IBM Security QRadar
Versão 7.2.2

Guia de Instalação

G517-1616-00

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 47.

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 4
Ativar o modo de documento e modo de navegação no Internet Explorer 5

Capítulo 2. Instalando um QRadar Console ou Host Gerenciado 7

Capítulo 3. Instalações de Software QRadar em seu Próprio Dispositivo 11
Pré-requisitos para Instalar QRadar em seu Próprio Dispositivo 11
Preparando as instalações de software do QRadar para os sistemas de arquivos HA e XFS 12
Propriedades da Partição do Linux para seu Próprio Dispositivo 12
Instalando o RHEL em seu Próprio Dispositivo 14

Capítulo 4. Instalações do Dispositivo Virtual para QRadar SIEM e QRadar Log Manager 17
Visão Geral dos Dispositivos Virtuais Suportados. 17
Requisitos do sistema para dispositivos virtuais 19
Criando sua Máquina Virtual 20
Instalando o Software QRadar em uma Máquina Virtual 21
Incluindo seu Dispositivo Virtual para sua Implementação 22

Capítulo 5. Instalações a Partir da Partição de Recuperação 25
Reinstalando a partir da partição de recuperação 25

Capítulo 6. Gerenciamento de Configurações de Rede 29
Alterando as Configurações de Rede em um Sistema Multifuncional 29
Alterando as Configurações de Rede de um QRadar Console em uma Implementação Multissistema 30
Atualizando Configurações de Rede Após uma Substituição de NIC 31

Capítulo 7. Resolução de Problemas 33
Recursos de Resolução de Problemas 34
Support Portal 34
Solicitações de Serviço. 34
Fix Central 34
Bases de Conhecimento 35
Arquivos de Log do QRadar. 35
Portas Usadas pelo QRadar 36
Procurando Portas em Uso por QRadar 44
Visualizando Associações de Porta do IMQ. 45

Avisos 47
Marcas Registradas 49
Considerações de Política de Privacidade 49

Índice Remissivo 51

Introdução às Instalações do QRadar

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

Informações sobre a instalação do software IBM Security QRadar se aplicam aos produtos IBM Security QRadar SIEM, IBM Security QRadar Log Manager e IBM Security QRadar Network Anomaly Detection.

Para instalar ou recuperar um sistema de alta disponibilidade (HA), consulte o *Guia de Alta Disponibilidade do IBM Security QRadar*.

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 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 do QRadar, consulte Acessando a nota técnica da documentação doIBM Security (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

4.1 Entrando em Contato com o Suporte ao Cliente

Para obter informações sobre como contatar o suporte ao cliente, consulte Suporte e download da nota técnica (http://www.ibm.com/support/docview.wss?rs=0 &uid=swg21612861).

Declaração de Boas Práticas de Segurança

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

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 *Guia de Alta Disponibilidade do IBM Security QRadar*.

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 comprou um dispositivo que é pré-instalado com o software QRadar, a chave de ativação é incluída em um documento no CD anexo.
- 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 e QRadar Network Anomaly Detection

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 7
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 14
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 21
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.

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 apenas para implementações do QRadar SIEM e do QRadar Network Anomaly Detection.

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.

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 Identificador QRadar (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.

Magistrate
Fornece os componentes do processamento principal. 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.

Para obter mais informações sobre cada componente, consulte *Administration Guide*.

Conceitos relacionados:

Capítulo 7, "Resolução de Problemas", na página 33
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.

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) version 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 7
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 14
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 21
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 nos 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 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 para Produtos QRadar

navegador da web	**Versão Suportada**
Mozilla Firefox	17.0 24.0
Microsoft Internet Explorer de 32 bits, com o modo de documento e modo de navegador ativados	8.0 9.0
Google Chrome	A versão atual a partir da data de liberação dos produtos IBM Security QRadar V7.2.2

Ativar o modo de documento e modo de navegação no Internet Explorer

Se você usar o Microsoft Internet Explorer para acessar os produtos IBM Security QRadar, você deve ativar o modo de navegação e o modo de documento.

Procedimento

1. Em seu navegador da web Internet Explorer, pressione F12 para abrir a janelaFerramentas de Desenvolvedor.
2. Clique em **Modo de navegador** e selecione a versão do seu navegador da Web.
3. Clique em **Modo de Documento**.
   - Para o Internet Explorer V9.0, selecione **Padrões do Internet Explorer 9**
   - Para Internet Explorer V8.0, selecione **Padrões do Internet Explorer 8**

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.

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.

O IBM Security QRadar Network Anomaly Detection é um dispositivo independente. Instale o QRadar Network Anomaly Detection Console em um 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.

__ • Para dispositivos QRadar, um notebook está conectado à porta serial na parte traseira do dispositivo ou um teclado e monitor estão conectados.

__ • Você está conectado como usuário raiz.

__ • A chave de ativação está disponível.

Se você utilizar um notebook para conexão com o sistema, deverá utilizar um programa de terminal, como o HyperTerminal. Assegure que você configurou a opção **Conectar Usando** com a porta COM apropriada do conector serial. Assegure-se de ter configurado também as seguintes propriedades:

Tabela 4. Propriedades de Conexão do Terminal

Propriedade	**Configuração**
Bits por segundo	9600
Bits de Parada	1
Bits de dados	8
Paridade	Nenhum

Procedimento

1. Se você estiver utilizando seu próprio dispositivo, monte a imagem ISO do QRadar
   a. Crie o diretório `/media/cdrom` digitando o seguinte comando:
      `mkdir /media/cdrom`
   b. Obtenha o software do QRadar.
   c. Monte a imagem ISO do QRadar digitando o seguinte comando:
      `mount -o loop <path to the QRadar ISO> /media/cdrom`
   d. Para iniciar a instalação, digite o seguinte comando:
      `/media/cdrom/setup`
2. Para todas as instalações, certifique-se de que o End User License Agreement (EULA) esteja exibido.

Dica: Pressione a tecla Barra de Espaço para avançar através do documento.

Se você estiver instalando QRadar em seu próprio dispositivo, será solicitado para continuar a instalação. Esse processo pode demorar várias horas.

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**.
5. Siga as instruções no assistente de instalação para concluir a instalação.

   A tabela a seguir contém descrições e notas para ajudá-lo a configurar a instalação.

Tabela 5. Descrição de Configurações de Rede

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`.
Senha raiz	A senha deve atender aos seguintes critérios: • Conter pelo menos 5 caracteres • Não conter espaços • Pode incluir os seguintes caracteres especiais: @, #, ^ e *.

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

6. 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 de 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 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.

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 6. 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 24 GB **Importante:** Você deve fazer upgrade de sua memória do sistema antes de instalar o QRadar.
Memória (RAM) para Processador de Eventos	12 GB
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

Tabela 6. Requisitos do Sistema para Instalações do RHEL em seu Próprio Dispositivo (continuação)

Requisito	Descrição
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 da Partição do Linux para 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 7. 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
/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

Tabela 7. 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/ariel/ persistent_data	Área de armazenamento para o cursor do banco de dados ariel	/store/ariel/ persistent_data	XFS em Consoles EXT4 em hosts gerenciados	[1]Em dispositivos do Console: 20% do armazena-mento disponível. Em hosts gerenciados diferentes de Coletores QFlow e Coletores de Eventos de Armazena-mento e Encaminha-mento: 10% do armazena-mento disponível.	Não	SDA Se 2 discos, SDB
[1]/store e /store/ariel/persistent_data em conjunto utilizam 100% do espaço em disco que permanece após você criar as primeiras 5 partições.						

Restrições

Upgrades de software futuros poderão falhar se você reformatar qualquer uma das seguintes partições ou suas subpartições:

- /store
- /store/tmp
- /store/ariel
- /store/ariel/persistent_data

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.

Procedimento

1. Copie o DVD do sistema operacional Red Hat Enterprise Linux 6.4 ISO para um dos seguintes dispositivos de armazenamento móveis:
   - Digital Versatile Disk (DVD)
   - Unidade Flash USB Inicializável

     Para obter informações sobre como criar uma unidade flash USB inicializável, consulte a nota técnica do *Instalando QRadar usando uma unidade flash USB inicializável* no website da IBM (www.ibm.com/support).
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 arquivo para as partições `/`, `/boot` e `/var/log`.
   h. Reformate a partição de troca com um tipo de sistema de arquivo 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 da Partição do Linux para seu Próprio Dispositivo" na página 12
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.

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 *Administration Guide*.

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 Virtual1799 :

QRadar SIEM Flow Processor Virtual1799

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 Virtual1799 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 Virtual1799 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.

Nó 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 8. Requisitos para Dispositivos Virtuais

Requisito	Descrição
Cliente VMware	VMware ESXi Versão 5.0 VMware ESXi Versão 5.1 Para obter mais informações sobre os clientes VMWare, consulte o Website do VMware (www.vmware.com)
Tamanho do disco virtual em todos os dispositivos, exceto nos dispositivos do QRadar QFlow Collector	Mínimo: 256 GB **Importante:** Para obter desempenho ideal, assegure que um extra de 2-3 vezes do espaço em disco mínimo esteja disponível.
Tamanho do disco virtual para dispositivos do QRadar QFlow Collector	Mínimo: 70 GB

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

Tabela 9. 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 Virtual1799	12 GB	48 GB
QRadar SIEM All-in-One Virtual 3199	24 GB	48 GB
QRadar Log Manager Virtual 1790	24 GB	48 GB

Tarefas relacionadas:

"Criando sua Máquina Virtual"
Para instalar um dispositivo virtual, primeiro você deve usar o VMware vSphere Client 5.0 para criar uma máquina virtual.

Criando sua Máquina Virtual

Para instalar um dispositivo virtual, primeiro você deve usar o VMware vSphere Client 5.0 para criar uma máquina virtual.

Procedimento

1. A partir do VMware vSphere Client, clique em **Arquivo** > **Novo** > **Máquina Virtual**.
2. 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 (OS)**, 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:

      Ao configurar os parâmetros na página **CPU**, você deverá configurar um mínimo de dois processadores. A combinação de número de soquetes virtuais e número de núcleos por soquete virtual determina quantos processadores estão configurados no sistema.

      A tabela a seguir fornece exemplos de configurações da página **CPU** que você pode utilizar:

Tabela 10. Configurações da Página **CPU** *de Amostra*

Número de Processadores	Configurações da Página CPU de Amostra
2	Número de soquetes virtuais = 1 Número de núcleos por soquete virtual = 2

Tabela 10. Configurações da Página **CPU** *de Amostra (continuação)*

Número de Processadores	Configurações da Página CPU de Amostra
2	Número de soquetes virtuais = 2 Número de núcleos por soquete virtual = 1
4	Número de soquetes virtuais = 4 Número de núcleos por soquete virtual = 1
4	Número de soquetes virtuais = 2 Número de núcleos por soquete virtual = 2

e. No campo **Tamanho da Memória**, digite ou selecione 8 ou superior.

f. Utilize a tabela a seguir para configurar suas conexões de rede.

Tabela 11. 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 12. 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

3. 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. Na área de janela **Status do Dispositivo**, selecione a caixa de seleção **Conectar com energia ligada**.

6. Na área de janela **Tipo de Dispositivo**, selecione **Arquivo ISO do Armazenamento de Dados** e clique em **Procurar**.
7. Na janela Procurar Armazenamentos de Dados, localize e selecione o arquivo ISO do produto QRadar, clique em **Abrir** e, em seguida, clique em **OK**.
8. 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.**
9. Efetue login na máquina virtual digitando `root` para o nome de usuário.

   O nome de usuário faz distinção entre maiúsculas e minúsculas.
10. Assegure que End User License Agreement (EULA) seja exibido.

    Dica: Pressione a tecla Barra de Espaço para avançar através do documento.
11. Para o tipo de configuração, selecione **normal**.
12. Para instalações do QRadar Console, selecione o modelo ajuste **Corporativo**.
13. Siga as instruções no assistente de instalação para concluir a instalação.

    A tabela a seguir contém descrições e notas para ajudá-lo a configurar a instalação.

Tabela 13. Descrição de Configurações de Rede

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`.
Senha raiz	A senha deve atender aos seguintes critérios: • Conter pelo menos 5 caracteres • Não conter espaços • Pode incluir os seguintes caracteres especiais: @, #, ^ e *.

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 20
Para instalar um dispositivo virtual, primeiro você deve usar o VMware vSphere Client 5.0 para criar uma máquina 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 de 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 20
Para instalar um dispositivo virtual, primeiro você deve usar o VMware vSphere Client 5.0 para criar uma máquina 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.

Depois de uma falha de disco rígido, você pode não ser capaz de reinstalar a partir da partição de recuperação, porque a partição de recuperação não está mais disponível. Se ocorrer uma falha de disco rígido, entre em contato com o Suporte ao Cliente para obter assistência.

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 *Guia armazenamento não integrado*.

Procedimento

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

   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. 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.

   A tabela a seguir contém descrições e notas para ajudá-lo a configurar a instalação.

Tabela 14. Descrição de Configurações de Rede

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`.
Senha raiz	A senha deve atender aos seguintes critérios: • Conter pelo menos 5 caracteres • Não conter espaços • Pode incluir os seguintes caracteres especiais: @, #, ^ e *.

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

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 15. 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.

Alterando as Configurações de Rede de um QRadar Console em uma Implementação Multissistema

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

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. Para alterar as configurações de rede no QRadar Console, utilize o SSH para efetuar login no QRadar como o usuário raiz.

   O nome de usuário é `raiz`.

   a. Digite o seguinte comando: `qchange_netsetup`.
   b. 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 16. Descrição de Configurações de Rede para uma Implementação Multissistema do QRadar Console

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.

3. Para ler 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

4. 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 `root`.
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 7. 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 17. 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 35
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

No IBM Support Portal (http://www.ibm.com/support/entry/portal), é possível procurar 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:
   - https://*console_ip*/system_info.cgi
   - `/var/log/qradar-sql.log`
   - `/opt/tomcat5/logs/catalina.out`
   - `/opt/imq/share/var/instances/imqbroker/log/log.txt`
   - `/var/log/qflow.debug`
3. Para coletar arquivos de log para um representante de suporte técnico IBM, a partir da linha de comandos, execute o seguinte comando:

   `/opt/qradar/support/get_logs.sh -s`

   O comando cria um arquivo `logs_<console_name>_<date_time>.tar.bz2` no diretório `/var/log`.

Conceitos relacionados:

"Recursos de Resolução de Problemas" na página 34
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 18. 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 18. 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 consultados para eventos. Tráfego bidirecional entre componentes do QRadar Console que usam o Microsoft Security Event Log Protocol e sistemas operacionais Windows que são pesquisados remotamente para eventos ou tráfego bidirecional entre Event Collectors que usam o Microsoft Security Event Log Protocol e sistemas operacionais Windows que são pesquisados remotamente para 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 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 18. 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 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 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 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 18. 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 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 utilize 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 18. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Orientação	Requisito
762	Montagem Deamon Network File System (NFS)	TCP/UDP	Conexões entre o QRadar Console e o servidor NFS	A montagem Daemon de Network File System (NFS), no qual o processo solicita a montagem de um arquivo de sistema em uma locação específica.
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 log interno para syslog-ng
2049	NFS	TCP	Conexões entre o QRadar Console e o servidor NFS	O protocolo do Sistema de Arquivos de Rede (NFS) para compartilhar arquivos ou dados entre componentes
2055	Dados do NetFlow	UDP	Do gerenciador de interfaces na fonte de fluxo (normalmente um roteador) ao 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 pedidos de Protocolo de Resolução de Endereço (ARP) em QRadar resolução de ofensa.
5432	Postgres	TCP	Comunicação para o host gerenciado que é utilizado para acessar a instância do banco de dados local	Obrigatório para fornecimento hosts gerenciados na guia **Admin**

Tabela 18. 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 principal 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	Fila de mensagens de comunicações entre os componentes do em um host gerenciado.	Fila de mensagens do broker 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	Porta de servidor JMX	TCP	Comunicações internas: estas portas não estão disponíveis externamente.	monitoramento do servidor JMX (de Mbean) para ECS, hostcontext, Tomcat, VIS, Relatório, ariel, e accumulator serviços **Nota:** Essas portas são utilizadas pelo Suporte do QRadar.
7789	Dispositivo de bloco replicado distribuído 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 nas 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 18. 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, onde o pedido é utilizado e um 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, onde o pedido é utilizado e um 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 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	os sistemas desktop do usuário que se conectam aQRadar dispositivos com uma placa Fibre Channel	serviço Fibre Channel Remote Management HBAnywhere Emulex (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 Event Collectors
32005	Fluxo de dados	TCP	Bidirecional entre componentes do QRadar	Porta de comunicação do fluxo de dados entre 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 18. 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, eventos, fluxo de contexto)	TCP	Bidirecional entre componentes do QRadar	Fluxos de dados, como eventos, fluxos de mensagens, contexto de fluxo e consultas de procura de eventos
40799	PCAP de dados	TCP	Na Série SRX para dispositivos Juniper Networks 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. 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 licenças relacionados a informações sobre 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, esta disposição pode não se aplicar ao Cliente.

Estas informações podem incluir imprecisões técnicas ou erros tipográficos. Alterações são periodicamente realizadas nas informações aqui constantes; essas alterações serão incorporadas em novas edições da 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 ou websites. Os materiais nesses websites não fazem parte dos materiais deste produto IBM e o uso desses websites é um risco 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 de 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. Resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

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

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

Todos os preços 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 em operações de negócios diárias. Para ilustrá-lo da forma mais completa possível, os exemplos podem incluir 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 Registradas

IBM, o logotipo IBM e ibm.com são marcas ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca registrada da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca registrada (® ou ™), estes símbolos indicarão marcas registradas ou de direito consuetudinário dos Estados Unidos de propriedade da IBM no momento em que estas informações forem publicadas. Estas marcas comerciais também podem ser marcas registradas ou marcas comerciais de direito consuetudinário em outros países. Uma lista atual de marcas comerciais IBM está disponível na Web em Informações de copyright e de marca registrada (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 ou marcas registradas da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

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

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

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

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

Se as configurações implementadas para esta Oferta de Software permitirem que você, como cliente, colete informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, você deverá consultar seu conselho jurídico sobre as leis aplicáveis a essa coleta de dados, incluindo requisitos para aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para tais propósitos, consulte a Política de Privacidade da IBM em http://www.ibm.com/privacy e a Declaração de Privacidade On-line da IBM em http://www.ibm.com/privacy/details, a seção intitulada “Cookies, Web Beacons and Other Technologies” e “IBM Software Products and Software-as-a-Service Privacy Statement” 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 35
arquitetura
  componentes 3

B

bases de conhecimento
  procura no cabeçalho principal 35
  Support Portal 35
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 29
  Console multifuncional 29
  implementação multissistema 30
  substituições de NIC 31
Console
  componentes 3
  instalando 7
Console QRadar
  instalando 7

D

dispositivos virtuais
  descrição 17
  instalando 17
  requisitos 19
documentação
  biblioteca técnica v
documentação de vídeo
  YouTube 35

F

Fix Central
  obtendo correções 34

H

hosts gerenciados
  instalando 7

I

instalando
  Console QRadar 7
  dispositivos virtuais 17
  host gerenciado 7
  partições de recuperação 25

M

Magistrate
  descrição do componente 3
máquinas virtuais
  criando 20
  incluindo 23
  instalando software 21
modo de documento
  Navegador da web do Internet Explorer 5
modo do navegador
  Navegador da web do Internet Explorer 5
Módulo de Gerenciamento Integrado
  Veja também Módulo de Gerenciamento Integrado
  visão geral 2

N

navegador da Web
  versões suportadas 5
notas técnicas
  base de conhecimento 35

P

partições de recuperação
  instalações 25
portas
  procurando 44
portasuso 36
preparando
  instalação 11
Problem Management Records
  solicitações de serviço
    Veja Problem Management Records
propriedades da partição
  requisitos 12

R

reinstalando
  partições de recuperação 25
requisitos de software
  descrição 4
resolução de problemas
  entendendo sintomas de um problema 33
  obtendo correções 34
  recursos 34
  recursos de documentação de vídeo 34
  Support Portal 34

S

sistema operacional Linux
  instalando em seu próprio dispositivo 14
  propriedades da partição 12
solicitações de serviço
  abrindo Problem Management Records (PMR) 34
suporte ao cliente
  informações do contato v
Support Portal
  visão geral 34