário raiz.

   O nome de usuário é `raiz`.
2. Digite o comando a seguir:

   `cd /etc/udev/rules.d/`
3. Para editar o arquivo de configurações de rede, digite o seguinte comando:

   `vi 70-persistent-net.rules`
4. Remova o par de linhas para o NIC que foi substituído: `NAME="eth0"`.
5. Renomeie os valores `Name=<eth>` para o NIC recém-instalado.

   Exemplo: Renomeie `NAME="eth4"` para `NAME="eth0"`.
6. Salve e feche o arquivo.
7. Digite o seguinte comando: `reboot`.

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 22290-240

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 mudanças 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:

Adobe, o logotipo Adobe, PostScript e o logotipo PostScript são marcas registradas ou marcas comerciais da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

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 de política de privacidade

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 pessoalmente identificáveis, informações específicas sobre o uso de cookies desta oferta serão apresentadas 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 de sessões e autenticação. Esses cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade ativada por eles.

Se as configurações implementadas para esta Oferta de Software fornecerem a você, como cliente, a capacidade de coletar informações pessoalmente identificáveis dos usuários finais por meio de cookies e outras tecnologias, deve-se buscar o seu próprio conselho jurídico a respeito de quaisquer leis aplicáveis a tal 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, 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.

Índice Remissivo

Numéricos

A

B

C

D

F

H

I

M

N

P

R

S

V