IBM Security QRadar
Versão 7.2.5

Guia de Instalação

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 63.

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 QRadar v

Capítulo 1. Visão Geral de Implementação do QRadar 1
Chaves de Ativação e Chaves de Licença 1
Módulo de Gerenciamento Integrado 2
Componentes do QRadar 2
Acessórios de Hardware e Software de Desktop de Pré-requisito para Instalações do QRadar 4
Navegadores da web suportados 5
Ativando o modo de documento e o modo de navegador no Internet Explorer 6
Instalações da unidade flash USB 6
Criando uma unidade flash USB inicializável com um dispositivo QRadar. 7
Criando uma unidade flash USB com Microsoft Windows 8
Criando uma unidade flash USB inicializável com Red Hat Linux 9
Configurando uma unidade flash USB para dispositivos apenas seriais 10
Instalando um QRadar com uma unidade flash USB. 11

Capítulo 2. Instalando um QRadar Console ou Host Gerenciado 13

Capítulo 3. Instalações de Software QRadar em seu Próprio Dispositivo 15
Pré-requisitos para Instalar QRadar em seu Próprio Dispositivo 15
Preparando as instalações de software do QRadar para os sistemas de arquivos HA e XFS 16
Propriedades de partição do sistema operacional Linux para instalações QRadar em seu próprio dispositivo . . 17
Instalando o RHEL em seu Próprio Dispositivo 18

Capítulo 4. Instalações do Dispositivo Virtual para QRadar SIEM e QRadar Log Manager 21
Visão Geral dos Dispositivos Virtuais Suportados. 21
Requisitos do sistema para dispositivos virtuais 23
Criando sua Máquina Virtual 25
Instalando o Software QRadar em uma Máquina Virtual 26
Incluindo seu Dispositivo Virtual para sua Implementação 27

Capítulo 5. Instalações a Partir da Partição de Recuperação 29
Reinstalando a partir da partição de recuperação 29

Capítulo 6. Configurando as instalações silenciosas para o QRadar 31

Capítulo 7. Visão geral da implementação do QRadar em um ambiente de nuvem . . . 37
Configurando end points do servdior para instalações em nuvem 37
Configurando redes de clientes para instalações em nuvem 38
Configurando um membro para instalações em nuvem 40

Capítulo 8. Visão geral do nó de dados. 41

Capítulo 9. Gerenciamento de Configurações de Rede 45
Alterando as Configurações de Rede em um Sistema Multifuncional 45
Alternando as configurações de rede de um QRadar Console em uma implementação de múltiplos sistemas . . . 46
Atualizando Configurações de Rede Após uma Substituição de NIC 47

Capítulo 10. Resolução de Problemas 49
Recursos de Resolução de Problemas 50
Support Portal 50
Solicitações de Serviço. 50

Fix Central 50
Bases de Conhecimento 51
Arquivos de Log do QRadar. 51
Portas Usadas pelo QRadar 52
Procurando Portas em Uso por QRadar 60
Visualizando Associações de Porta do IMQ. 61

Avisos 63
Marcas comerciais 65
Considerações de política de privacidade 65

Índice Remissivo 67

Introdução às Instalações do QRadar

Os dispositivos IBM® Security QRadar vêm com o software e o sistema operacional Red Hat Enterprise Linux pré-instalados. Você também pode instalar o software QRadar em seu próprio hardware.

Obrigado por pedir seu dispositivo da IBM! É fortemente recomendado aplicar a última manutenção ao seu dispositivo para os melhores resultados. Visite o IBM Fix Central (http://www.ibm.com/support/fixcentral) para determinar qual é a última correção recomendada para o seu produto.

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

Público-alvo

Os administradores de rede que são responsáveis pela instalação e configuração de sistemas QRadar devem estar familiarizados com os conceitos de segurança da rede e o sistema operacional Linux.

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.

Para desempenho máximo e escalabilidade, você deve instalar um dispositivo de host gerenciado de alta disponibilidade (HA) para cada sistema gerenciado que requer proteção de HA. Para obter mais informações sobre a instalação ou a recuperação de um sistema de HA, consulte *IBM Security QRadar High Availability Guide*.

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 13
Instale o Console IBM Security QRadar ou um host gerenciado no dispositivo QRadar ou em seu próprio dispositivo.

"Instalando o RHEL em seu Próprio Dispositivo" na página 18
É possível instalar o sistema operacional Red Hat Enterprise Linux em seu próprio dispositivo para uso com o IBM Security QRadar.

"Instalando o Software QRadar em uma Máquina Virtual" na página 26
Depois de criar sua máquina virtual, você deve instalar o software IBM Security QRadar na máquina virtual.

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.

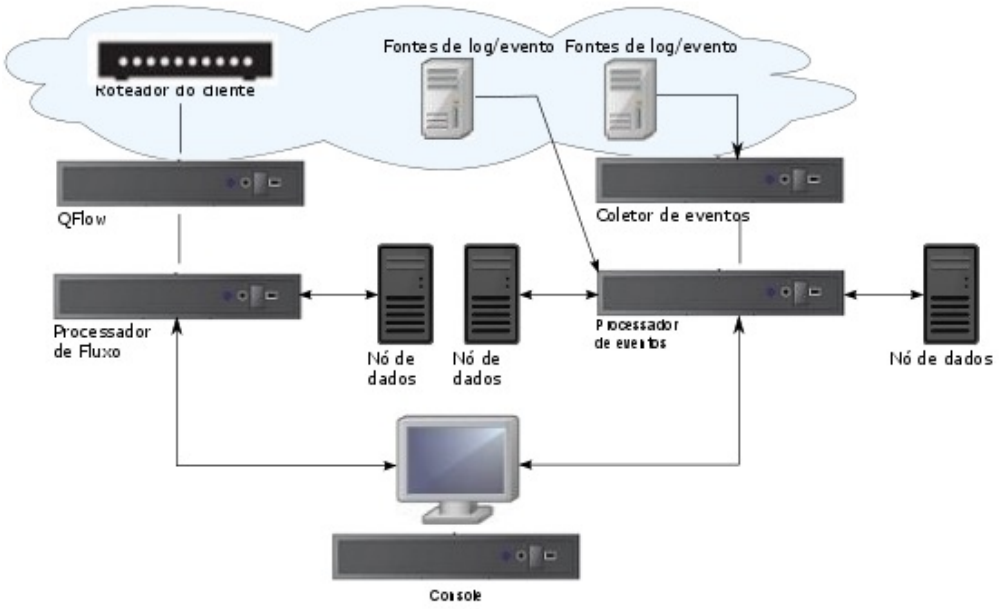

Figura 1. Exemplo de implementação do QRadar

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.

Nó de dados

Os Nós de dados permitem que implementações novas e existentes do QRadar incluam capacidade de armazenamento e processamento sob demanda conforme o necessário.

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

Conceitos relacionados:

Capítulo 10, “Resolução de Problemas”, na página 49
A resolução de problemas é uma abordagem sistemática para resolver um problema. O objetivo da resolução de problemas é determinar por que algo não funciona conforme o esperado e como resolver o problema.

Capítulo 8, “Visão geral do nó de dados”, na página 41
Entenda como usar Nós de dados na sua implementação do IBM Security QRadar.

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 13
Instale o Console IBM Security QRadar ou um host gerenciado no dispositivo QRadar ou em seu próprio dispositivo.

"Instalando o RHEL em seu Próprio Dispositivo" na página 18
É possível instalar o sistema operacional Red Hat Enterprise Linux em seu próprio dispositivo para uso com o IBM Security QRadar.

"Instalando o Software QRadar em uma Máquina Virtual" na página 26
Depois de criar sua máquina virtual, você deve instalar o software IBM Security QRadar na máquina virtual.

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

Tabela 3. Navegadores da web suportados para produtos QRadar (continuação)

Navegador da web	Versões suportadas
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.

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*.

Capítulo 3. Instalações de Software QRadar em seu Próprio Dispositivo

Para assegurar uma instalação bem-sucedida do IBM Security QRadar em seu próprio dispositivo, você deve instalar o sistema operacional Red Hat Enterprise Linux.

Assegure-se de que seu dispositivo atenda aos requisitos do sistema para implementações do QRadar.

Se estiver instalando o software QRadar em seu próprio hardware, agora será possível comprar a licença RHEL como parte da sua compra de software QRadar e usar o RHEL que é enviado com a imagem ISO de software QRadar.

Instale o RHEL separadamente se sua compra do QRadar não incluir o sistema operacional RHEL. Se o seu sistema QRadar incluir o RHEL, não será preciso configurar partições e executar outra preparação RHEL. Continue em Capítulo 2, “Instalando um QRadar Console ou Host Gerenciado”, na página 13.

Importante: Não instale pacotes RPM que não foram aprovados pela IBM. Instalações RPM não aprovadas podem causar erros de dependência ao fazer upgrade do software QRadar e podem também causar problemas de desempenho em sua implementação. Não use YUM para atualizar seu sistema operacional ou instalar software não aprovado nos sistemas QRadar.

Pré-requisitos para Instalar QRadar em seu Próprio Dispositivo

Antes de instalar o sistema operacional Red Hat Enterprise Linux (RHEL) em seu próprio dispositivo, assegure-se de que seu sistema atenda aos requisitos do sistema.

A tabela a seguir descreve os requisitos do sistema:

Tabela 4. Requisitos do Sistema para Instalações do RHEL em seu Próprio Dispositivo

Requisito	Descrição
Versão de software suportada	Versão 6.5
Versão de Bit	64 bits
Discos de KickStart	Não Suportados
Pacote de Network Time Protocol (NTP)	Opcional Se desejar utilizar NTP como servidor de horário, assegure que você instalou o pacote NTP
Memória (RAM) para sistemas do Console	Mínimo de 32 GB **Importante:** Você deve fazer upgrade de sua memória do sistema antes de instalar o QRadar.
Memória (RAM) para Processador de Eventos	24 GB
Memória (RAM) para o coletor de eventos	16 GB

Tabela 4. Requisitos do Sistema para Instalações do RHEL em seu Próprio Dispositivo (continuação)

Requisito	Descrição
Memória (RAM) para QRadar QFlow Collector	6 GB
Espaço livre em disco para sistemas de Console	Mínimo de 256 GB **Importante:** Para obter desempenho ideal, assegure que um extra de 2-3 vezes do espaço em disco mínimo esteja disponível.
Unidade primária do QRadar QFlow Collector	Mínimo de 70 GB
Configuração de firewall	WWW (http, https) ativado SSH ativado **Importante:** Antes de configurar o firewall, desative a opção SELinux. A instalação do QRadar inclui um modelo de firewall padrão que você pode atualizar na janela Configuração do Sistema.

Preparando as instalações de software do QRadar para os sistemas de arquivos HA e XFS

Como parte da configuração de alta disponibilidade (HA), o instalador do QRadar requer uma quantidade mínima de espaço livre no sistema de arquivos de armazenamento, `/store/`, para processos de replicação. Espaço deve ser alocado antecipadamente porque os sistemas de arquivos XFS não podem ser reduzidos de tamanho depois que são formatados.

Para preparar a partição XFS para uso com sistemas de HA, você deve executar as seguintes tarefas:

1. Use o comando **`mkdir`** para criar os diretórios a seguir:
   - `/media/cdrom`
   - `/media/redhat`
2. Monte a imagem ISO de software do QRadar digitando o comando a seguir:
   `mount -o loop <path_to_QRadar_iso> /media/cdrom`
3. Monte o software do RedHat Enterprise Linux V6.5 digitando o comando a seguir:
   `mount -o loop <path_to_RedHat_6.5_64bit_dvd_iso_1> /media/redhat`
4. Se o seu sistema estiver designado como host primário no par de HA, execute o script a seguir:
   `/media/cdrom/post/prepare_ha.sh`
5. Para iniciar a instalação, digite o seguinte comando:
   `/media/cdrom/setup`

Nota: Este procedimento não é necessário em seu host de HA secundário.

Propriedades de partição do sistema operacional Linux para instalações QRadar em seu próprio dispositivo

Se você utilizar seu próprio dispositivo, poderá excluir e recriar partições em seu sistema operacional Red Hat Enterprise Linux em vez de modificar as partições padrão.

Utilize os valores na seguinte tabela como um guia ao recriar o particionamento no sistema operacional Red Hat Enterprise Linux.

Restrição: O redimensionamento de volumes lógicos utilizando um gerenciador de volumes lógicos (LVM) não é suportado.

Tabela 5. Guia de Partição para RHEL

Partição	Descrição	Ponto de Montagem	Tipo do Sistema de Arquivos	Tamanho	Forçado a ser Primário	SDA ou SDB
/boot	Arquivos de inicialização do sistema	/boot	EXT4	200 MB	Sim	SDA
troca	Usado como memória quando a RAM está cheia.	vazio	troca	Sistemas com 4 a 8 GB de RAM, o tamanho da partição de troca deve corresponder à quantidade de RAM Sistemas com 8 a 24 GB de RAM, configure o tamanho da partição de troca para ser 75% de RAM, com um valor mínimo de 8 GB e um valor máximo de 24 GB.	Não	SDA
/	Área de instalação para QRadar, o sistema operacional e os arquivos associados.	/	EXT4	20000 MB	Não	SDA
/store/tmp	Área de armazenamento para arquivos temporários do QRadar	/store/tmp	EXT4	20000 MB	Não	SDA
/var/log	Área de armazenamento para QRadar e os arquivos de log do sistema	/var/log	EXT4	20000 MB	Não	SDA

Tabela 5. Guia de Partição para RHEL (continuação)

Partição	Descrição	Ponto de Montagem	Tipo do Sistema de Arquivos	Tamanho	Forçado a ser Primário	SDA ou SDB
/store	Área de armazenamento para dados e arquivos de configuração do QRadar	/store	XFS	[1]Em dispositivos do Console: aproximadamente 80% do armazenamento disponível. Em hosts gerenciados diferentes de Coletores QFlow e Coletores de Eventos de Armazenamento e Encaminhamento: aproximadamente 90% do armazenamento disponível.	Não	SDA Se 2 discos, SDB
/store/transient	Área de armazenamento para o cursor do banco de dados ariel	/store/transient	XFS em Consoles EXT4 em hosts gerenciados	[1]Em dispositivos do Console: 20% do armazenamento disponível. Em hosts gerenciados diferentes de Coletores QFlow e Coletores de Eventos de Armazenamento e Encaminhamento: 10% do armazenamento disponível.	Não	SDA Se 2 discos, SDB
[1]O /store e o /store/transient juntos ocupam 100% do espaço em disco que permanece após criar as primeiras 5 partições.						

Restrições

Futuros upgrades de software podem falhar se você reformatar qualquer uma das partições a seguir ou suas subpartições:

- /store
- /store/tmp
- /store/ariel
- /store/transient

Instalando o RHEL em seu Próprio Dispositivo

É possível instalar o sistema operacional Red Hat Enterprise Linux em seu próprio dispositivo para uso com o IBM Security QRadar.

Sobre Esta Tarefa

Instale o RHEL separadamente se sua instalação do QRadar não incluir o sistema operacional RHEL. Se o seu sistema QRadar não incluir o RHEL, continue com Capítulo 3, “Instalações de Software QRadar em seu Próprio Dispositivo”, na página 15.

Procedimento

1. Copie o DVD do sistema operacional do Red Hat Enterprise Linux 6.5 ISO para um dos seguintes dispositivos de armazenamento móveis:
   - Digital Versatile Disk (DVD)
   - Unidade Flash USB Inicializável
2. Insira o dispositivo de armazenamento móvel em seu dispositivo e reinicie seu dispositivo.
3. No menu inicial, selecione uma das seguintes opções:
   - Selecione a unidade de `USB` ou `DVD` como a opção de inicialização.
   - Para instalar em um sistema que suporta Extensible Firmware Interface (EFI), você deve iniciar o sistema no modo `legado`.
4. Quando solicitado, efetue login no sistema como o usuário raiz.
5. Para evitar um problema com a nomenclatura do endereço da interface Ethernet, na página Bem-vindo, pressione a tecla Tab e no final da linha `Vmlinuz initrd=initrd.image`, inclua `biosdevname=0`.
6. Siga as instruções no assistente de instalação para concluir a instalação:
   a. Selecione a opção **Dispositivos de Armazenamento Básico**.
   b. Quando você configura o nome do host, a propriedade **Hostname** pode incluir letras, números e hifens.
   c. Quando você configurar a rede, na janela Conexões de Rede, selecione **System eth0** e, em seguida, clique em **Editar** e selecione **Conectar automaticamente**.
   d. Na guia **Configurações de IPv4**, a partir da lista **Método**, selecione **Manual**.
   e. No campo **Servidores DNS**, digite uma lista separada por vírgula.
   f. Selecione a opção **Criar Layout Customizado**.
   g. Configure `EXT4` para o tipo de sistema de arquivos para as partições `/`, `/boot`, `store/tmp` e `/var/log`.

      Para obter informações adicionais sobre tipos de sistemas de arquivos com base nos tipos de dispositivos, consulte “Propriedades de partição do sistema operacional Linux para instalações QRadar em seu próprio dispositivo” na página 17.
   h. Reformate a partição de troca com um tipo de sistema de arquivos de troca.
   i. Selecione **Servidor Básico**.
7. Quando a instalação estiver concluída, clique em **Reinicializar**.

O que Fazer Depois

Após a instalação, se suas interfaces de rede integradas forem nomeadas com algo diferente de `eth0`, `eth1`, `eth2` e `eth3`, você deverá renomear as interfaces de rede.

Referências relacionadas:

"Propriedades de partição do sistema operacional Linux para instalações QRadar em seu próprio dispositivo" na página 17
Se você utilizar seu próprio dispositivo, poderá excluir e recriar partições em seu sistema operacional Red Hat Enterprise Linux em vez de modificar as partições padrão.

Capítulo 4. Instalações do Dispositivo Virtual para QRadar SIEM e QRadar Log Manager

É possível instalar o IBM Security QRadar SIEM e o IBM Security QRadar Log Manager em um dispositivo virtual. Certifique-se de utilizar um dispositivo virtual suportado que atenda aos requisitos mínimos do sistema.

Restrição: O redimensionamento de volumes lógicos utilizando um gerenciador de volumes lógicos (LVM) não é suportado.

Para instalar um dispositivo virtual, conclua as seguintes tarefas na sequência:

__ • Crie uma máquina virtual.

__ • Instale o software QRadar na máquina virtual.

__ • Inclua o seu dispositivo virtual na implementação.

Visão Geral dos Dispositivos Virtuais Suportados

Um dispositivo virtual é um sistema IBM Security QRadar que consiste em software QRadar que está instalado em uma máquina virtual VMWare ESX .

Um dispositivo virtual fornece a mesma visibilidade e função em sua infraestrutura de rede virtual que dispositivos do QRadar fornecem em seu ambiente físico.

Depois de instalar os dispositivos virtuais, utilize o editor de implementação para incluir os dispositivos virtuais em sua implementação. Para obter mais informações sobre como conectar dispositivos, consulte *Guia de Administração*.

Os seguintes dispositivos virtuais estão disponíveis:

QRadar SIEM All-in-One Virtual 3199

Esse dispositivo virtual é um sistema QRadar SIEM que pode definir o perfil de comportamento da rede e identificar ameaças à segurança da rede. O dispositivo virtual QRadar SIEM All-in-One Virtual 3199 inclui um Coletor de Eventos integrado e armazenamento interno para eventos.

O dispositivo virtual QRadar SIEM All-in-One Virtual 3199 suporta os seguintes itens:

- Até 1.000 objetos de rede
- 200.000 fluxos por intervalo, dependendo de sua licença
- 5.000 eventos por segundo (EPS), dependendo de sua licença
- 750 feeds de evento (mais dispositivos podem ser incluídos em seu licenciamento)
- As origens de dados de fluxo externo para NetFlow, sFlow, J-Flow, Packeteer e arquivos de Flowlog
- Monitoramento da atividade de rede do QRadar QFlow Collector e Camada 7

Para expandir a capacidade do QRadar SIEM All-in-One Virtual 3199 além das opções de upgrade baseadas em licença, você pode incluir um ou mais dos

dispositivos virtuais QRadar SIEM Event Processor Virtual 1699 ou QRadar SIEM Flow Processor Virtual 1799 :

QRadar SIEM Flow Processor Virtual 1799

Esse dispositivo virtual é implementado com qualquer dispositivo série QRadar SIEM 3105 ou QRadar SIEM 3124. O dispositivo virtual é utilizado para aumentar o armazenamento e inclui um Processador de Eventos integrado e armazenamento interno.

O dispositivo QRadar SIEM Flow Processor Virtual 1799 suporta os seguintes itens:

- 600.000 fluxos por intervalo, dependendo dos tipos de tráfego
- 2 TB ou mais de armazenamento de fluxo dedicado
- 1.000 objetos da rede
- Monitoramento da atividade de rede do QRadar QFlow Collector e Camada 7

Você pode incluir dispositivos QRadar SIEM Flow Processor Virtual 1799 em qualquer dispositivo série QRadar SIEM 3105 ou QRadar SIEM 3124 para aumentar o armazenamento e o desempenho de sua implementação.

QRadar SIEM Event Processor Virtual 1699

Esse dispositivo virtual é um Processador de Eventos dedicado que permite escalar sua implementação do QRadar SIEM para gerenciar maiores taxas de EPS. O QRadar SIEM Event Processor Virtual 1699 inclui um Coletor de Eventos integrado, Processador de Eventos e armazenamento interno para eventos.

O dispositivo QRadar SIEM Event Processor Virtual 1699 suporta os seguintes itens:

- Até 10.000 eventos por segundo
- 2 TB ou mais de armazenamento de eventos dedicados

O dispositivo virtual QRadar SIEM Event Processor Virtual 1699 é um dispositivo Processador de Eventos distribuído e requer uma conexão com qualquer dispositivo série QRadar SIEM 3105 ou QRadar SIEM 3124.

QRadar Data Node Virtual 1400

Esse dispositivo virtual fornece retenção e armazenamento para eventos e fluxos. O dispositivo virtual expande o armazenamento de dados disponível de Processadores de Eventos e Processadores de Fluxo e também aprimora o desempenho da procura.

Dimensione o Dispositivo QRadar Data Node Virtual 1400 de acordo, com base na taxa de EPS e nas regras de retenção de dados da implementação.

As políticas de retenção de dados são aplicadas a um Dispositivo QRadar Data Node Virtual 1400 da mesma maneira que são aplicadas aos Processadores de Eventos e aos Processadores de Fluxo independentes. As políticas de retenção de dados são avaliadas em uma base nó por nó. Critérios, como espaço livre, têm como base o Dispositivo QRadar Data Node Virtual 1400 individual e não o cluster como um todo.

Nós de Dados podem ser incluídos nos seguintes dispositivos:

- Processador de Eventos (16XX)
- Processador de Fluxo (17XX)
- Processador de Evento/Fluxo (18XX)
- Multifuncional (2100 e 31XX)

Para ativar todos os recursos incluídos no Dispositivo QRadar Data Node Virtual 1400, faça a instalação utilizando a chave de ativação 1400.

QRadar VFlow Collector 1299

Esse dispositivo virtual fornece a mesma visibilidade e função em sua infraestrutura de rede virtual que um QRadar QFlow Collector oferece em seu ambiente físico. O dispositivo virtual do QRadar QFlow Collector analisa o comportamento de rede e fornece visibilidade da Camada 7 dentro de sua infraestrutura virtual. A visibilidade de rede é derivada de uma conexão direta com o comutador virtual.

O dispositivo virtual do QRadar VFlow Collector 1299 suporta um máximo dos seguintes itens:

- 10.000 fluxos por minuto
- Três comutadores virtuais, com mais um comutador que é designado como a interface de gerenciamento.

O dispositivo virtual QRadar VFlow Collector 1299 não suporta NetFlow.

Requisitos do sistema para dispositivos virtuais

Para assegurar que o IBM Security QRadar funcione corretamente, assegure que o dispositivo virtual que você utiliza atenda aos requisitos mínimos de software e hardware.

Antes de instalar seu dispositivo virtual, assegure que os requisitos mínimos a seguir sejam atendidos:

Tabela 6. Requisitos para Dispositivos Virtuais

Requisito	Descrição
Cliente VMware	VMWare ESX 5.0 VMWare ESX 5.1 VMWare ESX 5.5 Para obter mais informações sobre os clientes VMWare, consulte o Website do VMware (www.vmware.com)
Tamanho do disco virtual nos dispositivos QRadar VFlow Collector, QRadar Coletor de Eventos, QRadar Processador de Eventos, QRadar Processador de Fluxo, QRadar All-in-One e QRadar Log Manager	Mínimo: 256 GB **Importante:** Para obter desempenho ideal, assegure que um extra de 2-3 vezes do espaço em disco mínimo esteja disponível.

Tabela 6. Requisitos para Dispositivos Virtuais (continuação)

Requisito	Descrição
Tamanho do disco virtual para dispositivos do QRadar QFlow Collector	Mínimo: 70 GB
Tamanho do disco virtual para dispositivos do QRadar Risk Manager	Tamanho de disco virtual sugerido para implementação com até 10000 fontes de configuração: 1 TB.
Tamanho do disco virtual para dispositivos de processador QRadar Vulnerability Manager	50000 IPs - 500 GB 150000 IPs - 750 GB 300000 IPs - 1 TB
Tamanho do disco virtual para dispositivos de scanner QRadar Vulnerability Manager	20000 IPs - 150 GB

A tabela a seguir descreve os requisitos mínimos de memória para dispositivos virtuais.

Tabela 7. Requisitos de Memória Mínimos e Opcionais para Dispositivos Virtuais QRadar

Dispositivo	Requisito Mínimo de Memória	Requisito Sugerido de Memória
QRadar VFlow Collector 1299	6 GB	6 GB
QRadar Event Collector Virtual 1599	12 GB	16 GB
QRadar SIEM Event Processor Virtual 1699	12 GB	48 GB
QRadar SIEM Flow Processor Virtual 1799	12 GB	48 GB
QRadar SIEM All-in-One Virtual 3199	24 GB	48 GB
QRadar Log Manager Virtual 8090	24 GB	48 GB
QRadar Risk Manager	24 GB	48 GB
Processador QRadar Vulnerability Manager	8 GB	16 GB
Scanner QRadar Vulnerability Manager	2 GB	4 GB

Tarefas relacionadas:

"Criando sua Máquina Virtual" na página 25
Para instalar um dispositivo virtual, deve-se primeiro usar o VMWare ESX para criar umamáquina virtual.

Criando sua Máquina Virtual

Para instalar um dispositivo virtual, deve-se primeiro usar o VMWare ESX para criar umamáquina virtual.

Procedimento

1. A partir do VMware vSphere Client, clique em **Arquivo** > **Novo** > **Máquina Virtual**.
2. Inclua o **Nome e a Localização** e selecione o **Armazenamento de Dados** para a nova máquina virtual.
3. Use as etapas a seguir para guiá-lo pelas opções:
   a. Na área de janela **Configuração** da janela Criar Nova Máquina Virtual, selecione **Customizado**.
   b. Na área de janela **Versão da Máquina Virtual**, selecione **Versão da Máquina Virtual: 7**.
   c. Para o **Sistema operacional**, selecione **Linux** e depois selecione **Red Hat Enterprise Linux 6 (64 bits)**.
   d. Na página **CPUs**, configure o número de processadores virtuais que você deseja para a máquina virtual:

      A tabela a seguir fornece exemplos de configurações da página **CPU** que você pode utilizar com base no desempenho dos dispositivos IBM Security QRadar.

Tabela 8. Configurações da Página **CPU** *de Amostra*

Número de Processadores	**Desempenho baseado em dispositivos QRadar**
4	Gerenciador de log 3190: 2500 eventos por segundo ou menos. Processador de Eventos do Gerenciador de Log 1690 ou Processador de Eventos SIEM 1690: 2500 eventos por segundo ou menos Multifuncional 3190: 25000 fluxos por minuto ou menos, 500 eventos por segundo ou menos Processador de Fluxo 1790: 150.000 fluxos por minuto. Console Dedicado 3190
8	Gerenciador de log 3190: 5000 eventos por segundo ou menos. Processador de Eventos do Gerenciador de Log 1690 ou Processador de Eventos SIEM 1690: 5000 eventos por segundo ou menos Multifuncional 3190: 50000 fluxos por minuto ou menos, 1000 eventos por segundo ou menos Processador de Fluxo 1790: 300.000 fluxos por minuto.
12	Multifuncional 3190: 100.000 fluxos por minuto ou menos, 1000 eventos por segundo ou menos.
16	Processador de Eventos do Gerenciador de Log 1690 ou Processador de Eventos SIEM 1690: 20.000 eventos por segundo ou menos Multifuncional 3190: 200.000 fluxos por minuto ou menos, 5000 eventos por segundo ou menos.

   e. No campo **Tamanho da Memória**, digite ou selecione 24 ou mais.
   f. Utilize a tabela a seguir para configurar suas conexões de rede.

Tabela 9. Descrições para Parâmetros de Configuração de Rede

Parâmetro	Descrição
Quantos NICs você deseja conectar	Você deve incluir pelo menos um Controlador de Interface de Rede (NIC)
Adaptador	`VMXNET3`

g. Na área de janela **Controlador SCSI**, selecione **VMware Paravirtual**.
h. Na área de janela **Disco**, selecione **Criar um novo disco virtual** e utilize a tabela a seguir para configurar os parâmetros de disco virtual.

Tabela 10. Configurações para o Tamanho do Disco Virtual e Parâmetros da Política de Fornecimento

Propriedade	Opção
Capacidade	256 ou superior (GB)
Fornecimento de Disco	Thin provision
Opções Avançadas	Não Configurar

4. Na página **Pronto para Concluir**, revise as configurações e clique em **Concluir**.

Instalando o Software QRadar em uma Máquina Virtual

Depois de criar sua máquina virtual, você deve instalar o software IBM Security QRadar na máquina virtual.

Antes de Iniciar

Assegure que a chave de ativação esteja prontamente disponível.

Procedimento

1. Na área de janela de navegação à esquerda de seu VMware vSphere Client, selecione sua máquina virtual.
2. Na área de janela direita, clique na guia **Resumo**.
3. Na área de janela **Comandos**, clique em **Editar Configurações**.
4. Na área de janela esquerda da janela **Propriedades da Máquina Virtual**, clique em **Unidade 1 de CD/DVD**.
5. No painel **Tipo de dispositivo**, selecione **Arquivo ISO de armazenamento de dados**.
6. Na área de janela **Status do Dispositivo**, selecione a caixa de seleção **Conectar com energia ligada**.
7. Na área de janela **Tipo de dispositivo**, clique em **Procurar**.
8. Na janela Procurar Armazenamentos de Dados, localize e selecione o arquivo ISO do produto QRadar, clique em **Abrir** e, em seguida, clique em **OK**.
9. Após a imagem ISO do produto QRadar ser instalada, clique com o botão direito do mouse em sua máquina virtual e clique em **Energia** > **Ligar.**
10. Efetue login na máquina virtual digitando `root` para o nome de usuário.
    O nome de usuário faz distinção entre maiúsculas e minúsculas.
11. Assegure que End User License Agreement (EULA) seja exibido.

    Dica: Pressione a tecla Barra de Espaço para avançar através do documento.
12. Para o tipo de configuração, selecione **normal**.

13. Para instalações do QRadar Console, selecione o modelo ajuste **Corporativo**.
14. Siga as instruções no assistente de instalação para concluir a instalação.

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

Tarefas relacionadas:

"Criando sua Máquina Virtual" na página 25
Para instalar um dispositivo virtual, deve-se primeiro usar o VMWare ESX para criar umamáquina virtual.

Incluindo seu Dispositivo Virtual para sua Implementação

Depois de o software IBM Security QRadar ser instalado, inclua o dispositivo virtual em sua implementação.

Procedimento

1. Efetue login no QRadar Console.
2. Na guia **Administração**, clique no ícone **Editor de Implementação**.
3. Na área de janela **Componentes de Evento** na página **Visualização de Eventos**, selecione o componente do dispositivo virtual que você deseja incluir.
4. Na primeira página do assistente de tarefa **Incluindo um Novo Componente**, digite um nome exclusivo para o dispositivo virtual.

   O nome que você designa para o dispositivo virtual pode ter até 20 caracteres de comprimento e pode incluir sublinhados ou hifens.
5. Conclua as etapas no assistente de tarefas.
6. A partir do menu**Editor de Implementação**, clique em **Arquivo** > **Salvar para Preparação**.
7. No menu da guia **Admin**, clique em **Implementar Mudanças**.
8. 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**.

Tarefas relacionadas:

"Criando sua Máquina Virtual" na página 25
Para instalar um dispositivo virtual, deve-se primeiro usar o VMWare ESX para criar umamáquina virtual.

Capítulo 5. Instalações a Partir da Partição de Recuperação

Ao instalar produtos IBM Security QRadar, o instalador (imagem ISO) é copiado para a partição de recuperação. A partir desta partição, é possível reinstalar produtos QRadar. Seu sistema é restaurado de volta para a configuração padrão. Sua configuração atual e os arquivos de dados são sobrescritos

Quando você reinicia o dispositivo do QRadar, uma opção para reinstalar o software é exibida. Se não responder ao aviso em 5 segundos, o sistema continuará a ser iniciado normalmente. Seus arquivos de configuração e de dados são mantidos. Se você escolher a opção de reinstalação, uma mensagem de aviso será exibida e você deverá confirmar que deseja reinstalar.

A mensagem de aviso informa que você pode reter os dados no dispositivo. Esses dados incluem eventos e fluxos. A seleção da opção de retenção faz backup dos dados antes da reinstalação e restaura os dados após a instalação ser concluída. Se a opção de retenção não estiver disponível, a partição onde residem os dados poderá não estar disponível e não será possível fazer backup e restaurar os dados. A ausência da opção de retenção pode indicar uma falha no disco rígido. Entre em contato com Suporte ao Cliente se a opção de retenção não estiver disponível.

Importante: A opção de retenção não está disponível nos sistemas de Alta Disponibilidade. Consulte o *IBM Security QRadar High Availability Guide* para obter informações sobre recuperação de dispositivos de Alta Disponibilidade.

Todos os upgrades de software de QRadar Versão 7.2.0 substituem o arquivo ISO existente pela versão mais recente.

Essas diretrizes se aplicam às novas instalações ou upgrades do QRadar Versão 7.2.0 a partir de novas instalações do QRadar versão 7.0 nos dispositivos QRadar versão 7.0.

Reinstalando a partir da partição de recuperação

É possível reinstalar os produtos IBM Security QRadar a partir da partição de recuperação.

Antes de Iniciar

Localize sua chave de ativação. A chave de ativação é uma sequência alfanumérica de 24 dígitos, com quatro partes, que você recebe da IBM. É possível localizar a chave de ativação em um dos seguintes locais:

- Impresso em uma etiqueta e colocado fisicamente em seu dispositivo.
- Incluído com o código da embalagem; todos os dispositivos são listados juntamente com suas chaves associadas.

Se você não tiver sua chave de ativação, acesse o website de Suporte IBM (www.ibm.com/support) para obter sua chave de ativação. Você deve fornecer o número de série do dispositivo QRadar. As chaves de ativação de software não requerem números de série.

Se sua implementação incluir soluções de armazenamento não integrado, você deverá desconectar o seu armazenamento não integrado antes de reinstalar o QRadar. Depois de reinstalar, você pode remontar suas soluções de armazenamento externo. Para obter mais informações sobre a configuração de armazenamento não integrado, consulte o *Offboard Storage Guide*.

Procedimento

1. Reinicie seu dispositivo QRadar e selecione **Reinstalação de Fábrica**.
2. Digite `flatten` ou `retain`.

   O instalador particiona e reformata o disco rígido, instala o sistema operacional e, em seguida, reinstala o produto QRadar. Você deve aguardar a conclusão do processo de compressão ou de retenção. Esse processo pode demorar alguns minutos. Quando o processo for concluído, uma confirmação será exibida.
3. Digite `SETUP`.
4. Efetue login como o usuário raiz.
5. Assegure que End User License Agreement (EULA) seja exibido.

   Dica: Pressione a tecla Barra de Espaço para avançar através do documento.
6. Para instalações do QRadar Console, selecione o modelo ajuste **Corporativo**.
7. Siga as instruções no assistente de instalação para concluir a instalação.
8. 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**.

Capítulo 6. Configurando as instalações silenciosas para o QRadar

Instale o IBM Security QRadar "silenciosamente" ou execute uma instalação não assistida.

Antes de Iniciar

Esta instalação requer o sistema operacional do Red Hat Enterprise Linux e o ISO do QRadar V7.2.5. Para obter informações sobre os números de versão e requisitos, consulte Capítulo 3, “Instalações de Software QRadar em seu Próprio Dispositivo”, na página 15.

Procedimento

1. Instale o RHEL no host em que deseja instalar o QRadar para configurar as partições necessárias. Para obter mais informações, consulte “Instalando o RHEL em seu Próprio Dispositivo” na página 18.
2. Como o usuário raiz, use o SSH para efetuar logon no host em que deseja instalar o QRadar.
3. No host em que deseja instalar o QRadar, acesse o diretório-raiz e crie um arquivo chamado `AUTO_INSTALL_INSTRUCTIONS` e que contenha as informações a seguir:

   Exemplo: O exemplo de arquivo AUTO_INSTALL_INSTRUCTIONS a seguir mostra os parâmetros corretos para a instalação silenciosa do QRadar no fuso horário da América/Moncton.

   ```
   timezone=America/Moncton
   sectempl=Enterprise
   date=2015/05/19
   ntpserver=q1dc04.canlab.ibm.com
   ntpsync=1
   timechoice=manual
   nicid=eth0
   box_ip=1.2.3.4
   ip_v6=
   netmask=255.255.255.255
   ipverchoice=ipv4
   gateway_v6=
   hostname=name
   pdns=1.2.3.4
   bdns=5.6.7.8
   newkey=######-######-######-######
   defpass=password
   isconsole=yes
   setuptypechoice=normal
   is_ha_appl=0
   isconstandby=yes
   smtpname=localhost
   bonding_interfaces=
   bonding_options=
   bonding_enabled=false
   ```

   Importante: O arquivo `AUTO_INSTALL_INSTRUCTIONS` não deve ter extensões.

   Saiba mais sobre instalações silenciosas:

Tabela 11. Parâmetros do arquivo de instalação silenciosa

Parâmetro	Obrigatório?	Descrição	Valores permitidos
setuptypechoice	Obrigatório	Especifica o tipo de instalação para este host	normal- Um host gerenciado pelo QRadar padrão ou implementação de console. recuperação - Uma instalação de recuperação de alta disponibilidade (HA) neste host.
fuso horário	Obrigatório	O fuso horário a partir do banco de dados TZ. Para obter mais informações, consulte http://timezonedb.com/.	Europa/Londres América/Montreal América/New_York América/Los_Angeles Ásia/Tokyo e assim por diante.
data	Obrigatório	A data atual para este host. Use o formato a seguir: formato DD/MM/AAAA	
Escolha de horário	Obrigatório	Especifica como este host obtém o horário atual	manual - o horário inserido manualmente no parâmetro de horário. servidor - Use um servidor do Network Time Protocol (NTP) especificado pelo parâmetro ntpserver
horário	Se escolha de horário estiver configurado como manual, então é obrigatório.	O horário para o host no formato de 24 horas HH:MM:SS.	
ntpserver	Se escolha de horário estiver configurado como servidor, então é obrigatório.	O FQHN ou o endereço IP do servidor do protocolo de tempo de rede (NTP).	

Tabela 11. Parâmetros do arquivo de instalação silenciosa (continuação)

Parâmetro	Obrigatório?	Descrição	Valores permitidos
ntpsync	Se escolha de horário estiver configurado como servidor, então é obrigatório.	Insira 1 para sincronizar com o servidor NTP, caso contrário, insira 0.	
nicid	Obrigatório	O identificador para a placa da interface de rede	Valores: eth0, eth1, eth*x*
management_iface	Obrigatório	O identificador para a interface de gerenciamento	Valores: eth0, eth1, eth*x*
nome do host	Opcional	O nome completo do host para o sistema QRadar.	
ipverchoice	Obrigatório	Especifica o protocolo IP padrão para este host	IPv4, IPv6
box_ip	Se ipverchoice estiver configurado como IPv4, então é obrigatório	O endereço IP do host em que está instalando o software	Um endereço IPv4 válido
ip_v6	Se ipverchoice estiver configurado como IPv6, então é obrigatório	Insira o endereço IPv6 para a instalação do QRadar se necessário.	Um endereço IPv6 válido
máscara de rede	Se ipverchoice estiver configurado como IPv4, então é obrigatório	A máscara de rede para este host	
gateway	Se ipverchoice estiver configurado como IPv4, então é obrigatório	O gateway de rede para este host	Um endereço IPv4 válido
gateway_v6	Se ipverchoice estiver configurado como IPv6, então é obrigatório	O gateway de rede para este host	Um endereço IPv6 válido

Tabela 11. Parâmetros do arquivo de instalação silenciosa (continuação)

Parâmetro	Obrigatório?	Descrição	Valores permitidos
`ip_v6_nocidr`	Opcional	O endereço IPv6 sem nenhum Classless Inter-Domain Routing (CIDR)	Um endereço IPv6 válido
`pdns`	Se `ipverchoice` estiver configurado como `IPv4`, então é obrigatório	O servidor DNS primário.	Um endereço IPv4 válido
`bdns`	Se `ipverchoice` estiver configurado como `IPv4`, então é obrigatório	O servidor DNS secundário.	Um endereço IPv4 válido
`newkey`	Obrigatório	A chave de ativação para a instalação do QRadar.	
`defpass`	Obrigatório	A senha raiz padrão a usar para esse host.	
`isconsole`	Obrigatório	Especifique se este host é o console dentro da implementação	`Y` - Este host é o console na implementação `N` - Este não é o console e é um outro tipo de host gerenciado (Evento ou Processador de fluxo e assim por diante)
`sectempl`	Se `isconsole` estiver configurado como `Y`, então é obrigatório	O modelo de segurança.	`Corporativo` - para todos os hosts baseados em SIEM `Criador de logs` - para o Log Manager
`is_ha_appl`	Obrigatório	Especifique se este host é um par HA ou host de lembrete	`0` - Este host não é um aplicativo/uma instalação de HA `1` - Este host é um aplicativo/uma instalação de HA
`isconstandby`	Se `isconsole` estiver configurado como `Y`, então é obrigatório.	Especifique se este host é um console de HA de espera	`0` - Este host não é um console de HA de espera `1` - Este host é um console de HA de espera
`clusterip`	Opcional	Especifica o endereço IP para o cluster de alta disponibilidade (HA).	`ip_address`

Tabela 11. Parâmetros do arquivo de instalação silenciosa (continuação)

Parâmetro	Obrigatório?	Descrição	Valores permitidos
`smtpname`	Obrigatório	Insira o servidor de correio ou o nome SMTP, como um host local.	
`bond _interfaces`	Se estiver usando interfaces de ligação, então, será necessário.	Os endereços MAC para as interfaces que você estiver ligando, separados por vírgulas.	`mac_addresses`
`bonding_options`	Se estiver usando interfaces de ligação, então, será necessário.	As opções Linux para interfaces de ligação.	**Exemplo:** `miimon=100 mode=4 lacp_rate=1`
`ligação ativada`	Se estiver usando interfaces de ligação, então, será necessário.	Especifica se você está usando interfaces de ligação.	`true` ou `false`

4. Usando um programa de Protocolo de Transferência de Arquivos Segura (SFTP), como WinSCP, copie o ISO do QRadar para o host em que deseja instalar o QRadar.
5. Usando um programa como o WinSCP, copie o ISO do RHEL para o host em que deseja instalar o QRadar.
6. Crie um diretório `/media/cdrom` usando o comando a seguir:
   ```
   mkdir /media/cdrom
   ```
7. Crie um diretório `/media/redhat` usando o comando a seguir:
   ```
   mkdir /media/redhat
   ```
8. Monte o ISO do QRadar usando o comando a seguir:
   ```
   mount -o loop <qradar.iso> /media/cdrom
   ```
9. Monte o ISO do RHEL usando o comando a seguir:
   ```
   mount -o loop <RHEL.iso> /media/redhat
   ```
10. Execute a configuração do QRadar usando o comando a seguir:
    ```
    /media/cdrom/setup
    ```

Capítulo 7. Visão geral da implementação do QRadar em um ambiente de nuvem

É possível instalar instâncias do software IBM Security QRadar em um servidor em nuvem que é hospedado pelo Amazon Web Service. Para estabelecer comunicações seguras entre instâncias on-premises e da nuvem do QRadar, deve-se configurar uma conexão VPN. É possível configurar uma conexão OpenVPN ou usar um outro mecanismo, como uma infraestrutura de VPN de provedor em nuvem.

Importante: Assegure-se de que os requisitos a seguir sejam atendidos para evitar dados de segurança comprometidos:

- Configure uma senha raiz forte.
- Permita somente conexões específicas para as portas 443 (https), 22 (ssh), 10000 (webmin) e 1194 (UDP, TCP for OpenVPN).

Configure o QRadar para a nuvem na ordem a seguir:

1. Instale o QRadar no AWS: para obter mais informações, veja Configurando um host do QRadar no Amazon Web Service (http://www.ibm.com/support/docview.wss?uid=swg27044417).
2. Para hosts em nuvem e on-premises, defina a função:
   - O end point do servidor de um túnel VPN.
   - O endpoint do cliente de um túnel VPN.
   - O host do membro que roteia o tráfego que é destino ao túnel VPN por meio do endpoint de VPN local.
   - Nenhuma, se um host não tiver necessidade de se comunicar com os hosts no outro lado do túnel VPN.
3. Confirme se as configurações de firewall do QRadar protegem sua segurança de rede.

Configurando end points do servdior para instalações em nuvem

Use o OpenVPN para configurar um end point do servidor no servidor em nuvem, quando o console do IBM Security QRadar estiver em instalações, com mais nós de processamento e armazenamento instalados na nuvem.

Sobre Esta Tarefa

Um end point do servidor requer os itens a seguir:

- Um arquivo de configuração principal do OpenVPN.
- Instruções de roteamento para cada cliente no arquivo de configuração do servidor.
- Um arquivo de configuração para cada cliente que registra instruções de roteamento para cada cliente que pode se conectar.
- Regras adicionais de iptables que permitem encaminhamento através do túnel.
- Encaminhamento de IP ativado no kernel.
- Uma autoridade de certificação (CA) customizada para emitir os certificados que são usados para autenticar servidores e clientes.
- Um certificado do servidor que é emitido pela autoridade de certificação local.

Para obter mais informações sobre as opções da ferramenta OpenVPN, insira `-h`.

Procedimento

1. Para especificar o end point do servidor, digite o comando a seguir para definir o end point do servidor na nuvem.

   ```
   /opt/qradar/bin/vpntool server server_host_IP_address network_address_behind_VPN
   ```

   Exemplo:

   ```
   /opt/qradar/bin/vpntool server 1.2.3.4 5.6.7.8/24
   ```

   Se sua rede requerer TCP em vez do modo UDP em seus clientes e servidores, digite o comando a seguir com seus endereços IP requeridos:

   ```
   /opt/qradar/bin/vpntool server server_host_IP_address
    network_address_behind_VPN --tcp
   ```

   Depois que você define o end point do servidor, o VPNtool Server conclui as tarefas a seguir:

   - Se a autoridade de certificação local não estiver estabelecida, a autoridade de certificação será inicializada e a chave e o certificado de autoridade de certificação criados.
   - A autoridade de certificação local cria uma chave e um certificado para serem usados por esse end point do servidor.
   - As propriedades de configuração são gravadas no arquivo de configuração da VPN.
2. Para construir e implementar a configuração, digite o comando a seguir:

   ```
   /opt/qradar/bin/vpntool deploy
   ```

   Após construir e implementar a configuração, o VPNtool Server conclui as tarefas a seguir:

   - A configuração do servidor OpenVPN é gerada e copiada para o diretório `/etc/openvpn`.
   - O certificado de autoridade de certificação e a chave e o certificado do servidor são copiados para o local padrão em `/etc/openvpn/pki`.
   - As regras de IPtables são construídas e recarregadas.
   - O encaminhamento de IP é ativado e tornado persistente atualizando o arquivo `/etc/sysctl.conf`.
3. Para iniciar o servidor, digite o comando a seguir:

   ```
   /opt/qradar/bin/enable --now
   ```

   Inserir `/opt/qradar/bin/enable --now` cria o estado persistente ativado e inicia automaticamente o OpenVPN na reinicialização do sistema.

Configurando redes de clientes para instalações em nuvem

Nos ambientes em instalações, use o OpenVPN para configurar uma rede de clientes que se comunicam com endpoints que estão na nuvem.

Sobre Esta Tarefa

Um cliente requer os itens a seguir:

- Um arquivo de configuração principal do OpenVPN.
- Regras extras de iptables para permitir encaminhamento através do túnel.
- O encaminhamento de IP está ativado no kernel.
- Um certificado de cliente que é emitido pela autoridade de certificação local.

Procedimento

1. No servidor, informe o servidor do novo cliente, digite o comando a seguir:

   ```
   /opt/qradar/bin/vpntool addclient Console name, role, or IP  1.2.3.4/24
   ```

   Informar o servidor do cliente inclui as tarefas a seguir:

   - O certificado de autoridade de certificação é copiado para um local conhecido.
   - A chave e o certificado do cliente do arquivo PKCS#12 são extraídos e copiados para locais conhecidos.
   - As propriedades de configuração do cliente são gravadas no arquivo de configuração da VPN.

2. Implemente e reinicie o servidor usando o comando a seguir:

   ```
   /opt/qradar/bin/vpntool deploy
   service openvpn restart
   ```

3. Copie o arquivo de credenciais do cliente gerado e o arquivo de autoridade de certificação para o host do QRadar que é usado para esse endpoint do cliente.

   Exemplo:

   ```
   scp root@ server_IP_address :/opt/qradar/conf
   /vpn/pki/ca.crt /root/ca.crtscp root@ server_IP_address
   :/opt/qradar/conf/vpn/pki/Console.p12 /root/Console.p12
   ```

4. No cliente, configure o host como um cliente de VPN:

   ```
   /opt/qradar/bin/vpntool client server_IP_address ca.crt client.pk12
   ```

   Se a sua rede requer que o modo UDP não seja configurado em seus clientes e servidores, é possível usar TCP.

   ```
   /opt/qradar/bin/vpntool client server_IP_address /root/ca.crt /root/Console.p12 --tcp
   ```

5. Para construir e implementar a configuração, digite o comando a seguir:

   ```
   /opt/qradar/bin/vpntool deploy
   ```

   Construir e implementar a configuração inclui as seguintes etapas:

   - O arquivo de configuração do OpenVPN do cliente é gerado e copiado no local em `/etc/openvpn`.
   - O certificado de autoridade de certificação e a chave e o certificado de cliente são copiados para os locais padrão em `/etc/openvpn/pki`.
   - Regras de iptables são geradas e carregadas.
   - O encaminhamento de IP é ativado e tornado persistente atualizando o arquivo `/etc/sysctl.conf`.

6. Para iniciar o cliente, insira o comando a seguir:

   ```
   /opt/qradar/bin/enable --now
   ```

   Inserir `/opt/qradar/bin/enable --now` cria o estado persistente ativado e inicia automaticamente o OpenVPN na reinicialização do sistema.

7. Para conectar o cliente por meio de um proxy HTTP, insira o comando a seguir:

   ```
   /opt/qradar/bin/vpntool client IP Address  /root/ca.crt
    /root/Console.p12 --http-proxy= IP Address:port
   ```

   - A configuração de proxy está sempre no modo TCP, mesmo se você não inserir TCP no comando.
   - Consulte a documentação do OpenVPN para obter as opções de configuração para autenticação de proxy. Inclua estas opções de configuração no arquivo a seguir:

     ```
     /etc/openvpn/client.conf
     ```

Configurando um membro para instalações em nuvem

Use o OpenVPN para estabelecer conexões seguras para hosts do IBM Security QRadar que não são servidores ou clientes.

Procedimento

Para associar um host do QRadar SIEM à VPN local, para que se comunique diretamente com hosts no outro lado do túnel, usando o comando a seguir:

```
/opt/qradar/bin/vpntool join local_host_IP_address remote host IP address
/opt/qradar/bin/vpntool deploy
```

Capítulo 8. Visão geral do nó de dados

Entenda como usar Nós de dados na sua implementação do IBM Security QRadar.

Os Nós de dados permitem que implementações novas e existentes do QRadar incluam capacidade de armazenamento e processamento sob demanda conforme o necessário.

Os usuários podem dimensionar capacidade de armazenamento e processamento independentemente de cota de dados, o que resulta em uma implementação com a capacidade de armazenamento e processamento adequada. Nós de dados são do tipo plug-n-play e podem ser incluídos em uma implementação a qualquer momento. Os Nós de dados integram-se sem interrupções à implementação existente.

Volumes de dados crescentes nas implementações exigem que a compactação de dados ocorra mais cedo. A compactação de dados desacelera o desempenho do sistema, uma vez que o sistema precisa descompactar dados consultados antes de poder analisá-los. Incluir dispositivos de Nós de dados a uma implementação permite manter dados não compactados por mais tempo.

A implementação do QRadar distribui todos os novos dados através dos processadores de Fluxo e Evento e os Nós de dados conectados.

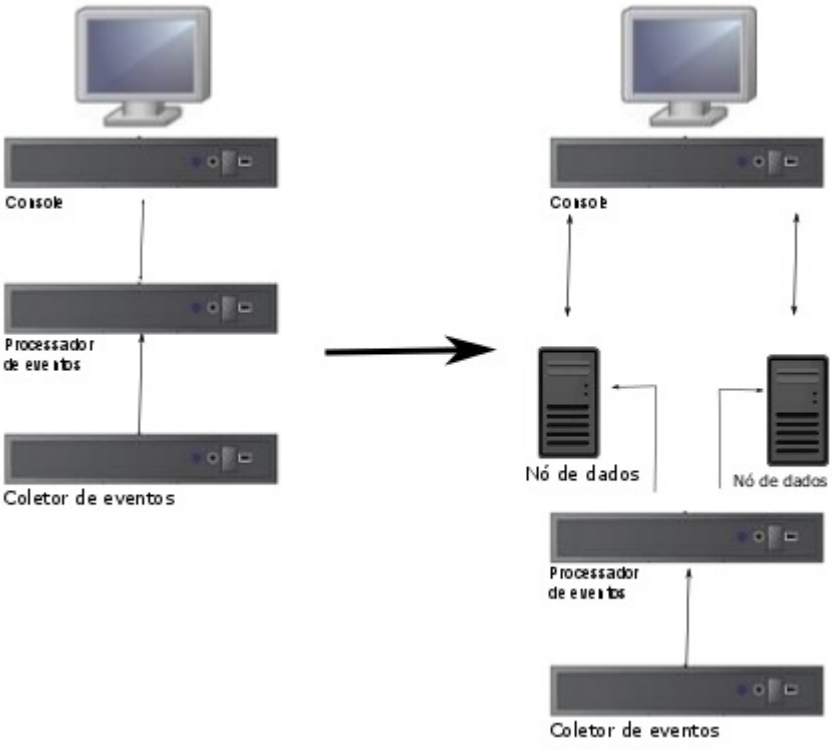

Figura 2. Implementação do QRadar antes e depois de incluir dispositivos de Nós de dados

Armazenamento em cluster

Nós de dados incluem capacidade a uma implementação, mas também melhoram o desempenho distribuindo os dados em toda a implementação. As consultas são executadas por muitos hosts, usando os recursos do sistema de todo o cluster. O armazenamento em cluster permite procuras muito mais rápidas que em uma abordagem não agrupada.

Considerações de implementação

- Os Nós de dados estão disponíveis no QRadar 7.2.2 e posteriores
- Nós de dados realizam pesquisa e funções analíticas similares a de processadores de Eventos e Fluxo em uma implementação do QRadar. As operações em um cluster são afetadas pelo membro mais lento de um cluster. O desempenho do sistema de Nó de dados melhora se os Nós de dados tiverem tamanhos similares aos dos processadores de eventos e fluxos em uma implementação. Para facilitar o dimensionamento semelhante entre Nós de dados e processadores de eventos e fluxos, os Nós de dados estarão disponíveis nos dispositivos centrais XX05 e XX28.
- Os Nós de dados estão disponíveis em três formatos: Software (no seu próprio hardware), Físico e Dispositivos. É possível combinar os formatos em um único cluster.

Largura da banda e latência

Assegure um link de 1 Gbps link e menos de 10 ms entre os hosts no cluster.

Compatibilidade

Nós de dados são compatíveis com todos os dispositivos QRadar existentes que possuem um componente de Processador de Eventos ou Fluxos, incluindo os dispositivos All-In-One. Os Nós de dados não são compatíveis com dispositivos QRadar Incident Forensics PCAP.

Nós de dados têm suporte para alta disponibilidade (HA).

Instalação

Nós de dados usam rede TCP/IP padrão e não exigem hardware de interconexão proprietário ou especializado. Instale cada Nó de dados que desejar incluir à sua implementação como instalaria qualquer outro dispositivo QRadar. Associe Nós de dados a processadores de eventos ou fluxos no Editor de Implementação do QRadar. Consulte o *Guia de Administração do IBM Security QRadar*.

É possível conectar vários Nós de dados a um único Processador de eventos ou fluxo em uma configuração de muitos para um.

Ao implementar pares de alta disponibilidade com dispositivos de Nó de dados, instale, implemente e rebalanceie os dados com dispositivos de Alta Disponibilidade antes de sincronizar o par de alta disponibilidade. O efeito combinado de rebalanceamento de dados e o processo de replicação usado para alta disponibilidade resulta em degradação significativa do desempenho. Se houver alta disponibilidade nos dispositivos existentes aos quais os Nós de dados estão sendo introduzidos, também é preferível que a conexão de alta disponibilidade seja interrompida e restabelecida quando o rebalanceamento do cluster tiver sido concluído.

Desatribuição

Remova os Nós de dados da sua implementação com o Editor de Implementação, como com qualquer outro dispositivo QRadar. A desatribuição não apaga dados balanceados no host. É possível recuperar os dados para arquivamento e redistribuição.

Rebalanceamento de dados

Incluir um Nó de dados a um cluster distribui os dados uniformemente para cada Nó de dados. Cada dispositivo de Nó de dados mantém a mesma percentagem de espaço disponível. Novos Nós de dados incluídos a um cluster iniciam o rebalanceamento inicial de processadores de fluxos e eventos do cluster para atingir um uso de disco eficiente em dispositivos de Nó de dados recém-incluídos.

A partir do QRadar 7.2.3, o rebalanceamento de dados é automático e simultâneo a outras atividades do cluster, como consultas e coleta de dados. Não há tempo de inatividade durante o rebalanceamento de dados.

Os Nós de dados não oferecem melhoria de desempenho no cluster até o rebalanceamento de dados ser concluído. O rebalanceamento pode causar uma pequena degradação de desempenho durante operações de procura, mas a coleta de dados e o processamento continuam sem serem afetados.

Gerenciamento e operações

Os Nós de dados são autogerenciados e não exigem intervenção do usuário regular para a manutenção da operação normal. O QRadar gerencia atividades, como backups de dados, políticas de retenção e de alta disponibilidade, para todos os hosts, incluindo dispositivos de Nó de dados.

Falhas

Se um Nó de dados falhar, os membros restantes do cluster continuam a processar dados.

Quando o Nó de dados com falha retornar ao serviço, o balanceamento de dados poderá ocorrer para manter a distribuição de dados adequada no clustere, então, o processamento normal continuará. Durante o tempo de inatividade, os dados no Nó de dados com falha ficam indisponíveis.

Para falhas catastróficas que exigem troca do dispositivo ou reinstalação de QRadar, desatribua os Nós de dados da implementação e substitua-os usando etapas de instalação padrão. Copie quaisquer dados que não tenham sido perdidos na falha para o novo Nó de dados antes da implementação. O algoritmo de rebalanceamento responde por dados existentes em um nó de dados e ordena aleatoriamente somente os dados coletados durante a falha.

Para Nós de dados implementados com um par de alta disponibilidade, uma falha de hardware causa um failover, e as operações continuam funcionando normalmente.

Conceitos relacionados:

"Componentes do QRadar" na página 2
IBM Security QRadar consolida os dados do evento a partir de origens de log que são utilizadas pelos dispositivos e aplicativos em sua rede.

Capítulo 9. 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.

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 12. 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).
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 13. 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
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`.

Capítulo 10. Resolução de Problemas

A resolução de problemas é uma abordagem sistemática para resolver um problema. O objetivo da resolução de problemas é determinar por que algo não funciona conforme o esperado e como resolver o problema.

Revise a tabela a seguir para ajudar você ou o suporte ao cliente a resolver um problema.

Tabela 14. Ações de Resolução de Problemas para Evitar Problemas

Ação	Descrição
Aplicar todos os fix packs, níveis de serviço ou correções temporárias de programa (PTF) conhecidos.	Uma correção de produtos pode estar disponível para corrigir o problema.
Assegurar que a configuração seja suportada.	Revise os requisitos de software e hardware.
Consultar os códigos de mensagem de erro selecionando o produto a partir do IBM Support Portal (http://www.ibm.com/support/entry/portal) e, em seguida, digitando o código de mensagem de erro na caixa **Suporte de Procura**.	As mensagens de erro fornecem importantes informações para ajudar a identificar o componente que está causando o problema.
Reproduza o problema para assegurar que não seja apenas um erro simples.	Se as amostras estiverem disponíveis com o produto, você poderá tentar reproduzir o problema usando os dados da amostra.
Verifique as permissões de arquivo e estrutura do diretório de instalação.	O local da instalação deve conter a estrutura do arquivo apropriada e as permissões de arquivo. Por exemplo, se o produto precisar de acesso de gravação para os arquivos de log, certifique-se de que o diretório tenha a permissão correta.
Revise a documentação relevante, como notas sobre a liberação, notas técnicas e documentação de práticas comprovadas.	Procure nas bases de conhecimento IBM para determinar se o seu problema é conhecido, possui uma solução alternativa ou se já está resolvido e documentado.
Revise as mudanças recentes no seu ambiente de computação.	Às vezes, a instalação do novo software pode causar problemas de compatibilidade.

Se você ainda precisar resolver problemas, deverá coletar dados de diagnóstico. Esses dados são necessários para que um representante de suporte técnico da IBM solucione problemas de forma efetiva e o ajude na resolução do problema. Também é possível coletar os dados diagnósticos e analisá-los sozinho.

Conceitos relacionados:

"Componentes do QRadar" na página 2
IBM Security QRadar consolida os dados do evento a partir de origens de log que são utilizadas pelos dispositivos e aplicativos em sua rede.

Recursos de Resolução de Problemas

Os recursos de resolução de problemas são fontes de informações que podem ajudar a resolver um problema que você tem com um produto. Muitos dos links de recursos fornecidos também podem ser visualizados em um curto vídeo de demonstração.

Para visualizar a versão em vídeo, procure por "resolução de problemas" por meio de um mecanismo de procura no Google ou na comunidade de vídeo do YouTube.

Conceitos relacionados:

"Arquivos de Log do QRadar" na página 51
Utilize os arquivos de log do IBM Security QRadar para ajudar a resolver problemas.

Support Portal

O IBM Support Portal é uma visualização unificada, centralizada de todas as ferramentas de suporte técnico e informações para todos os sistemas, softwares e serviços IBM.

Utilize o IBM Support Portal para acessar todos os recursos de suporte IBM a partir de um único local. É possível ajustar as páginas para se concentrar nas informações e recursos necessários para a prevenção de problemas e a resolução de problemas mais rápida. Familiarize-se com o IBM Support Portal visualizando os vídeos demo (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos).

Localize o conteúdo do IBM Security QRadar necessário selecionando seus produtos a partir do IBM Support Portal (http://www.ibm.com/support/entry/portal).

Solicitações de Serviço

As solicitações de serviço também são conhecidas como Problem Management Records (PMRs). Existem diversos métodos para submeter as informações de diagnóstico ao Suporte Técnico do Software IBM.

Para abrir uma solicitação de serviço, ou para trocar informações com o suporte técnico, visualize a página do Suporte ao Software IBM, Trocando Informações com o Suporte Técnico (http://www.ibm.com/software/support/exchangeinfo.html). As solicitações de serviço também podem ser enviadas diretamente utilizando a ferramenta de Solicitações de Serviço (PMRs) (http://www.ibm.com/support/entry/portal/Open_service_request) ou um dos outros métodos suportados que estão detalhados na página de troca de informações.

Fix Central

Fix Central fornece correções e atualizações para seu software do sistema, hardware e sistema operacional.

Utilize o menu suspenso para acessar as correções de seu produto no Fix Central (http://www.ibm.com/support/fixcentral). Você também pode desejar visualizar Introdução ao Fix Central (http://www.ibm.com/systems/support/fixes/en/fixcentral/help/getstarted.html).

Bases de Conhecimento

Geralmente você encontra soluções para problemas procurando nas bases de conhecimento da IBM. É possível otimizar os resultados usando recursos disponíveis, ferramentas de suporte e métodos de procura

Use as bases de conhecimento a seguir para localizar informações úteis.

Notas técnicas e APARs

A partir do IBM Support Portal (http://www.ibm.com/support/entry/portal), é possível buscar notas técnicas e APARs (relatórios de problemas).

Procura no cabeçalho principal da IBM

Utilize a procura de cabeçalho principal IBM, digitando sua sequência de caracteres de procura no campo **Procurar** na parte superior de qualquer página ibm.com.

Mecanismos de procura externos

Procure pelo conteúdo usando qualquer mecanismo de procura externo, como Google, Yahoo ou Bing. Se usar um mecanismo de procura externo, seus resultados muito provavelmente incluirão informações que estão fora do domínio ibm.com. Entretanto, algumas vezes é possível localizar informações de resolução de problemas úteis sobre produtos IBM em grupos de notícias, fóruns e blogs que não estão em ibm.com.

Dica: Inclua "IBM" e o nome do produto em sua procura se você estiver procurando informações sobre um produto IBM.

Arquivos de Log do QRadar

Utilize os arquivos de log do IBM Security QRadar para ajudar a resolver problemas.

É possível revisar os arquivos de log para a sessão atual individualmente ou você pode coletá-los para revisão posterior.

Siga estas etapas para revisar os arquivos de log do QRadar.

1. Para ajudar a resolver erros ou exceções, revise os seguintes arquivos de log.
   - `/var/log/qradar.log`
   - `/var/log/qradar.error`
2. Se você necessitar de informações adicionais, revise os seguintes arquivos de log:
   - /var/log/qradar-sql.log
   - /opt/tomcat6/logs/catalina.out
   - /var/log/qflow.debug
3. Revise todos os logs logs selecionando **Administrador** > **Gerenciamento do sistema e da licença** > **Ações** > **Coletar arquivos de log**.

Conceitos relacionados:

"Recursos de Resolução de Problemas" na página 50
Os recursos de resolução de problemas são fontes de informações que podem ajudar a resolver um problema que você tem com um produto. Muitos dos links de recursos fornecidos também podem ser visualizados em um curto vídeo de demonstração.

Portas Usadas pelo QRadar

Revise as portas comuns usadas pelo IBM Security QRadar, pelos serviços e pelos componentes.

Por exemplo, você pode determinar as portas que devem ser abertas para o QRadar Console se comunicar com o Processadores de Eventos remoto.

Portas e Iptables

As portas de atendimento para QRadar são válidas apenas quando iptables estão ativadas em seu sistema QRadar.

Comunicação do SSH na Porta 22

Todas as portas que estão descritas na tabela a seguir podem ser encapsuladas, por criptografia, por meio da porta 22 através do SSH. Os hosts gerenciados que utilizam a criptografia podem estabelecer várias sessões de SSH bidirecionais para se comunicarem com segurança. Essas sessões de SSH são iniciadas a partir do host gerenciado para fornecer dados ao host que precisa dos dados na implementação. Por exemplo, dispositivos do Processador de Eventos podem iniciar várias sessões de SSH para o QRadar Console para comunicação segura. Esta comunicação pode incluir portas conectadas por SSH, como dados HTTPS para a porta 443 e dados de consulta do Ariel para a porta 32006. QRadar QFlow Collectors que utilizam criptografia podem iniciar sessões de SSH para dispositivos do Processador de Fluxo que requerem dados.

Portas QRadar

A menos que observado o contrário, as informações sobre o número de porta designado, descrições, protocolos e a direção de sinalização para a porta se aplicam a todos os produtos IBM Security QRadar.

A tabela a seguir lista as portas, protocolos, direção de comunicação, descrição e o motivo pelo qual a porta é utilizada.

Tabela 15. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes

Porta	Descrição	Protocolo	Orientação	Requisito
22	SSH	TCP	Bidirecional a partir do QRadar Console para todos os outros componentes.	Acesso de gerenciamento remoto Incluindo um sistema remoto como um host gerenciado Protocolos de origem de log para recuperar arquivos a partir de dispositivos externos, por exemplo, o protocolo de arquivo de log Os usuários que utilizam a interface da linha de comandos para se comunicar a partir de desktops com o Console Alta Disponibilidade (HA)
25	SMTP	TCP	A partir de todos os hosts gerenciados para o gateway SMTP	E-mails a partir de QRadar para um gateway SMTP Entrega de mensagens de email de erro e de aviso para um contato de e-mail administrativo
37	rdate (horário)	UDP/TCP	Todos os sistemas para o QRadar Console QRadar Console para o servidor NTP ou rdate	Sincronização de tempo entre o QRadar Console e os hosts gerenciados
111	Mapeador da porta	TCP/UDP	Hosts gerenciados que se comunicam com o QRadar Console Usuários que se conectam ao QRadar Console	Chamadas de Procedimento Remoto (RPC) para serviços necessários, como o Network File System (NFS)

Tabela 15. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Orientação	Requisito
135 e portas dinamica-mente alocadas acima de 1024 para chamadas de RPC.	DCOM	TCP	Agentes WinCollect e sistemas operacionais Windows que são remotamente pesquisados em busca de eventos. Tráfego bidirecional entre componentes do QRadar Console que usam o Microsoft Security Event Log Protocol e sistemas operacionais Windows que são pesquisados remotamente em busca de eventos ou tráfego bidirecional entre QRadar Event Collectors que usam o Microsoft Security Event Log Protocol e sistemas operacionais Windows que são pesquisados remotamente em busca de eventos. Tráfego bidirecional entre os agentes do Adaptive Log Exporter e os sistemas operacionais Windows que são pesquisados remotamente em busca de eventos.	Este tráfego é gerado pelo WinCollect, pelo Microsoft Security Event Log Protocol ou pelo Adaptive Log Exporter. **Nota:** O DCOM normalmente aloca um intervalo de portas aleatório para comunicação. Você pode configurar produtos Microsoft Windows para utilizar uma porta específica. Para obter mais informações, consulte a documentação do Microsoft Windows.
137	Serviço de nomes NetBIOS do Windows	UDP	Tráfego bidirecional entre agentes WinCollect e sistemas operacionais Windows que são pesquisados remotamente em busca de eventos Tráfego bidirecional entre componentes do QRadar Console ou o QRadar Event Collectors que usam o Microsoft Security Event Log Protocol e os sistemas operacionais Windows que são pesquisados remotamente em busca de eventos. Tráfego bidirecional entre os agentes do Adaptive Log Exporter e os sistemas operacionais Windows que são pesquisados remotamente em busca de eventos	Este tráfego é gerado pelo WinCollect, pelo Microsoft Security Event Log Protocol ou pelo Adaptive Log Exporter.

Tabela 15. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Orientação	Requisito
138	Serviço de datagrama NetBIOS do Windows	UDP	Tráfego bidirecional entre agentes WinCollect e sistemas operacionais Windows que são pesquisados remotamente em busca de eventos Tráfego bidirecional entre componentes do QRadar Console ou o QRadar Event Collectors que usam o Microsoft Security Event Log Protocol e os sistemas operacionais Windows que são pesquisados remotamente em busca de eventos. Tráfego bidirecional entre os agentes do Adaptive Log Exporter e os sistemas operacionais Windows que são pesquisados remotamente em busca de eventos	Este tráfego é gerado pelo WinCollect, pelo Microsoft Security Event Log Protocol ou pelo Adaptive Log Exporter..
139	Serviço de sessão NetBIOS do Windows	TCP	Tráfego bidirecional entre agentes WinCollect e sistemas operacionais Windows que são pesquisados remotamente em busca de eventos Tráfego bidirecional entre componentes do QRadar Console ou o QRadar Event Collectors que usam o Microsoft Security Event Log Protocol e os sistemas operacionais Windows que são pesquisados remotamente em busca de eventos. Tráfego bidirecional entre os agentes do Adaptive Log Exporter e os sistemas operacionais Windows que são pesquisados remotamente em busca de eventos	Este tráfego é gerado pelo WinCollect, pelo Microsoft Security Event Log Protocol ou pelo Adaptive Log Exporter.
199	NetSNMP	TCP	Hosts gerenciados do QRadar que se conectam ao QRadar Console Origens de log externas para QRadar QRadar Event Collectors	Porta TCP para o daemon NetSNMP que atende as comunicações (v1, v2c e v3) a partir de origens de log externas
427	Protocolo de Localização de Serviço (SLP)	UDP/TCP		O Módulo de Gerenciamento Integrado utiliza a porta para localizar serviços em uma LAN.

Tabela 15. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Orientação	Requisito
443	Apache/HTTPS	TCP	Tráfego bidirecional para comunicação segura a partir de todos os produtos para o QRadar Console	Downloads de configuração para hosts gerenciados a partir do QRadar Console Hosts gerenciados do QRadar que se conectam ao QRadar Console Usuários para ter acesso ao efetuar login no QRadar QRadar Console que gerenciam e fornecem atualizações de configuração para agentes WinCollect
445	Microsoft Directory Service	TCP	Tráfego bidirecional entre agentes WinCollect e sistemas operacionais Windows que são pesquisados remotamente em busca de eventos Tráfego bidirecional entre componentes do QRadar Console ou QRadar Event Collectors que utilizam o Microsoft Security Event Log Protocol e sistemas operacionais Windows que são consultados remotamente em busca de eventos Tráfego bidirecional entre os agentes do Adaptive Log Exporter e os sistemas operacionais Windows que são pesquisados remotamente em busca de eventos	Este tráfego é gerado pelo WinCollect, pelo Microsoft Security Event Log Protocol ou pelo Adaptive Log Exporter.
514	Syslog	UDP/TCP	Dispositivos de rede externos que fornecem eventos syslog TCP utilizam o tráfego bidirecional. Dispositivos de rede externos que fornecem eventos syslog UDP utilizam tráfego unidirecional.	Origens de log externas para enviar dados do evento para componentes do QRadar O tráfego de Syslog inclui os agentes do WinCollect e os agentes do Adaptive Log Exporter capazes de enviar eventos UDP ou TCP para o QRadar

Tabela 15. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Orientação	Requisito
762	Daemon de montagem Network File System (NFS) (mountd)	TCP/UDP	Conexões entre o QRadar Console e o servidor NFS	O daemon de montagem Network File System (NFS), que processa solicitações para montar um sistema de arquivos em um local especificado
1514	Syslog-ng	TCP/UDP	Conexão entre o componente local do Coletor de Eventos e componente local do Processador de Eventos para o daemon syslog-ng para criação de log	Porta de criação de log interna para syslog-ng
2049	NFS	TCP	Conexões entre o QRadar Console e o servidor NFS	O protocolo Network File System (NFS) para compartilhar arquivos ou dados entre componentes
2055	Dados do NetFlow	UDP	A partir da interface de gerenciamento na fonte de fluxo (normalmente um roteador) para o QRadar QFlow Collector.	Datagrama NetFlow a partir de componentes, como roteadores
3389	Remote Desktop Protocol (RDP) e Ethernet sobre USB estão ativados	TCP/UDP		Se o sistema operacional Windows estiver configurado para suportar RDP e o Ethernet sobre USB, um usuário poderá iniciar uma sessão para o servidor por meio da rede de gerenciamento. Isso significa que a porta padrão para RDP, 3389, deve ser aberta.
3900	Porta de presença remota do Módulo de Gerenciamento Integrado	TCP/UDP		Utilize esta porta para interagir com o console do QRadar por meio do Módulo de Gerenciamento Integrado.
4333	Porta de redirecionamento	TCP		Esta porta é designada como uma porta de redirecionamento para solicitações de Protocolo de Resolução de Endereço (ARP) na resolução de ofensa do QRadar
5432	Postgres	TCP	Comunicação para o host gerenciado que é utilizado para acessar a instância do banco de dados local	Obrigatório para fornecimento de hosts gerenciados na guia **Administração**

Tabela 15. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Orientação	Requisito
6543	Pulsação de alta disponibilidade	TCP/UDP	Bidirecional entre o host secundário e o host primário em um cluster de HA	Ping de pulsação a partir de um host secundário para um host primário em um cluster de HA para detectar falha de hardware ou de rede
7676, 7677, e quatro portas aleatoria-mente limitadas acima de 32000.	Conexões do sistema de mensagens (IMQ)	TCP	Comunicações da fila de mensagens entre os componentes em um host gerenciado.	Broker de fila de mensagens para comunicações entre os componentes em um host gerenciado As portas 7676 e 7677 são portas TCP estáticas e quatro conexões extras são criadas em portas aleatórias.
7777 – 7782, 7790, 7791	Portas do servidor JMX	TCP	Comunicações internas, essas portas não estão disponíveis externamente	Monitoramento do servidor JMX (Mbean) para serviços ECS, contexto de host, Tomcat, VIS, de relatório, ariel e de acumulador **Nota:** Essas portas são utilizadas pelo Suporte do QRadar.
7789	Distributed Replicated Block Device de alta disponibilidade	TCP/UDP	Bidirecional entre o host secundário e o host primário em um cluster de HA	O Distributed Replicated Block Device é usado para manter unidades sincronizadas entre os hosts primário e secundário em configurações de HA
7800	Apache Tomcat	TCP	A partir do Coletor de Eventos para o QRadar Console	Tempo real (fluxo) para eventos
7801	Apache Tomcat	TCP	A partir do Coletor de Eventos para o QRadar Console	Tempo real (fluxo) para fluxos
7803	Apache Tomcat	TCP	A partir do Coletor de Eventos para o QRadar Console	Porta do mecanismo de detecção de anomalias
8000	Event Collection Service (ECS)	TCP	A partir do Coletor de Eventos para o QRadar Console	Porta de atendimento para Event Collection Service (ECS) específico.
8001	Porta do daemon SNMP	UDP	Sistemas externos SNMP que solicitam informações de trap SNMP do QRadar Console	Porta de atendimento UDP para solicitações de dados SNMP externas.
8005	Apache Tomcat	TCP	Nenhum	Uma porta local que não é utilizada pelo QRadar

Tabela 15. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Orientação	Requisito
8009	Apache Tomcat	TCP	A partir do processo do daemon de HTTP (HTTPd) para o Tomcat	Conector do Tomcat, no qual a solicitação é utilizada e colocada em proxy para o serviço da Web
8080	Apache Tomcat	TCP	A partir do processo do daemon de HTTP (HTTPd) para o Tomcat	Conector do Tomcat, no qual a solicitação é utilizada e colocada em proxy para o serviço da Web.
9995	Dados do NetFlow	UDP	A partir da interface de gerenciamento na fonte de fluxo (normalmente um roteador) para o Coletor de QFlow	Datagrama NetFlow a partir de componentes, como roteadores
10000	Interface de administração do sistema baseada na web do QRadar	TCP/UDP	Sistemas de desktop do usuário para todos os hosts do QRadar	Mudanças do servidor, tais como a senha raiz de hosts e acesso ao firewall
23111	Servidor da web SOAP	TCP		Porta do servidor da web SOAP para o serviço de coleta de eventos (ECS)
23333	Fibre Channel Emulex	TCP	Sistemas de desktop do usuário que se conectam aos dispositivos QRadar com uma placa Fibre Channel	Serviço Emulex Fibre Channel HBAnywhere Remote Management (elxmgmt)
32004	Encaminhamento de evento normalizado	TCP	Bidirecional entre componentes do QRadar	Dados do evento normalizado que são comunicados a partir de uma origem externa ou entre QRadar Event Collectors
32005	Fluxo de dados	TCP	Bidirecional entre componentes do QRadar	Porta de comunicação do fluxo de dados entre QRadar Event Collectors quando em hosts gerenciados separados
32006	Consultas do Ariel	TCP	Bidirecional entre componentes do QRadar	Porta de comunicação entre o servidor proxy Ariel e o servidor de consulta do Ariel
32009	Dados de identificação	TCP	Bidirecional entre componentes do QRadar	Dados de identificação que são comunicados entre o serviço de informações de vulnerabilidade (VIS) passivo e o Event Collection Service (ECS)
32010	Porta de origem de recebimento do fluxo	TCP	Bidirecional entre componentes do QRadar	Porta de atendimento do fluxo para coletar dados do QRadar QFlow Collectors

Tabela 15. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Orientação	Requisito
32011	Porta de atendimento do Ariel	TCP	Bidirecional entre componentes do QRadar	A porta de atendimento do Ariel para procuras de banco de dados, informações de progresso e outros comandos associados
32000-33999	Fluxo de dados (fluxos de mensagens, eventos, contexto de fluxo)	TCP	Bidirecional entre componentes do QRadar	Fluxos de dados, como eventos, fluxos de mensagens, contexto de fluxo e consultas de procura de eventos
40799	dados do PCAP	TCP	A partir de dispositivos Juniper Networks SRX Series para QRadar	Coletando dados de captura de pacote de entrada (PCAP) a partir de dispositivos Juniper Networks SRX Series. **Nota:** A captura de pacote em seu dispositivo pode utilizar uma porta diferente. Para obter mais informações sobre a configuração de captura de pacote, consulte a documentação do dispositivo Juniper Networks SRX Series
ICMP	ICMP		Tráfego bidirecional entre o host secundário e o host primário em um cluster de HA	Testando a conexão de rede entre o host secundário e o host primário em um cluster de HA utilizando o Internet Control Message Protocol (ICMP)

Procurando Portas em Uso por QRadar

Utilize o comando **netstat** para determinar quais portas estão sendo utilizadas no QRadar Console ou no host gerenciado. Utilize o comando **netstat** para visualizar todas as portas em atendimento e estabelecidas no sistema.

Procedimento

1. Utilizando SSH, efetue login no QRadar Console, como o usuário raiz.
2. Para exibir todas as conexões ativas e as portas TCP e UDP nas quais o computador está atendendo, digite o seguinte comando:

   ```
   netstat -nap
   ```

3. Para procurar informações específicas a partir da lista de portas netstat, digite o seguinte comando:

   ```
   netstat -nap | grep port
   ```

   Exemplos:

- Para exibir todas as portas que correspondem a 199, digite o seguinte comando: `netstat -nap | grep 199`
- Para exibir todas as portas relacionadas ao postgres, digite o seguinte comando: `netstat -nap | grep postgres`
- Para exibir informações sobre todas as portas de atendimento, digite o seguinte comando: `netstat -nap | grep LISTEN`

Visualizando Associações de Porta do IMQ

É possível visualizar associações de números de portas para conexões do sistema de mensagens (IMQ) para as quais serviços de aplicativo são alocados. Para consultar os números de portas adicionais, conecte-se ao host local utilizando telnet.

Importante: Associações de porta aleatórias não são números de porta estáticos. Se um serviço for reiniciado, as portas geradas para um serviço serão realocadas e o serviço terá designado um novo conjunto de números de portas.

Procedimento

1. Utilize o SSH para efetuar login no QRadar Console, como o usuário root.
2. Para exibir uma lista de portas associadas para a conexão do sistema de mensagens IMQ, digite o seguinte comando:

   ```
   telnet localhost 7676
   ```
3. Se nenhuma informação for exibida, pressione a tecla Enter para fechar a conexão.

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

A

administrador de rede
  descrição v
APAR (relatório de análise de programa autorizado)
  base de conhecimento 51
arquitetura
  componentes 3

B

bases de conhecimento
  procura no cabeçalho principal 51
  Support Portal 51
biblioteca técnica
  local v

C

chaves de ativação
  descrição 1
chaves de licença
  descrição 1
Coletor QRadar QFlow
  descrição do componente 3
componentes
  descrição 3
configurações de rede
  alterando 45
  Console multifuncional 45
  implementação multissistema 46
  substituições de NIC 47
Console
  componentes 3
  instalando 13
Console QRadar
  instalando 13

D

dispositivos virtuais
  descrição 21
  instalando 21
  requisitos 23
documentação
  biblioteca técnica v
documentação de vídeo
  YouTube 51

F

Fix Central
  obtendo correções 50

H

hosts gerenciados
  instalando 13

I

instalações da unidade flash USB 6
  com dispositivos apenas seriais 10
  com Microsoft Windows 8
  com Red Hat Linux 9
  criando uma unidade USB inicializável 7
  instalando 11
instalando
  Console QRadar 13
  dispositivos virtuais 21
  host gerenciado 13
  partições de recuperação 29
  usando unidade flash USB 6

M

Magistrate
  descrição do componente 3
máquinas virtuais
  criando 25
  incluindo 27
  instalando software 26
modo de documento
  navegador da web Internet Explorer 6
modo de navegador
  navegador da web Internet Explorer 6
Módulo de Gerenciamento Integrado
  Veja também Módulo de Gerenciamento Integrado
  visão geral 2

N

navegador da web
  versões suportadas 5
nó de dados
  visão geral 41
notas técnicas
  base de conhecimento 51
nuvem
  instalação, OneVPN 37
  Instalação, OpenVPN em nuvem 38
  membro 40
  OpenVPN 38
  visão geral de implementação 37

P

partições de recuperação
  instalações 29
portas
  procurando 60
portasuso 52
preparando
  instalação 15
Problem Management Records
  solicitações de serviço
    Veja Problem Management Records
propriedades da partição
  requisitos 17

R

reinstalando
  partições de recuperação 29
requisitos de software
  descrição 5
resolução de problemas
  entendendo sintomas de um problema 49
  obtendo correções 50
  recursos 50
  recursos de documentação de vídeo 50
  Support Portal 50

S

sistema operacional Linux
  instalando em seu próprio dispositivo 19
  propriedades da partição 17
solicitações de serviço
  abrindo Problem Management Records (PMR) 50
suporte ao cliente
  informações do contato v
Support Portal
  visão geral 50