IBM Security QRadar Incident Forensics
Versão 7.3.0

Guia de Instalação

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 33.

Informações do produto

Esse documento se aplica ao IBM QRadar Security Intelligence Platform V7.3.0 e liberações subsequentes, a menos que seja substituído por uma versão atualizada desse documento.

Índice

Introdução à instalação do IBM Security QRadar Incident Forensics

Informações sobre a instalação do IBM® Security QRadar Incident Forensics e a integração do produto ao IBM Security QRadar. Os dispositivos do QRadar Incident Forensics contêm software pré-instalado e o sistema operacional Red Hat Enterprise Linux. Você também pode instalar o software QRadar Incident Forensics em seu próprio hardware.

Público desejado

Administradores da rede responsáveis pela instalação e configuração de sistemas QRadar Incident Forensics.

Os administradores requerem um conhecimento de trabalho de rede e de sistemas operacionais Linux.

Documentação técnica

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

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

Entrando em contato com o suporte ao cliente

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

Declaração de boas práticas de segurança

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

Observe que:

O uso desse programa pode implicar em várias leis ou regulamentações, incluindo aquelas relacionadas à privacidade, proteção de dados, emprego, e armazenamento e comunicações eletrônicas. O IBM Security QRadar pode ser usado apenas para propósitos legais e de maneira legal. O cliente concorda em usar este Programa de acordo com leis, regulamentos e políticas e assume toda a responsabilidade pelo seu cumprimento. O licenciado declara que obterá ou obteve quaisquer consentimentos, permissões ou licenças necessárias para permitir o uso legal do IBM Security QRadar.

Nota

O IBM Security QRadar Incident Forensics foi projetado para ajudar as empresas a melhorarem seu ambiente e dados de segurança. Mais especificamente, o IBM Security QRadar Incident Forensics foi projetado para ajudar as empresas a investigarem e entenderem melhor o que aconteceu nos incidentes de segurança de rede. A ferramenta permite que as empresas indexem e procurem dados capturados do pacote de rede (PCAPs) e incluam um recurso que possa reconstruir esses dados novamente em sua forma original. Esse recurso de reconstrução pode reconstruir dados e arquivos, incluindo mensagens de email, anexos de arquivo e figuras, telefonemas VoIP e websites. Informações adicionais sobre os recursos e funções do Programa e como podem ser configurados estão contidas nos manuais e em outra documentação que acompanha o Programa. O uso desse Programa pode implicar em várias leis ou regulamentos, incluindo aqueles relacionados à privacidade, proteção de dados, emprego e comunicações e armazenamento eletrônico. O IBM Security QRadar Incident Forensics pode ser usado apenas para propósitos legais e de forma legal. O cliente concorda em usar este Programa conforme as leis, os regulamentos e as políticas aplicáveis, assumindo toda a responsabilidade em seu cumprimento. O Licenciado declara que obterá ou que obteve quaisquer consentimentos, permissões ou licenças necessárias para permitir o uso legal do IBM Security QRadar Incident Forensics.

Capítulo 1. Fazendo upgrade do QRadar Incident Forensics

Você deve fazer upgrade de todos os produtosIBM Security QRadar de sua implementação para a mesma versão. É possível fazer upgrade do IBM Security QRadar Incident Forensics V7.2.8 para V7.3.0 usando um instalador de upgrade.

Se você estiver fazendo upgrade de QRadar Incident Forensics V7.2.4 ou versões anteriores e deseja manter seus dados, entre em contato com seu representante de vendas IBM. Caso contrário, se deseja fazer upgrade do QRadar Incident Forensics V7.2.4 ou de versões anteriores, mas não deseja manter os dados, faça upgrade diretamente para o V7.3.0 fazendo uma nova instalação.

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

Procedimento

1. Faça download do arquivo <*QRadar_patchupdate*>.*sfs* do IBM Fix Central (www.ibm.com/support/fixcentral).
2. Use SSH para efetuar login no sistema como usuário raiz.
3. Copie o arquivo de correção para o diretório `/tmp` ou para outro local que tiver espaço em disco suficiente.
4. Para criar o diretório `/media/updates`, digite o comando a seguir:

   ```
   mkdir -p /media/updates
   ```
5. Mude para o diretório em que você copiou o arquivo de correção.
6. Para montar o arquivo de correção para o diretório `/media/updates`, digite o comando a seguir:

   ```
   mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates/
   ```
7. Para executar o instalador de upgrade, digite o comando a seguir:

   ```
   /media/updates/installer
   ```

   Da primeira vez que o script do instalador de correções for executado, poderá haver um atraso antes de o primeiro menu do instalador de correções ser exibido.
8. Forneça respostas para as perguntas de pré-instalação com base na sua implantação.
9. Use o instalador de upgrade para fazer upgrade de todos os hosts na sua implantação.

   Se você não selecionar **Corrigir Todos**, você deverá fazer upgrade dos sistemas na seguinte ordem:

   - QRadar Console
   - QRadar Incident Forensics

   Se a sua sessão SSH estiver desconectada enquanto o upgrade estiver em andamento, o upgrade continuará. Quando você reabrir sua sessão SSH e executar novamente o instalador, a instalação continuará.
10. Após o upgrade ser concluído, desmonte a atualização de software usando o comando a seguir: **`umount /media/updates`**

O que Fazer Depois

Faça upgrade dos dispositivos de captura de pacote. Para obter informações adicionais, consulte *Guia de referência rápida do IBM Security QRadar Packet Capture*.

Capítulo 2. Componentes de instalação do QRadar Incident Forensics

O QRadar Incident Forensics é integrado na arquitetura escalável de IBM QRadar Security Intelligence Platform. Dependendo de seu requisito, é possível instalar os componentes do IBM Security QRadar Incident Forensics em um dispositivo (*all-in-one*) ou em múltiplos dispositivos.

Opções de instalação

Dependendo dos componentes que você instala, nem todas as capacidades de segurança estão disponíveis. Por exemplo, se você instalar o QRadar Incident Forensics em um dispositivo, somente a rede forense fica disponível. No entanto, se você instalar um host gerenciado por QRadar Incident Forensics, mais capacidades de segurança ficam disponíveis. Para a maioria das instalações, instale o QRadar Console, pelo menos, um QRadar Incident Forensics Processor, e um ou mais dispositivos do QRadar Packet Capture.

O diagrama a seguir resume as múltiplas capacidades de segurança e estrutura arquitetural do IBM QRadar Security Intelligence Platform.

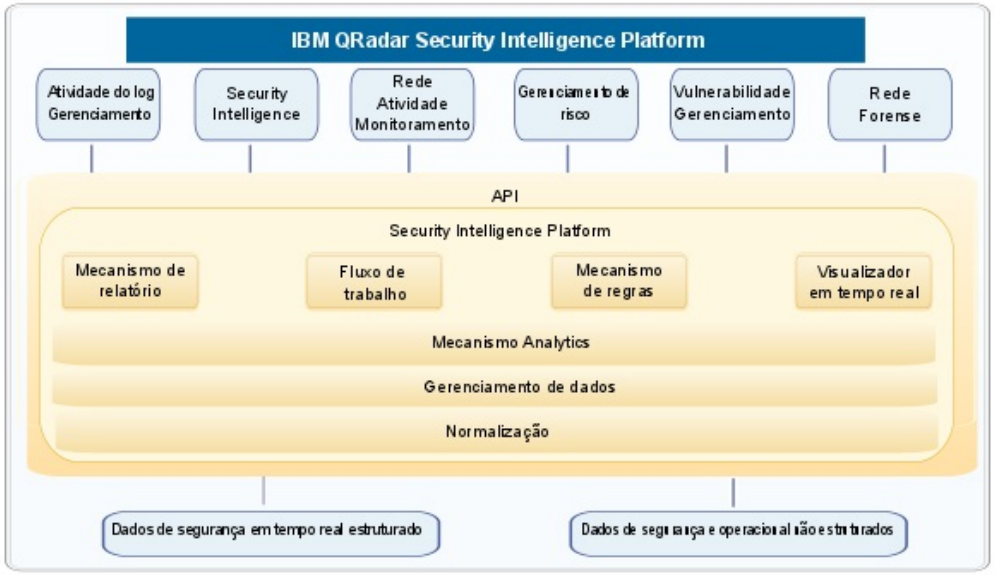


Figura 1. Visão geral arquitetural da inteligência de segurança do QRadar

Implementações all-in-one

Nas implementações independentes ou all-in-one, você instala o software IBM Security QRadar Incident Forensics Standalone. Essas implementações de dispositivo únicas são semelhantes a instalar o host gerenciado QRadar Console e QRadar Incident Forensics em um dispositivo, mas sem gerenciamento de log, monitoramento de atividade de rede ou outros recursos de inteligência de segurança. Para uma solução forense de rede independente, instale o QRadar Incident Forensics Standalone em implementações de pequeno a médio porte.

Conforme mostrado no diagrama a seguir, é possível anexar os dispositivos QRadar Packet Capture no IBM Security QRadar Incident Forensics Standalone.

Figura 2. Exemplo de implementação do IBM Security QRadar Incident Forensics Standalone

Restrição: Não é possível incluir hosts gerenciados no QRadar Incident Forensics Standalone nem anexar o QRadar Incident Forensics Standalone ao QRadar Console.

Implementações distribuídas

Em implementações em que você precisa de análise forense de rede e outras capacidades de inteligência de segurança ou quando precisar distribuir a carga de trabalho para recuperações forenses, instale o QRadar Console e um ou mais hosts gerenciados pelo QRadar Incident Forensics. O QRadar Console fornece informações e gerenciamento de evento (SIEM), gerenciamento de log, detecção de anomalia, gerenciamento de risco e gerenciamento de vulnerabilidade.

Em uma implementação distribuída, existem três dispositivos:

- QRadar Console
- Host gerenciado por QRadar Incident Forensics (QRadar Incident Forensics Processor)
- QRadar Packet Capture (opcional)

As versões de software para todos os dispositivos IBM Security QRadar em uma implementação devem ser da mesma versão e nível de correção. As implementações que usam diferentes versões do software não são suportadas.

O diagrama a seguir mostra que é possível conectar múltiplos hosts gerenciados por QRadar Incident Forensics ao QRadar Console. É possível conectar dispositivos QRadar Packet Capture aos hosts gerenciados por QRadar Incident Forensics (QRadar Incident Forensics Processor).

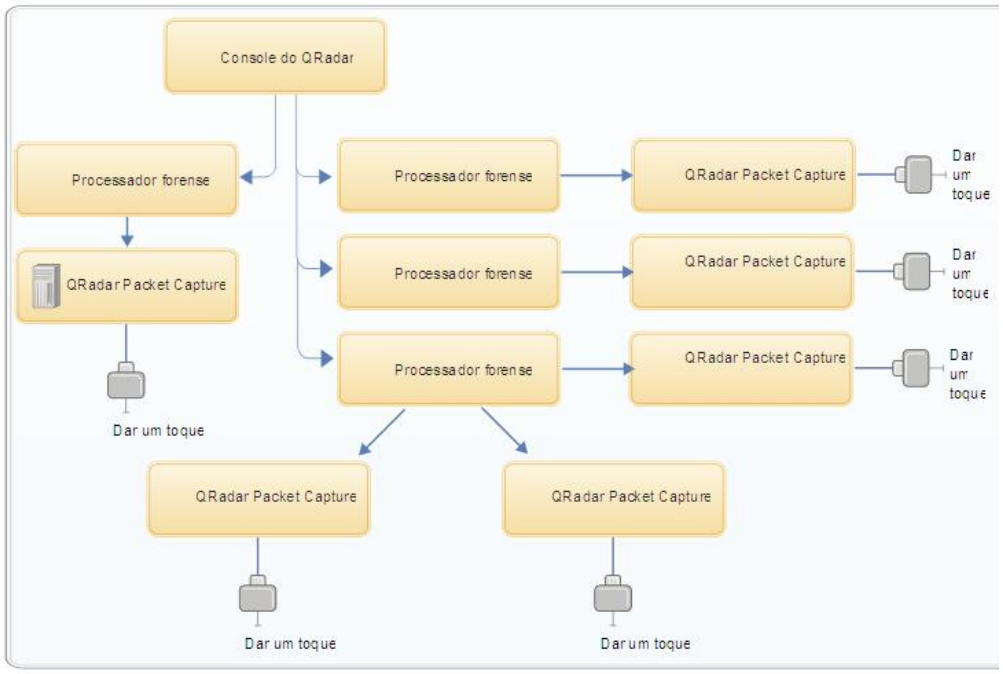


Figura 3. Exemplo de implementação distribuída

Componentes do QRadar Incident Forensics

Os componentes do QRadar podem incluir os componentes a seguir:

QRadar Console

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

Em implementações distribuídas, use o QRadar Console para gerenciar múltiplos hosts do QRadar Incident Forensics Processor.

QRadar Incident Forensics Processor

Fornece a interface de produto QRadar Incident Forensics. A interface fornece ferramentas para traçar novamente ações passo-a-passo de crimes cibernéticos, reconstruir dados brutos de rede que estejam relacionados a um incidente de segurança, pesquisa nos dados não estruturados disponíveis e reconstruir visualmente as sessões e os eventos.

Você deve incluir o QRadar Incident Forensics Processor como um host gerenciado antes que possa usar a capacidade forense de inteligência de segurança.

QRadar Incident Forensics Standalone

Fornece a interface com o usuário do produto QRadar Incident Forensics. A instalação de QRadar Incident Forensics Standalone fornece as ferramentas que você precisa para executar investigações forenses. Somente as funções administrativas relacionadas e investigativas forenses estão disponíveis.

QRadar Packet Capture

É possível instalar um dispositivo QRadar Packet Capture opcional. Se nenhum outro dispositivo de captura de pacote de rede (PCAP) for implementado, será possível usar esse dispositivo para armazenar dados

usados pelo QRadar Incident Forensics. É possível instalar qualquer número desses dispositivos como um toque de rede ou sub-rede para coletar os dados brutos do pacote.

Se nenhum dispositivo de captura de pacote for conectado, será possível fazer upload manualmente dos arquivos de captura de pacote na interface com o usuário ou usando o FTP.

Capítulo 3. Visão geral da instalação do QRadar Incident Forensics

Instale o software QRadar Incident Forensics em seu próprio dispositivo ou em um dispositivo virtual. Os dispositivos QRadar Incident Forensics possuem o software QRadar Incident Forensics instalado

O QRadar Incident Forensics deve ser instalado em um sistema operacional Red Hat Enterprise Linux.

Seleção do ID do dispositivo

Para a maior de QRadar Incident Forensics, instale pelo menos duas imagens ISO:

- QRadar Console

  Os produtos QRadar usam a mesma imagem de software de instalação. A *chave de ativação* determina o tipo de dispositivo e os componentes a serem instalados. Quando você entra na chave de ativação, é solicitado que identifique o tipo de dispositivo. Você deve instalar o QRadar Console
- 6000 QRadar Incident Forensics Processor (host gerenciado)

  Devido a controles de exportação, os componentes QRadar Incident Forensics são instalados a partir de uma imagem ISO diferente. Você deve instalar o host gerenciado do QRadar Incident Forensics e configurá-lo para conectar-se ao QRadar Console

Para obter instalações all-in-one, instale somente a imagem ISO 6100 QRadar Incident Forensics e selecione o componente QRadar Incident Forensics Standalone.

Ao instalar o QRadar Incident Forensics, uma chave de licença padrão fornecerá acesso durante cinco semanas. Antes da expiração da licença padrão, você deve alocar uma chave de licença para seu sistema.

Etapas de instalação

Para instalações distribuídas, use essas etapas para orientá-lo através do processo de instalação.

1. Revise os requisitos de hardware e de software.
2. Instale o software do QRadar Console.
3. Instale o host gerenciado pelo QRadar Incident Forensics.
4. Implemente o host gerenciado pelo QRadar Incident Forensics.
5. Inclua dispositivos de captura de pacote.

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.

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.

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
- A fonte de alimentação ininterrupta (UPS) para todos os sistemas que armazenam dados, como QRadar Console, componentes do Event Processor ou componentes do QRadar QFlow Collector.

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

Navegadores da web suportados

A tabela a seguir lista os navegadores da web suportados:

Tabela 1. Navegadores da web suportados para produtos QRadar

Navegador da web	**Versões suportadas**
Mozilla Firefox	45.2 Extended Support Release
64 bits Microsoft Internet Explorer com o modo do Microsoft Edge ativado.	11.0
Google Chrome	Latest

Se você usar o Microsoft Internet Explorer, deve ativar o modo de documento e modo de navegador:

1. Em seu navegador da web do 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**.

Comunicação entre hosts QRadar Incident Forensics requer portas abertas

A tabela a seguir lista as portas que devem ser abertas entre hosts QRadar Incident Forensics:

Tabela 2. Abrir portas entre hosts

Port	**Descrição**
443	Requerido para análise de artefato.
28080	Requerido para procura distribuída

Capítulo 4. Instalações de Software QRadar Incident Forensics em seu Próprio Dispositivo

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

Para novas instalações de software que integram o QRadar Incident Forensics ao IBM Security QRadar, instale dois arquivos ISO:

- QRadar

  Um único ISO é usado para instalar cada produto QRadar, exceto para QRadar Incident Forensics. A chave de ativação que você insere determina o tipo de dispositivo QRadar que está instalado.
- QRadar Incident Forensics

  Essa imagem ISO contém o QRadar Incident Forensics Processor e o QRadar Incident Forensics Standalone. Você deve instalar o QRadar Incident Forensics Processor.

Pré-requisitos para Instalar QRadar Incident Forensics 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 3. Requisitos do Sistema para Instalações do RHEL em seu Próprio Dispositivo

Requisito	Detalhes
Versão de software suportada	Versão 6.7
Versão de Bit	64 bits
Discos de instalação com kickstart	Não Suportados
Memória (RAM) para o processador do Forensics	Mínimo de 128 GB **Importante:** Você deve fazer upgrade de sua memória do sistema antes de instalar o QRadar.
Espaço livre em disco para o processador do Forensics	Mínimo de 5% do espaço total em disco **Importante:** Para obter desempenho ideal, assegure que um extra de 2-3 vezes do espaço em disco mínimo esteja disponível.

Tabela 3. Requisitos do Sistema para Instalações do RHEL em seu Próprio Dispositivo (continuação)

Requisito	Detalhes
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.

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

As propriedades da partição do sistema operacional Linux para instalações do 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.

Use os valores da tabela a seguir como guia ao recriar o particionamento no sistema operacional Red Hat Enterprise Linux.

O sistema de arquivos para cada partição é XFS.

Tabela 4. Guia de particionamento para RHEL

Caminho de montagem	LVM suportado?	Existe na Instalação de software?	Tamanho
`/boot`	Não	Sim	1 GB
`/boot/efi`	Não	Sim	200 MB
`/recovery`	Não	Não	8 GB
`/var`	Sim	Sim	5 GB
`/var/log`	Sim	Sim	15 GB
`/var/log/audit`	Sim	Sim	3 GB
`/opt`	Sim	Sim	10 GB
`/home`	Sim	Sim	1 GB
`/storetmp`	Sim	Sim	15 GB
`/tmp`	Sim	Sim	3 GB
`troca`	N/D	Sim	Fórmula de troca: Configure o tamanho da partição de troca para 75% de RAM, com um valor mínimo de 12 GiB e um valor máximo de 24 GiB.
`/`	Sim	Sim	Até 15 GB

Tabela 4. Guia de particionamento para RHEL (continuação)

Caminho de montagem	LVM suportado?	Existe na Instalação de software?	Tamanho
/store	Sim	Sim	80% de espaço restante
/transient	Sim	Sim	20% de espaço restante

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 QRadar Incident Forensics.

Procedimento

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

     Para obter mais informações sobre criar uma unidade flash USB inicializável, consulte o *Guia de Instalação do IBM Security QRadar*.
2. Insira o dispositivo de armazenamento móvel em seu dispositivo e reinicie seu dispositivo.
3. No menu inicial, selecione uma das opções a seguir.
   - 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 a partição /boot.
   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**.
8. Assegure-se de que as interfaces de rede integradas tenham os nomes eth0, eth1, eth2 e eth3.

O que Fazer Depois

Capítulo 7, “Instalando o QRadar Console”, na página 21

Capítulo 5. Instalação do software do QRadar Incident Forensics em um dispositivo do QRadar Incident Forensics

Os dispositivos IBM Security QRadar Incident Forensics são pré-instalados com um sistema operacional Red Hat Enterprise Linux e software QRadar.

Para novas instalações de software que integram o QRadar Incident Forensics ao IBM Security QRadar, configure os dois arquivos ISO pré-carregados:

- QRadar

  Um único ISO é usado para instalar cada produto QRadar, exceto para QRadar Incident Forensics. A chave de ativação que você insere determina o tipo de dispositivo QRadar que está instalado.
- QRadar Incident Forensics

  Essa imagem ISO contém o QRadar Incident Forensics Processor e o QRadar Incident Forensics Standalone. Você deve instalar o QRadar Incident Forensics Processor.

Para novas instalações de software em que você precisa somente de capacidades forenses, instale o QRadar Incident Forensics Standalone do ISO QRadar Incident Forensics.

Capítulo 6. Instalações do dispositivo virtual para o QRadar Incident Forensics

É possível instalar o IBM Security QRadar Incident Forensics em um dispositivo virtual. Assegure-se de usar um dispositivo virtual suportado que atenda aos requisitos mínimos do sistema.

Um dispositivo virtual é um sistema QRadar Incident Forensics que consiste no software QRadar Incident Forensics que está instalado em uma máquina virtual do VMWare ESX .

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

Processo de instalação

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

__ • Crie uma máquina virtual.

__ • Instale o software do IBM Security QRadar Incident Forensics na máquina virtual.

__ • Se você tiver instalado o QRadar Incident Forensics Processor, inclua seu dispositivo virtual à implementação.

Requisitos do sistema para dispositivos virtuais

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

Tabela 5. Requisitos para Dispositivos Virtuais.

Requisito	Descrição
Cliente VMware	VMware ESXi Versão 5.0 VMware ESXi Versão 5.1 VMware ESXi Versão 5.5 Para obter mais informações sobre os clientes VMWare, consulte o Website do VMware (www.vmware.com)
Tamanho do disco virtual	Mínimo: 256 GB **Importante:** Para um desempenho ideal, assegure-se de que um extra de 2 a 3 vezes do espaço em disco mínimo esteja disponível.

Criando sua Máquina Virtual

Para instalar um dispositivo virtual, você deve usar primeiro o VMWare ESX para criar uma máquina virtual.

Procedimento

1. A partir do VMware vSphere Client, clique em **Arquivo** > **Novo** > **Máquina Virtual**.
2. Inclua o **Nome e local** 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 (OS)**, selecione **Linux** e selecione **Red Hat Enterprise Linux 6 (64 bits)**.
   d. Na página **CPUs**, configure o número de processadores virtuais que deseja para a máquina virtual. Selecione 40 ou mais.
   e. No campo **Tamanho da memória**, digite ou selecione a RAM requerida para sua implementação. Selecione 128 GB ou mais.
   f. Utilize a tabela a seguir para configurar suas conexões de rede.

Tabela 6. 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 7. Configurações para o Tamanho do Disco Virtual e Parâmetros da Política de Fornecimento

Propriedade	Opção
Capacidade	2 ou superior (TB)
Fornecimento de Disco	Thin provision
Opções Avançadas	Não Configurar

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

O que Fazer Depois

Instale o software QRadar em sua máquina virtual.

Instalando o Software QRadar Incident Forensics em uma Máquina Virtual

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

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

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 de CD/DVD 1**.
5. Na área de janela **Status do dispositivo**, selecione a caixa de seleção **Conectar ao ligar**.
6. Na área de janela **Tipo de dispositivo**, selecione **Arquivo ISO do armazenamento de dados** e clique em **Pesquisar**.
7. Na janela Pesquisar armazenamentos de dados, localize e selecione o arquivo ISO do produto, clique em **Abrir** e clique em **OK**.
8. Após a imagem ISO do produto ser instalada, clique com o botão direito em sua máquina virtual e clique em **Ligar** > **Ligado.**
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 barra de espaço para avançar pelo documento.
11. Na página **Selecionar o ID do dispositivo**, escolha o componente QRadar Incident Forensics a ser instalado.
    - Para instalação distribuída, selecione **6000 QRadar Incident Forensics Processor**.
    - Para implementações independentes, selecione **6100 QRadar Incident Forensics Standalone**.
12. Para o tipo de configuração, selecione **normal**.
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 8. 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)	Não Suportados
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.

O que Fazer Depois

Se não estiver instalando o IBM Security QRadar Incident Forensics Standalone, consulte Capítulo 9, “Incluindo um host gerenciado QRadar Incident Forensics no QRadar Console”, na página 25.

Capítulo 7. Instalando o QRadar Console

Para instalações distribuídas, instale o QRadar Console em um dispositivo e o host gerenciado IBM Security QRadar Incident Forensics em outro dispositivo.

Restrição: As versões de software para todos os dispositivos em uma implementação devem ser da mesma versão e nível de correção. As implementações que usam diferentes versões do software não são suportadas.

Antes de Iniciar

Assegure que os requisitos a seguir sejam atendidos:

- O hardware requerido está instalado.
- Você possui a chave de licença necessária para seu dispositivo.
- Um teclado e monitor estão conectados usando a conexão VGA.
- Se desejar configurar interface de redes de ligação, consulte www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/).
- Não há licenças expiradas no console ou nos hosts gerenciados.

Importante: Se for solicitado um nome de usuário e uma senha antes de o assistente de instalação ser iniciado, digite `root` para o nome do usuário e `password` para a senha.

Procedimento

1. Para obter instalações sobre seu próprio hardware ou em máquinas virtuais, inclua a imagem ISO QRadar Console no diretório-raiz.
   a. Crie o diretório `/media/dvd` digitando o comando a seguir:
      ```
      mkdir /media/dvd
      ```
   b. Monte a imagem ISO do QRadar Console, digitando o comando a seguir:
      ```
      mount -o loop <QRadar_ISO> /media/dvd
      ```
2. Use o script de configuração para iniciar a instalação.
   a. Mude o diretório ativo digitando o comando: `cd /media/dvd`
   b. Inicie o script de configuração digitando o comando: `setup.sh`
3. Siga as instruções no assistente de instalação.
   - Em **Inserir sua chave de ativação abaixo**, quando solicitado pela chave de ativação, insira uma sequência alfanumérica de 24 dígitos e 4 partes que você recebeu a partir 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.
   - Na página **Inserir as informações de rede a serem usadas**, se você não tiver um servidor de email, insira `localhost` no campo **Nome do servidor de email**.
   - No **Campo de senha raiz**, crie uma senha que atende aos critérios a seguir:
     – Contém pelo menos 5 caracteres
     – Não contém espaços
     – Pode incluir os seguintes caracteres especiais: @, #, ^ e *.

O processo de instalação pode demorar vários minutos.

4. Aplique sua chave de licença.
   a. Efetue login no QRadar:

      `https://IP_Address_QRadar`

      O nome de usuário padrão é `admin`. A senha é aquela da conta do usuário raiz.
   b. Clique em **Efetuar login no QRadar**.
   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 lista **Exibir**, selecione **Licenças** e faça upload para sua chave de licença.
   g. Selecione a licença não alocada e clique em **Alocar sistema para licença**.
   h. Na lista de sistemas, selecione um sistema e clique em **Alocar sistema para a licença**.

O que Fazer Depois

Agora é possível instalar o QRadar Incident Forensics.

Capítulo 8. Instalando o QRadar Incident Forensics

Para instalações distribuídas, instale o QRadar Console em um dispositivo e o host gerenciado IBM Security QRadar Incident Forensics (QRadar Incident Forensics Processor) em outro dispositivo. Para implementações independentes, instale somente o componente QRadar Incident Forensics Standalone.

Restrição: As versões de software para todos os dispositivos em uma implementação devem ser da mesma versão e nível de correção. As implementações que usam diferentes versões do software não são suportadas.

Antes de Iniciar

Assegure que os requisitos a seguir sejam atendidos:

__ • O hardware requerido está instalado.

__ • O teclado e o monitor estão conectados usando a conexão VGA.

__ • A chave de ativação está disponível.

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

Procedimento

1. Para obter instalações sobre seu próprio hardware ou em máquinas virtuais, inclua a imagem ISO QRadar Incident Forensics no diretório-raiz.
   a. Crie o diretório `/media/dvd` digitando o comando a seguir:
      `mkdir /media/dvd`
   b. Monte a imagem ISO do QRadar Console, digitando o comando a seguir:
      `mount -o loop <QRadar_Incident_Forensics_ISO>/media/dvd`
2. Use o script de configuração para iniciar a instalação.
   a. Mude o diretório ativo digitando o comando: `cd /media/dvd`
   b. Inicie o script de configuração digitando o comando: `setup.sh`
3. Siga as instruções no assistente de instalação.

   Na página **Selecionar o ID do dispositivo**, escolha o componente QRadar Incident Forensics a ser instalado.

   - Para instalações distribuídas, selecione **6000 QRadar Incident Forensics Processor**
   - Para implementações independentes, selecione **6100 QRadar Incident Forensics Standalone**

   Restrição: As opções de configuração a seguir não são suportadas para QRadar Incident Forensics:

   - Na página Escolher o tipo de configuração, a opção **Configuração de recuperação de alta disponibilidade**
   - Na página Selecione se deseja usar o modo de configuração de interface seguro-garantia, a opção **Usar modo de configuração de interface seguro-garantia**

   Se você instalar o QRadar Incident Forensics Processor, o processo de instalação pode levar vários minutos.

4. Aplique sua chave de licença.
   a. Efetue login no QRadar:

      `https://IP_Address_QRadar`

      O nome de usuário padrão é `admin`. A senha é aquela da conta do usuário raiz.
   b. Clique no 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 da sua 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**.

   Nota: Se estiver instalando uma implementação independente (6100), deverá alocar duas chaves de licença para o dispositivo IBM Security QRadar Incident Forensics Standalone. Uma licença é para o QRadar Incident Forensics Standalone e a outra licença é para a guia **Forense**.

   Para cada instalação distribuída (6000) em um ambiente IBM Security QRadar SIEM existente, pode ser necessário ter uma licença para cada host gerenciado do Forensics (6000) e também uma única licença para ativar a guia **Forensics** no console. Se a sua chave de licença existente do QRadar Console está alocada para acesso à guia **Forensics**, é necessária somente a chave de licença de instalação. Se a sua chave de licença existente do QRadar Console não está alocada para acesso à guia **Forensics**, é necessária a chave de licença de instalação, bem como uma chave de ativação atualizada do Forensics.

O que Fazer Depois

Implemente o host gerenciado pelo QRadar Incident Forensics Processor. Para obter mais informações, consulte Capítulo 9, “Incluindo um host gerenciado QRadar Incident Forensics no QRadar Console”, na página 25.

Capítulo 9. Incluindo um host gerenciado QRadar Incident Forensics no QRadar Console

Para obter instalações distribuídas, você deve incluir IBM Security QRadar Incident Forensics Processor como um host gerenciado no QRadar Console.

Um *host gerenciado* é cada dispositivo QRadar não console na implementação. Para distribuir o processamento, é possível incluir mais de um QRadar Incident Forensics Processor como um host gerenciado.

Restrição: Usar o Editor de implementação para incluir ou remover os hosts gerenciados QRadar Incident Forensics não é suportado. Você deve usar a ferramenta de Gerenciamento de licença e de sistema.

Antes de Iniciar

Você deve instalar o software QRadar Console primeiro. Para obter mais informações, consulte Capítulo 7, "Instalando o QRadar Console", na página 21.

Procedimento

1. Efetue login no QRadar Console como um administrador:

   `https://IP_Address_QRadar`

   O nome de usuário padrão é `admin`. A senha é a senha da conta de usuário raiz que foi inserida durante a instalação.
2. Clique na guia **Administrador**.
3. Na área de janela **Configuração do sistema**, clique em **Gerenciamento de licença e de sistema**.
4. Na tabela de host, clique no host QRadar Console e clique em > **Ações de implementação** > **Incluir host**.
5. Insira as informações para o dispositivo QRadar Incident Forensics Processor e, em seguida, clique em **Incluir**.

   Restrição: As propriedades **Host de criptografia** e **Conversão de endereço de rede** não são suportadas.
6. Na barra de menus da guia **Administrador**, clique em **Implementar mudanças**.
7. Atualize o navegador da web.

   A guia **Forense** agora está visível.

O que Fazer Depois

É possível incluir um dispositivo IBM Security QRadar Packet Capture no QRadar Incident Forensics Processor. Para obter mais informações, consulte "Incluindo dispositivos de captura de pacote em hosts do QRadar Incident Forensics" na página 31.

Removendo um host gerenciado QRadar Incident Forensics

Para alterar as definições de configuração de rede ou se houver um problema para ver a guia **Forense**, é possível remover o host gerenciado QRadar Incident Forensics (IBM Security QRadar Incident Forensics Processor) da implementação QRadar. Se o host gerenciado QRadar Incident Forensics foi responsável pelas recuperações forenses, os dados são perdidos quando você incluir novamente o QRadar Incident Forensics Processor.

Se você não remover o host gerenciado QRadar Incident Forensics, mas, em vez disso, ele se tornar temporariamente não responsivo, devido à falha de energia ou outro problema, as tarefas para o host gerenciado ainda serão planejadas e serão processadas quando o host gerenciado ficar novamente online.

Restrição: Usar o Editor de implementação para incluir ou remover os hosts gerenciados QRadar Incident Forensics não é suportado. Você deve usar a ferramenta de Gerenciamento de licença e de sistema.

Procedimento

1. Efetue login no QRadar Console como um administrador:

   `https://IP_Address_QRadar`

   O nome de usuário padrão é `admin`. A senha é a senha da conta de usuário raiz que foi inserida durante a instalação.
2. Clique na guia **Administrador**.
3. Na área de janela **Configuração do sistema**, clique em **Gerenciamento de licença e de sistema**.
4. Na tabela do host, clique no host QRadar Incident Forensics Processor que você deseja remover e clique em > **Ações de implementação** > **Remover host**.
5. Na barra de menus da guia **Administrador**, clique em **Implementar mudanças**.
6. Atualize o navegador da web.

Capítulo 10. Conexões entre dispositivos de captura de pacote e o QRadar Incident Forensics

Para recuperar dados de captura de pacote, deve-se conectar um ou mais dispositivos de captura de pacote a um host gerenciado do IBM Security QRadar Incident Forensics ou componente QRadar Incident Forensics Standalone. Se nenhum dispositivo de captura de pacote for conectado, será possível fazer upload manualmente dos arquivos de captura de pacote na interface com o usuário ou usando o FTP.

Sistema principal de captura de pacote

Dependendo dos requisitos de rede e de captura de pacote, é possível conectar até cinco dispositivos de captura de pacote a um dispositivo QRadar Incident Forensics. Ao enviar uma recuperação, tarefas separadas são enviadas para cada dispositivo de captura de pacote em cada dispositivo QRadar Incident Forensics. Por exemplo, se instalar dois hosts gerenciados do QRadar Incident Forensics e cada um tiver duas capturas de pacote, quatro tarefas serão enviadas.

Os diagramas a seguir mostram que você pode conectar múltiplos dispositivos de captura de pacote a um host gerenciado de QRadar Incident Forensics (QRadar Incident Forensics Processor) ou dispositivos QRadar Incident Forensics Standalone.

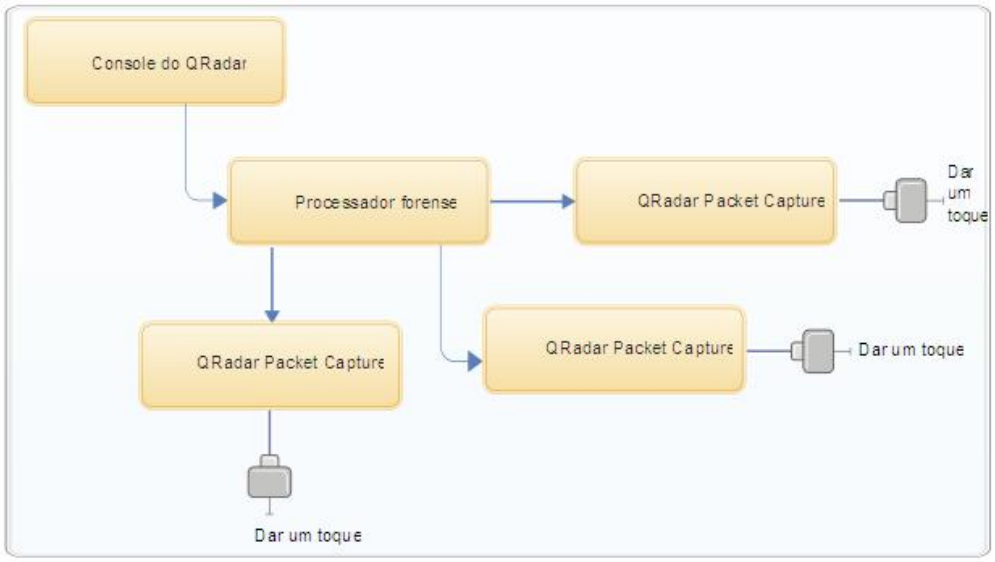


Figura 4. Exemplo de múltiplos dispositivos de captura de pacote conectados a um host gerenciado QRadar Incident Forensics

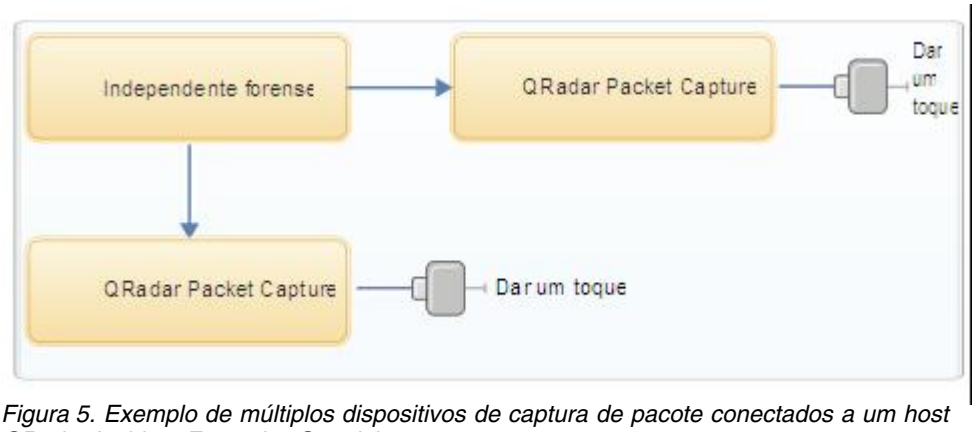
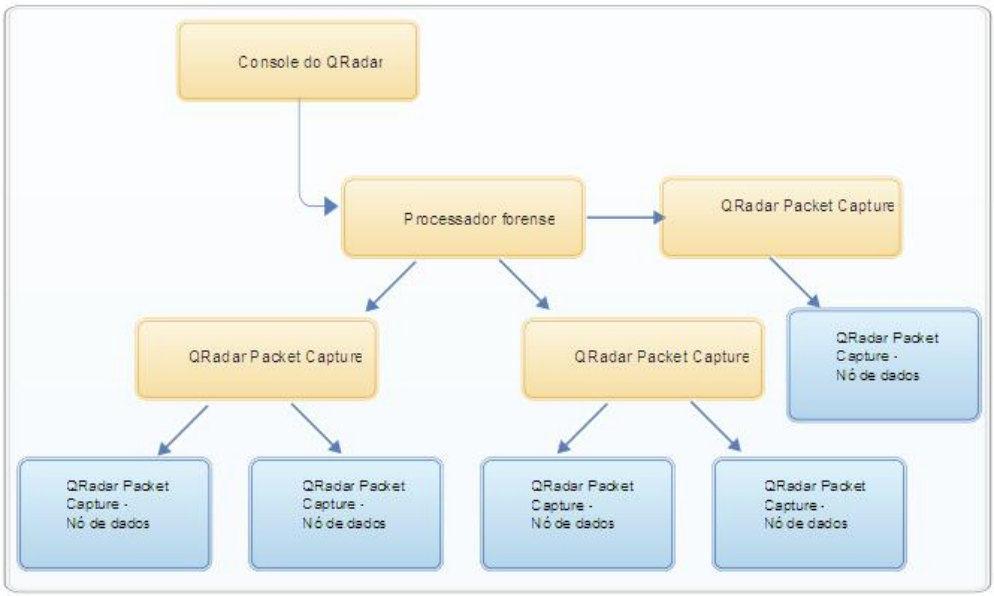


Figura 5. Exemplo de múltiplos dispositivos de captura de pacote conectados a um host QRadar Incident Forensics Standalone.

Dispositivos de nó de dados QRadar Packet Capture

Para capacidade de armazenamento extra, é possível conectar até dois dispositivos do Nó de dados QRadar Packet Capture a cada sistema principal QRadar Packet Capture. Cada dispositivo PCAP Data Node fornece 37 TB de área de armazenamento.



Depois de conectar os dispositivos de Nó de dados QRadar Packet Capture ao sistema principal, é possível configurar o cluster na interface com o usuário QRadar Packet Capture.

Para obter mais informações sobre as conexões físicas do dispositivo principal para o dispositivo de Nó de dados QRadar Packet Capture, consulte o *Guia de Referência Rápida do QRadar Packet Capture*. Para obter mais informações sobre a configuração do cluster de captura de pacote, consulte o *Guia do Usuário QRadar Packet Capture*.

Instalando o software QRadar Packet Capture em seu próprio dispositivo

Para assegurar uma instalação bem-sucedida do IBM Security QRadar Packet Capture no seu próprio dispositivo, deve-se instalar o sistema operacional Red Hat Enterprise Linux e o software QRadar Packet Capture. Você também deve assegurar que seu dispositivo atenda os requisitos do sistema.

Importante: O sistema no qual o software QRadar Packet Capture está instalado deve ser dedicado ao QRadar Packet Capture. Não instale os pacotes RPM que não são aprovados pela IBM. As instalações RPM não aprovadas podem causar erros de dependência ao fazer upgrade e também podem causar problemas de desempenho em sua implementação. Não use o YUM para atualizar seu sistema operacional ou instalar o software não aprovado nos sistemas QRadar Packet Capture.

Restrição: As instalações de software em uma máquina virtual não são suportadas.

Antes de Iniciar

Assegure-se de que seu dispositivo atenda aos requisitos do sistema a seguir:

Tabela 9. Requisitos do sistema para a instalação de um software QRadar Packet Capture

Especificação	Descrição
Processadores	Processadores de série Intel E5 V2 ou V3. As versões V4 requerem 6 núcleos ou mais.
Configurações do BIOS do processador	Deve suportar as normas do Intel AES e AVX introduzidos pela Intel em 2011. Configure suas definições do sistema BIOS para assegurar que a passagem do Hyper esteja ativada.
Memória	24 GB
Controlador RAID de hardware e armazenamento de extração e de captura	Configuração do RAID (usando uma combinação do RAID 0, 1 ou 5) entre um mínimo de 4 unidades de disco rígido, em que cada unidade de disco rígido tem o desempenho de, pelo menos, 7200 RPM e um mínimo de 1 TB por unidade
Unidade do sistema operacional	Unidade de disco rígido SATA ou SAS de classe corporativa de, no mínimo, 7200 RPM de 500 GB
Sistema operacional	Red Hat Enterprise Linux V6.7 **Nota:** O instalador SFS de 1 G deve ser instalado no sistema em que o PCAP de 1 G está instalado como um dispositivo PCAP dedicado. Ele não deve ser usado para nenhum outro propósito que não seja a captura de pacote.
Mínimo do total de espaço em disco	4 TB

Tabela 9. Requisitos do sistema para a instalação de um software QRadar Packet Capture (continuação)

Especificação	Descrição
NIC de captura (captura única de apoio de interface de 1 G ou 10 G para 1Gbps+)	Placas de rede PCI Express fabricadas pela Intel: • Adaptador PCI Express Intel E1G44ET2BLK Ethernet http://ark.intel.com/products/49187/Intel-Gigabit-ET2-Quad-Port-Server-Adapter • Adaptador de rede convergido Intel X520-SR2, portas duplas, 10 Gigabit Ethernet, PCI Express 2.0 x8, perfil baixo http://ark.intel.com/products/39774/Intel-Ethernet-Converged-Network-Adapter-X520-SR2 OU controladoras Ethernet Intel (qualquer adaptador de placa-mãe ou de rede que usa este controlador deveria funcionar: • Controlador Gigabit Ethernet Intel 82576 http://ark.intel.com/products/series/32261/Intel-82576-Gigabit-Ethernet-Controller OU placas de rede de computador base da Dell: • Adaptador para servidor Intel X520 DP 10Gb DA/SFP+ (DELL SKU#540-BBCT) http://accessories.ap.dell.com/sna/productdetail.aspx?c=sg&l=en&s=dhs&cs=sgdhs1&sku=540-11353 • Placa filha de rede Intel Ethernet i350 QP 1Gb (DELL SKU#540-BBCB) http://accessories.dell.com/sna/productdetail.aspx?c=us&l=en&s=gen&sku=430-4437 • Placa PCI Express de rede Intel Ethernet i350 QP 1Gb (DELL SKU#540-11357) http://accessories.ap.dell.com/sna/productdetail.aspx?c=au&l=en&s=bsd&cs=aubsd1&sku=540-11357
Interface de rede da interface com o usuário do PCAP	Qualquer interface de rede de 1 G ou (opcionalmente 10 G), por exemplo, eth0.

Antes de instalar o software QRadar Packet Capture em seu próprio dispositivo, sugere-se definir e configurar três unidades virtuais separadas. Essas unidades virtuais são para o sistema operacional, extração e armazenamento. A unidade de armazenamento deve ser a maior das três e o requisito mínimo para ela é de 4000 GB.

Consulte o seguinte exemplo:

Tabela 10. Exemplo de configuração do RAID para uma instalação de software do QRadar Packet Capture

Unidade Virtual	Nível de RAID	Tamanho

Tabela 10. Exemplo de configuração do RAID para uma instalação de software do QRadar Packet Capture (continuação)

0	RAID 1	128 GB
1	RAID 1	3587 GB
2	RAID 5	33527 GB

Procedimento

1. Insira o disco do sistema operacional Red Hat Enterprise Linux no seu dispositivo e reinicie-o.
2. 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. Na guia **Configurações de IPv4**, a partir da lista **Método**, selecione **Manual**.
   d. Na página Qual tipo de instalação você gostaria, selecione **Usar todo o espaço** e, em seguida, selecione a menor partição (partição de inicialização) para o sistema operacional no qual será instalado.
   e. Selecione somente a opção **Sistema base** a ser instalada.
3. Quando a instalação estiver concluída, clique em **Reinicializar**.
4. Copie o arquivo SFS do QRadar Packet Capture para seu dispositivo.
5. Monte o arquivo SFS do QRadar Packet Capture.
   a. Crie o diretório `/tmp/qpc_install`, digitando o comando a seguir:
      ```
      mkdir -p /tmp/qpc_install
      ```
   b. Monte o arquivo SFS do QRadar Packet Capture, digitando o comando a seguir:
      ```
      mount -o loop -t squashfs <QRadar_Packet_Capture_file.sfs>
      /tmp/qpc_install
      ```
   c. Acesse o diretório `/tmp/qpc_install`.
      ```
      cd /tmp/qpc_install
      ```
6. Para executar o script de instalação, digite o comando a seguir:
   ```
   sh installer.sh
   ```

Incluindo dispositivos de captura de pacote em hosts do QRadar Incident Forensics

Para fornecer aos investigadores acesso às informações de captura de pacote, é possível conectar até cinco dispositivos de captura de pacote a um host gerenciado do IBM Security QRadar Incident Forensics ou host IBM Security QRadar Incident Forensics Standalone. Os dispositivos de captura de pacote conectado processam os arquivos capturados para recuperações forenses.

Se nenhum dispositivo de captura de pacote for conectado, será possível fazer upload manualmente dos arquivos de captura de pacote na interface com o usuário ou usando o FTP.

Restrição: Usar o Editor de implementação para incluir dispositivos de captura de pacote não é suportado. Você deve usar a ferramenta de Gerenciamento de licença e de sistema.

Antes de Iniciar

Deve-se instalar e implementar um host gerenciado do QRadar Incident Forensics ou instalar um host do QRadar Incident Forensics Standalone. Para obter informações adicionais, consulte Capítulo 8, “Instalando o QRadar Incident Forensics”, na página 23 e Capítulo 9, “Incluindo um host gerenciado QRadar Incident Forensics no QRadar Console”, na página 25.

O diagrama interativo a seguir mostra as etapas principais no processo de instalação para instalações distribuídas. O processo de instalação é o mesmo para implementações independentes, mas você não implementa um host gerenciado.

Por padrão, o fuso horário para o dispositivo do QRadar Packet Capture é configurado como UTC (Hora Universal Coordenada).

Procedimento

1. Efetue login no QRadar Console como um administrador:

   `https://IP_Address_QRadar`

   O nome de usuário padrão é `admin`. A senha é a senha da conta de usuário raiz que foi inserida durante a instalação.
2. Clique na guia **Administrador**.
3. Na área de janela **Configuração do sistema**, clique em **Gerenciamento de licença e de sistema**.
4. Na tabela de host, selecione o QRadar Incident Forensics Processor (**Tipo de dispositivo** 6000) ou o host do QRadar Incident Forensics Standalone (**Tipo de dispositivo** 6100) e clique em **Ações de implementação** > **Editar host**
5. Clique em **Gerenciamento de componente**.
6. Para incluir dispositivos de captura de pacote, clique no ícone de adição (+) e insira as informações sobre o dispositivo.

   Dica: O nome do usuário padrão para o dispositivo QRadar Packet Capture é `continuum`.
7. Clique em **Salvar**.

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos EUA.

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 licenças 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:

Licença de propriedade intelectual
Lei de propriedade legal e intelectual
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tóquio 103-8510, Japão

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 renúncia de responsabilidade de garantias expressas ou implícitas em certas transações; portanto, essa instrução 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.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Gerência de Relações Comerciais e Industriais da IBM Brasil
Rio de Janeiro, RJ
CEP 22290-240
Brasil

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

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

Os dados de desempenho e os exemplos de cliente citados são apresentados apenas para propósitos ilustrativos. Os resultados de desempenho reais podem variar, dependendo das configurações específicas e das condições operacionais.

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

As instruções relacionadas aos objetivos e intenções futuros 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 podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com pessoas ou empresas reais é mera coincidência.

Marcas comerciais

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

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.

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

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

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

Termos e condições da documentação do produto

As permissões para uso destas publicações são concedidas sujeitas aos seguintes termos e condições.

Aplicabilidade

Estes termos e condições são acrescentados aos termos de uso do website da IBM.

Uso pessoal

O Cliente poderá reproduzir estas publicações para seu uso pessoal e não comercial, desde que todos os avisos do proprietário sejam preservados. O Cliente não pode distribuir, exibir ou criar trabalho derivado dessas publicações, ou de qualquer parte dela, sem o expresso consentimento da IBM.

Uso comercial

O Cliente pode reproduzir, distribuir e exibir essas publicações somente dentro de sua empresa, desde que todos os avisos do proprietário sejam preservados. O Cliente não pode reproduzir, distribuir ou exibir essa publicação, bem como fazer trabalhos derivados dela ou de qualquer parte nela contida fora de sua empresa sem o consentimento expresso da IBM.

Direitos

Exceto quando expressamente concedido nesta permissão, nenhum outro direito, licença ou permissão é concedido, expresso ou implícito, às publicações ou qualquer informação, dados, software ou outra propriedade intelectual nelas contidas.

A IBM reserva-se o direito de retirar as permissões aqui concedidas sempre que, ao seu critério, o uso das publicações for prejudicial para o seu interesse ou, conforme determinado pela IBM, as instruções acima não estiverem sendo devidamente seguidas.

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

A IBM NÃO FAZ NENHUMA GARANTIA QUANTO AO CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM" E SEM QUALQUER TIPO DE GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO, A GARANTIAS DE COMERCIALIZAÇÃO, NÃO VIOLAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

Declaração de privacidade on-line da IBM

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, 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 de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

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

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

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

Impresso no Brasil