Guia de Instalação
IBM Security QRadar Risk Manager
Versão 7.2.4

Guia de Instalação

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 25.

Informações do produto

Esse documento se aplica ao IBM QRadar Security Intelligence Platform V7.2.4 e às liberações subsequentes a menos que seja substituído por uma versão atualizada desse documento.

© Copyright IBM Corporation 2012, 2014.

Índice

© Copyright IBM Corp. 2012, 2014

Introdução à Instalação do IBM Security QRadar Risk Manager

Estas informações se destinam ao uso com o IBM® Security QRadar Risk Manager. O QRadar Risk Manager é um dispositivo usado para monitorar configurações do dispositivo, simular mudanças em seu ambiente de rede e priorizar riscos e vulnerabilidades de sua rede.

Esse guia contém instruções para instalação do QRadar Risk Manager e inclusão do QRadar Risk Manager como um host gerenciado no consoleIBM Security QRadar SIEM.

Os dispositivos QRadar Risk Manager são pré-instalados com software e um sistema operacional Red Hat Enterprise Linux. Também é possível instalar o software QRadar Risk Manager em seu próprio hardware.

Público alvo

Esse guia se destina a administradores de rede que são responsáveis pela instalação e configuração de sistemas QRadar Risk Manager em sua rede.

Os administradores precisam de um conhecimento de trabalho de rede e de sistemas Linux.

Documentação técnica

Para obter informações sobre como acessar a documentação mais técnica, notas técnicas e notas sobre a liberação, consulte Acessando a nota de documentação técnica do IBM Security (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Contatando o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte o Suporte e download de 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 proteger sistemas e informações por meio de prevenção, detecção e resposta para acesso incorreto de dentro e de fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mal uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum sistema de TI ou produto deve ser considerado completamente seguro e nenhum único produto, serviço ou medida de segurança pode ser completamente efetivo(a) na prevenção de uso ou acesso impróprio. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que envolverá necessariamente procedimentos operacionais adicionais, e poderão requerer que outros sistemas, produtos ou serviços sejam mais efetivos. A IBM NÃO GARANTE QUE NENHUM SISTEMA, PRODUTO OU SERVIÇO SEJA IMUNE OU TORNE A SUA EMPRESA IMUNE CONTRA A CONDUTA MALICIOSA OU ILEGAL DE TERCEIROS.

© Copyright IBM Corp. 2012, 2014

Capítulo 1. Prepare-se para instalar o IBM Security QRadar Risk Manager

É possível instalar um dispositivo IBM Security QRadar Risk Manager como um host gerenciado em seu console IBM Security QRadar. Apenas um QRadar Risk Manager pode existir em um console QRadar.

A partir da versão 7.1 do QRadar Risk Manager, o console QRadar e o QRadar Risk Manager usam o mesmo processo de instalação e o mesmo ISO para a instalação. Por esse motivo, é possível usar o editor de implementação no console QRadar para incluir o QRadar Risk Manager em sua implementação. Uma instalação do dispositivoQRadar Risk Manager inclui o software QRadar Risk Manager e um sistema operacional Red Hat Enterprise Linux.

Antes de instalar

Você deve concluir o processo de instalação para um console IBM Security QRadar antes de instalar o IBM Security QRadar Risk Manager. Como uma melhor prática, instale o QRadar SIEM e o QRadar Risk Manager no mesmo comutador de rede.

Para obter informações sobre a instalação do QRadar SIEM, inclusive os requisitos de hardware e software, consulte o *Guia de Instalação do IBM Security QRadar SIEM*.

Como o dispositivo IBM Security QRadar Risk Manager é de 64 bits, certifique-se de fazer download do software correto de instalação para seu sistema operacional.

Identificar configurações de rede

Deve-se reunir informações sobre suas configurações de rede antes de iniciar o processo de instalação.

Reúna as seguintes informações para suas configurações de rede:

- Nome do host
- endereço IP
- Endereço da máscara de rede
- Máscara de sub-rede
- Endereço de gateway padrão
- Endereço do servidor Sistema de Nomes de Domínio (DNS) principal
- Endereço do servidor DNS secundário (opcional)
- Endereço IP público para redes que usem nome de servidor de email de Conversão de Endereço de Rede (NAT)
- Nome do servidor de e-mail
- Servidor Network Time Protocol (NTP) (Console somente) ou nome do servidor de horário

Configurar o acesso a portas em firewalls

Os firewalls entre o console IBM Security QRadar e o IBM Security QRadar Risk Manager devem permitir tráfego em determinadas portas.

© Copyright IBM Corp. 2012, 2014

Assegure-se de que qualquer firewall localizado entre o console QRadar SIEM e o QRadar Risk Manager permita tráfego nas seguintes portas:

- Porta 443 (HTTPS)
- Porta 22 (SSH)
- Porta 37 UDP (Horário)

Recursos não suportados no QRadar Risk Manager

É importante estar ciente dos recursos que não são suportados pelo IBM Security QRadar Risk Manager.

Os recursos a seguir não são suportados no QRadar Risk Manager:

- Alta disponibilidade (HA)
- Roteamento Dinâmico para Protocolo de Roteamento de Borda (BGP), Open Shortest Path First (OSPF) ou Protocolo de Informações de Roteamento (RIP)
- IPv6
- Máscaras de rede não contíguas
- Rotas de carga balanceada
- Mapas de referência
- Armazenamento e Encaminhamento

Requisitos de Hardware Adicionais

Hardware adicional é requerido antes de poder instalar o IBM Security QRadar Risk Manager.

Antes de instalar os sistemas IBM QRadar Risk Manager, é necessário acessar os seguintes componentes de hardware:

- monitor e teclado ou um console serial
- Fonte de alimentação ininterrupta (UPS)

Sistemas ou dispositivos QRadar Risk Manager que estão executando o software QRadar Risk Manager que armazena dados devem ser equipados com uma fonte de alimentação ininterrupta (UPS). O uso de uma UPS garante que os dados do QRadar Risk Manager, como consoles, processadores de eventos e Coletores QFlow, sejam preservados durante uma falha de energia.

Requisitos de software adicionais

É requerido software adicional antes de poder instalar o IBM Security QRadar Risk Manager.

O software a seguir deve ser instalado no sistema desktop que você usa para acessar a interface com o usuário do QRadar Risk Manager:

- Java™ Runtime Environment
- Adobe Flash, versão 10 ou superior

Navegadores da web suportados

Para que os recursos em produtos IBM Security QRadar funcionem corretamente, você deverá usar um navegador da web suportado.

Ao acessar o sistema QRadar, será solicitado que você forneça um nome de usuário e uma senha. O nome do usuário e a senha devem ser configurados com antecedência pelo administrador.

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

Tabela 1. Navegadores da web suportados para produtos QRadar

Navegador da web	**Versões suportadas**
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer de 32 bits, com o modo de documento e modo de navegador ativados	9.0 10.0
Google Chrome	A versão atual a partir da data da liberação dos produtos IBM Security QRadar V7.2.4

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

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

Procedimento

1. No 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 do seu navegador da Web.
3. Clique em **Modo de documento**.
   - Para Internet Explorer V9.0, selecione **Padrões do Internet Explorer 9**.
   - Para o Internet Explorer V10.0, selecione **Padrões do Internet Explorer 10**.

Capítulo 2. Instale os dispositivos IBM Security QRadar Risk Manager

A implementação do IBM Security QRadar Risk Manager inclui um console IBM Security QRadar e um dispositivo QRadar Risk Manager como um host gerenciado.

A instalação do QRadar Risk Manager envolve as seguintes etapas:

1. Preparando seu dispositivo.
2. Instalando o QRadar Risk Manager.
3. Incluindo o QRadar Risk Manager no QRadar.

Preparando seu dispositivo

Você deve preparar seu dispositivo antes de instalar um dispositivo IBM Security QRadar Risk Manager.

Antes de Iniciar

Deve-se instalar todo o hardware necessário e você precisa de uma 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:

- 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.

Para evitar erros de digitação, a letra I e o número 1 (um) são tratados da mesma forma, assim como a letra O e o número 0 (zero).

Se você não tiver uma chave de ativação para o dispositivoQRadar Risk Manager, entre em contato com o suporte ao cliente (http://www.ibm.com/support).

Para obter informações sobre seu dispositivo, consulte o *Guia de Instalação do Hardware IBM Security QRadar*.

Procedimento

1. Escolha uma das opções a seguir:
   - Conecte um notebook à porta serial na parte traseira do dispositivo.

     Se você usar um notebook para conectar ao sistema, deverá usar um programa de terminal, como HyperTerminal, para conectar ao sistema. Certifique-se de configurar **Conectar Usando** à porta COM adequada do conector serial e **Bits por segundo** para 9600. Deve-se também configurar **Bits de Parada** (1), **Bits de Dado**s (8) e **Paridade** (Nenhuma).
   - Conecte um teclado e monitor a suas respectivas portas.
2. Ligue o sistema e efetue login. O nome do usuário, que distingue maiúsculas e minúsculas, é raiz.
3. Pressione Enter.
4. Leia as informações na janela. Pressione a Barra de Espaço para avançar cada janela até atingir o fim do documento.

© Copyright IBM Corp. 2012, 2014

5. Digite yes para aceitar o acordo e, em seguida, pressione Enter.
6. Digite sua chave de ativação e pressione Enter.

Acessar a interface com o usuário do IBM Security QRadar Risk Manager

O IBM QRadar Security Risk Manager usa informações de login padrão para a URL, o nome de usuário e a senha.

Você acessa o IBM Security QRadar Risk Manager por meio do console do QRadar. Use as informações na tabela a seguir ao efetuar login no console do IBM Security QRadar.

Tabela 2. Informações de login padrão do QRadar Risk Manager

Informações de login	Padrão
URL	https://<endereço IP>, em que <endereço IP> é o endereço IP do console do QRadar.
Nome de usuário	admin
Senha	A senha que é designada para o QRadar Risk Manager durante o processo de instalação.
Chave de licença	Uma chave de licença padrão fornece acesso ao sistema por 5 semanas.

Informações de parâmetro de rede para o IPv4

Informações de rede para configurações de rede do Protocolo da Internet versão 4 (IPv4) são requeridas ao instalar o IBM Security QRadar Risk Manager ou quando você alterar as configurações de rede.

Informações de rede são requeridas ao instalar ou reinstalar o IBM Security QRadar Risk Manager ou quando você precisar alterar configurações de rede.

A configuração de rede IP Pública é opcional. Esse endereço IP secundário é usado para acessar o servidor, geralmente de uma rede diferente ou da Internet e é gerenciado por seu administrador de rede. O endereço IP Público geralmente é configurado usando os serviços de Conversão de Endereço de Rede (NAT) nas configurações de rede ou do firewall em sua rede. O NAT converte um endereço IP em uma rede para um endereço IP diferente em outra rede.

Instalando o IBM Security QRadar Risk Manager

É possível instalar o IBM Security QRadar Risk Manager após preparar seu dispositivo.

Antes de Iniciar

Você deve concluir as etapas de preparação antes de instalar o QRadar Risk Manager.

Procedimento

1. Selecione normal para o tipo de configuração. Selecione **Avançar** e pressione Enter.

2. Selecione o continente ou área do fuso horário. Selecione **Avançar** e pressione Enter.
3. Selecione a região do fuso horário. Selecione **Avançar** e pressione Enter.
4. Selecione uma versão do protocolo da Internet. Selecione **Avançar** e pressione Enter.
5. Selecione a interface que você deseja especificar como a interface de gerenciamento. Selecione **Avançar** e pressione Enter.
6. Digite seu nome de host, endereço IP, máscara de rede, gateway, DNS primário, DNS secundário, IP público e servidor de email. Para obter informações do parâmetro de rede, consulte"Informações de parâmetro de rede para o IPv4" na página 6.
7. Selecione **Avançar** e pressione Enter.
8. Digite uma senha para configurar a senha raiz do QRadar Risk Manager.
9. Selecione **Avançar** e pressione Enter.
10. Redigite sua nova senha para confirmar. Selecione **Concluir** e pressione Enter. Esse processo geralmente leva vários minutos.

O que Fazer Depois

Use o editor de implementação para incluir o QRadar Risk Manager como um host gerenciado no console QRadar.

Incluindo o QRadar Risk Manager ao console do QRadar

Você deve incluir o IBM Security QRadar Risk Manager como um host gerenciado no console IBM Security QRadar.

Antes de Iniciar

Se você desejar ativar a compactação, então a versão mínima para cada host gerenciado deverá ser o console QRadar 7.1 ou o QRadar Risk Manager 7.1.

Para incluir um host gerenciado não ativado para NAT em sua implementação quando o Console for ativado para NAT, você deverá alterar o console QRadar para um host ativado para NAT. Deve-se alterar o console antes de incluir o host gerenciado em sua implementação. Para obter mais informações, consulte o *Guia de Administração do IBM Security QRadar SIEM*.

Procedimento

1. Abra seu navegador da web.
2. Digite a URL, `https://<IP Address>`, em que <IP Address> é o endereço IP do console QRadar.
3. Digite seu nome de usuário e senha.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. No menu, selecione **Ações** e, em seguida, selecione **Incluir um Host Gerenciado**.
6. Clique em **Avançar**.
7. Inserir valores para o parâmetros a seguir:

Opção	Descrição
Insira o IP do servidor ou dispositivo para incluir	O endereço IP do QRadar Risk Manager.

Opção	Descrição
Insira a senha raiz do host	A senha raiz para o host.
Confirme a senha raiz do host	Confirmação para sua senha.
O host é NATed	Para ativar NAT para um host gerenciado, a rede NATed deve estar usando tradução estática NAT. Para obter informações adicionais, consulte o Guia de Administração do *IBM Security QRadar SIEM*.
Ativar Criptografia	Cria um túnel de criptografia SSH para o host. Para ativar a criptografia entre dois hosts gerenciados, cada host gerenciado deve estar executando o console QRadar 7.1 ou o QRadar Risk Manager 7.1.
Ativar Compactação	Ativa a compactação de dados entre dois hosts gerenciados.

8. Escolha uma das opções a seguir:
   - Se você tiver marcado a caixa de seleção **Host é NATed**, deverá inserir valores para os parâmetros NAT.

Opção	Descrição
Insira o IP público do servidor ou dispositivo a incluir	O endereço IP público do host gerenciado. O host gerenciado usa esse endereço IP para se comunicar com outros hosts gerenciados em diferentes redes que usam NAT.
Selecione rede NATed	A rede que você deseja que este host gerenciado use. Se o host gerenciado estiver na mesma sub-rede do console QRadar, selecione o console da rede ativado para NAT. Se o host gerenciado não estiver na mesma sub-rede do console QRadar, selecione o host gerenciado da rede ativada para NAT.

   - Se você não tiver marcado a caixa de seleção **O Host é NATed**, clique em **Avançar**.
9. Clique em **Concluir**. Este processo pode levar vários minutos para ser concluído. Se a sua implementação incluir mudanças, você deverá implementar todas as mudanças.
10. Clique em **Implementar**.

O que Fazer Depois

Limpe o cache do navegador da web e, em seguida, efetue login no console QRadar. A guia **Riscos** agora está disponível.

Limpando o cache do navegador da web

Você deve limpar o cache do navegador da web browser para que possa acessar a guia **Riscos** no console QRadar.

Antes de Iniciar

Assegure-se de que somente um navegador da web esteja aberto. Se você tiver vários navegadores abertos, o cache poderá falhar na limpeza adequada.

Se você estiver usando um navegador da web Mozilla Firefox, você deverá limpar o cache de seu navegador da web Microsoft Internet Explorer também.

Procedimento

1. Abra seu navegador da web.
2. Limpe o cache do navegador da web. Para obter instruções, consulte a documentação do navegador da web.

Função de usuário do Risk Manager

Deve-se designar a função de usuário do Risk Manager para usuários que necessitem de acesso à guia **Riscos**.

Uma conta do usuário define a senha padrão e o endereço de email para um usuário. É necessário designar uma função de usuário e perfil de segurança para cada nova conta de usuário.

Antes de poder permitir acesso à funcionalidade IBM Security QRadar Risk Manager para outros usuários de sua organização, deve-se designar as permissões adequadas de função de usuário. Por padrão, o console QRadar fornece uma função administrativa padrão, que fornece acesso a todas as áreas do QRadar Risk Manager.

Para obter informações sobre a criação e gerenciamento de funções do usuário, consulte o*Guia de Administração do IBM Security QRadar SIEM*.

Designando a função de usuário do Risk Manager

É possível designar a função de usuário do Risk Manager para usuários que precisem de acesso à guia **Risco**.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do Sistema**.
3. Na área de janela **Gerenciamento do Usuário**, clique no ícone **Funções do Usuário**.
4. Clique no ícone **Editar** ao lado da função do usuário que você deseja editar.
5. Marque a caixa de seleção **Risk Manager**.
6. Clique em **Avançar**. Se você incluir Risk Manager na função de um usuário que tenha a permissão de Atividade de Log, você deverá, então, definir as origens de log que a função do usuário pode acessar. É possível incluir um grupo de origem de log inteiro clicando no ícone **Incluir** na área de janela **Grupo de Origem de Log**. É possível selecionar várias origens de log segurando a tecla Control e selecionando cada origem de log que você deseja incluir.
7. Clique em **Retornar**.
8. No menu da guia **Administração**, clique em **Implementar Mudanças**.

Guia Resolução de Problemas de Riscos

É possível resolver problemas se a guia **Riscos** não for exibida adequadamente ou estiver inacessível.

Quando a guia Riscos não for exibida adequadamente ou estiver inacessível, remova e leia o IBM Security QRadar Risk Manager como um host gerenciado.

Removendo um host gerenciado

É possível remover o host gerenciado do IBM Security QRadar Risk Manager do console IBM Security QRadar para alterar as configurações de rede ou se houver um problema com a guia **Riscos**.

Procedimento

1. Abra seu navegador da web.
2. Digite a URL `https://<IP Address>`, en que <IP Address> é o endereço IP do console QRadar.
3. Digite seu nome de usuário e senha.

   Para obter informações de login padrão, consulte Tabela 2 na página 6.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. Clique na guia **Visualização do sistema**.
6. Clique com o botão direito do mouse no host gerenciado que deseja excluir e selecione **Excluir**. Repita para cada host gerenciado que não seja do Console até que todos os hosts sejam excluídos.
7. Clique em **Salvar**.
8. Feche o editor de implementação.
9. Na guia **Admin**, clique em **Implementar Mudanças**.

Lendo o QRadar Risk Manager como um host gerenciado

Será possível ler o QRadar Risk Manager como host gerenciado depois de ele ser removido.

Procedimento

1. Abra seu navegador da web.
2. Digite a URL `https://<IP Address>`, en que <IP Address> é o endereço IP do console QRadar.
3. Digite seu nome de usuário e senha.

   Para obter informações de login padrão, consulte Tabela 2 na página 6.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. Clique na guia **Visualização do sistema**.
6. No menu, selecione **Ações** > **Incluir um host gerenciado**.
7. Clique em **Avançar**.
8. Inserir valores na janela Incluir novo host gerenciado.
9. Clique em **Avançar**.
10. Clique em **Concluir**. O processo de inclusão do QRadar Risk Manager pode levar vários minutos para ser concluído.
11. Feche o editor de implementação.
12. Na guia **Admin**, clique em **Implementar Mudanças**.

Capítulo 3. Instalações com unidade flash USB

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

As instalações com unidade flash USB são instalações integrais de produto. Não é possível usar uma unidade flash USB para atualizar ou aplicar correções de produtos. Para mais informações sobre aplicar fix packs, consulte as notas sobre a liberação do fix pack.

Versões suportadas

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

- Um dispositivo QRadar v7.2.1 ou posterior
- Um sistema Linux instalado com Red Hat Enterprise Linux 6.4
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 2008
- Microsoft Windows 2008R2

Visão geral da instalação

Siga este procedimento para instalar o software QRadar com uma unidade flash USB:

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

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

Criando uma unidade flash USB inicializável com um dispositivo QRadar

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

Antes de Iniciar

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

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

Se seu dispositivo QRadar não tiver conectividade com a Internet, será possível fazer o download do arquivo de imagem ISO QRadar para um computador

© Copyright IBM Corp. 2012, 2014

desktop ou outro dispositivo QRadar com acesso à Internet. Será possível, então, copiar o arquivo de imagem ISO para o dispositivo QRadar em que você tiver instalado o software.

Ao criar uma unidade flash USB inicializável, o conteúdo da unidade flash será excluído.

Procedimento

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

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

   `mount -o loop /tmp/<name of the ISO image>.iso /media/cdrom`
5. Digite o seguinte comando para copiar o script de criação do USB do ISO montado para o diretório `/tmp`.

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

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

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

    O processo de gravação da imagem ISO em sua unidade flash USB demora vários minutos para se concluir. Quando o ISO for carregado na unidade flash USB, uma mensagem de confirmação será exibida.
11. Pressione `q` para encerrar o script de chave do USB.
12. Remova a unidade flash USB do sistema QRadar.
13. Para liberar espaço, remova o arquivo de imagem ISO do arquivo `/tmp` do sistema.

O que Fazer Depois

Se a conexão com o dispositivo for uma conexão serial, consulte Configurando uma unidade flash para dispositivos que funcionam apenas com serial.

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

Criando uma unidade flash USB inicializável com Microsoft Windows

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

Antes de Iniciar

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

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

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

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

Deve-se fazer download dos seguintes arquivos da Internet.

- PeaZip Portable 4.8.1
- SYSLINUX 4.06

Dica: Procure o `Peazip Portal v4.8.1` e o `Syslinux` na web para encontrar os arquivos de download.

Ao criar uma unidade flash USB inicializável, o conteúdo da unidade flash será excluído.

Procedimento

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

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

   Não é necessário extrair os arquivos `.zip`. Os arquivos precisam apenas estar disponíveis no diretório `cuik/deps`.
3. Insira a unidade flash USB na porta USB do computador.
4. Verifique se a unidade flash USB está listada pela letra da unidade e se ela está acessível no Microsoft Windows.
5. Clique com o botão direito em `c:\cuik\cuik.exe`, selecione **Executar como administrador** e pressione **Enter**.
6. Pressione `1`, selecione o arquivo ISO QRadar e clique em **Abrir**.
7. Pressione `2` e selecione o número que corresponder à letra designada à unidade flash USB.
8. Pressione `3` para criar a unidade flash USB.
9. Pressione **Enter** para confirmar que você está ciente de que o conteúdo da unidade flash USB será excluído.
10. Digite `create` para criar uma unidade flash USB inicializável a partir da imagem ISO. Esse processo demora alguns minutos.
11. Pressione **Enter** e digite `q` para sair da ferramenta Create_USB_Install_Key.

12. Ejete a unidade flash USB do computador com segurança.

O que Fazer Depois

Se a conexão com o dispositivo for uma conexão serial, consulte Configurando uma unidade flash para dispositivos que funcionam apenas com serial.

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

Criando uma unidade flash USB inicializável com Red Hat Linux

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

Antes de Iniciar

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

- Uma unidade flash USB de 2 GB
- Um arquivo de imagem ISO QRadar V7.2.1 ou de versão posterior
- Um sistema Linux que tenha o seguinte software instalado:
  - Red Hat 6.4
  - Python 6.2 ou posterior

Ao criar uma unidade flash USB inicializável, o conteúdo da unidade flash será excluído.

Procedimento

1. Faça download do arquivo de imagem ISO QRadar.
   a. Acesse o website de suporte IBM (www.ibm.com/support).
   b. Localize o arquivo ISO IBM Security QRadar.
   c. Copie o arquivo de imagem ISO para um diretório `/tmp` do seu dispositivo QRadar.
2. Atualize o sistema baseado em Linux, de modo que ele inclua os seguintes pacotes.
   - syslinux
   - mtools
   - dosfstools
   - parted

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

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

   ```
   mount -o loop /tmp/<name of the ISO image>.iso /media/cdrom
   ```
6. Digite o seguinte comando para copiar o script de criação do USB do ISO montado para o diretório `/tmp`.

   ```
   cp /media/cdrom/post/create-usb-key.py /tmp/
   ```

7. Digite o seguinte comando para começar o script de criação do USB:
   `/tmp/create-usb-key.py`
8. Pressione `Enter`.
9. Pressione `1` e digite o caminho para o arquivo ISO. Por exemplo:
   `/tmp/Rhe664QRadar7_2_4_<build>.iso`
10. Pressione `2` e selecione a unidade que contiver a unidade flash USB.
11. Pressione `3` para criar a chave USB.

    O processo de gravação da imagem ISO em sua unidade flash USB demora vários minutos para se concluir. Quando o ISO for carregado na unidade flash USB, uma mensagem de confirmação será exibida.
12. Pressione `q` para encerrar o script de chave do USB.
13. Remova a unidade flash USB do sistema.

O que Fazer Depois

Se a conexão com o dispositivo for uma conexão serial, consulte Configurando uma unidade flash para dispositivos que funcionam apenas com serial.

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

Configurando uma unidade flash USB para dispositivos que funcionan somente com serial

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

Sobre Esta Tarefa

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

Procedimento

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

O que Fazer Depois

Agora, você estará pronto para instalar o QRadar com uma unidade flash USB.

Instalando o QRadar com uma unidade flash USB

Siga este procedimento para instalar o QRadar com uma unidade flash USB inicializável.

Antes de Iniciar

Deve-se criar uma unidade flash USB inicializável antes que você possa usá-la para instalar o software QRadar.

Sobre Esta Tarefa

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

O processo de instalação completo está documentado no guia de instalação do produto.

Procedimento

1. Instale todo o hardware necessário.
2. Escolha uma das opções a seguir:
   - Conecte um notebook à porta serial na parte traseira do dispositivo.
   - Conecte um teclado e monitor a suas respectivas portas.
3. Insira a unidade flash USB inicializável na porta USB do dispositivo.
4. Reinicie o dispositivo.

   A maioria dos dispositivos pode ser inicializada por padrão com uma unidade flash USB. Se você estiver instalando um software QRadar em seu próprio hardware, poderá ser necessário configurar a ordem de inicialização do dispositivo, de modo a priorizar o USB.

   Após o dispositivo iniciar, a unidade flash USB preparará o dispositivo para instalação. Esse processo pode levar até 1 hora para ser concluído.
5. Quando o menu do **Red Hat Enterprise Linux** for exibido, selecione uma das seguintes opções:
   - Se você tiver conectado um teclado e um monitor, selecione **Instalar ou atualizar usando console VGA**.
   - Se você tiver conectado um notebook com uma conexão serial, selecione **Instalar ou atualizar usando console serial**.
6. Digite `SETUP` para iniciar a instalação.
7. Quando o prompt de login for exibido, digite `root` para efetuar login no sistema como usuário-raiz.

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

   O processo de instalação completo está documentado no guia de instalação do produto.

Capítulo 4. Reinstale o IBM Security QRadar Risk Manager a partir da partição de recuperação

Quando você reinstala o IBM Security QRadar Risk Manager a partir do ISO do console IBM Security QRadar na partição de recuperação, o seu sistema é restaurado novamente para a configuração padrão de fábrica. Isso significa que seus arquivos de dados e de configuração atuais são sobrescritos.

Essas informações se aplicam às novas instalações ou upgrades do QRadar Risk Manager das novas instalações do QRadar Risk Manager nos dispositivos QRadar Risk Manager. Quando você instala o QRadar Risk Manager, o instalador (ISO do console QRadar) é copiado na partição de recuperação. A partir dessa partição, é possível reinstalar o QRadar Risk Manager, que restaura o QRadar Risk Manager para padrões de fábrica.

Nota: Se você fizer upgrade de seu software após instalar o QRadar Risk Manager, o arquivo ISO será substituído pela versão mais nova.

Quando você reinicializar o dispositivo QRadar Risk Manager, será apresentada uma opção de reinstalar o software. Como o console QRadar e o QRadar Risk Manager usam o mesmo arquivo de instalação ISO, o nome do ISO do console QRadar é exibido.

Se você não responder ao prompt após 5 segundos, o sistema reinicializará normalmente, o que mantém seus arquivos de dados e de configuração. Se você optar por reinstalar o ISO do console QRadar, uma mensagem de aviso será exibida e você deverá confirmar que deseja reinstalar o software. Após a confirmação, o instalador é executado e é possível seguir os prompts no processo de instalação.

Após uma falha no disco rígido, não é possível reinstalar a partir da partição de recuperação, porque não está mais disponível. Se você experimentar uma falha de disco rígido, entre em contato com o suporte ao cliente para obter assistência.

Reinstalando o QRadar Risk Manager usando a reinstalação de factory

É possível reinicializar e reinstalar o dispositivo QRadar Risk Manager usando a opção de reinstalação de factory.

Antes de Iniciar

Assegure-se de ter sua chave de ativação, que é uma sequência alfanumérica de 24 dígitos e quatro partes, que você recebe da IBM. É possível localizar a chave:

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

Para evitar erros de digitação, a letra I e o número 1 (um) são tratados da mesma forma, assim como a letra O e o número 0 (zero).

Se você não tiver uma chave de ativação para o dispositivoQRadar Risk Manager, entre em contato com o suporte ao cliente (http://www.ibm.com/support).

© Copyright IBM Corp. 2012, 2014

As chaves de ativação de software não requerem números de série.

Procedimento

1. Reinicialize o dispositivo QRadar Risk Manager.
2. Selecione **reinstalação de factory**.
3. Digite `comprimir` para continuar. O disco rígido é particionado e reformatado, o SO é instalado e, em seguida, o QRadar Risk Manager é reinstalado. Você deve aguardar a conclusão do processo de compressão. Esse processo pode levar vários minutos, dependendo de seu sistema.
4. Digite `SETUP`.
5. Efetue login no QRadar Risk Manager como usuário raiz.
6. Leia as informações na janela. Pressione a Barra de Espaço para avançar cada janela até atingir o fim do documento. Digite `yes` para aceitar o acordo e, em seguida, pressione Enter.
7. Digite sua chave de ativação e pressione Enter.
8. Selecione **normal** para o tipo de configuração. Selecione **Avançar** e pressione Enter.
9. Selecione o continente ou área do fuso horário. Selecione **Avançar** e pressione Enter.
10. Selecione a região do fuso horário. Selecione **Avançar** e pressione Enter.
11. Selecione uma versão do protocolo da Internet. Selecione **Avançar** e pressione Enter.
12. Selecione a interface que você deseja especificar como a interface de gerenciamento. Selecione **Avançar** e pressione Enter.
13. Insira as informações para o nome do host, endereço IP, máscara de rede, gateway, DNS primário, DNS secundário, IP público e servidor de email. Para obter informações de rede, consulte “Informações de parâmetro de rede para o IPv4” na página 6.
14. Digite uma senha para configurar a senha raiz do QRadar Risk Manager.
15. Selecione **Avançar** e pressione Enter.
16. Redigite sua nova senha para confirmar. Selecione **Concluir** e pressione Enter. Esse processo geralmente leva vários minutos.
17. Pressione Enter para selecionar OK.
18. Pressione Enter para selecionar OK.

O que Fazer Depois

Use o editor de implementação para incluir o QRadar Risk Manager como um host gerenciado no console QRadar.

Capítulo 5. Altere as configurações de rede

É possível alterar as configurações de rede de um dispositivo IBM Security QRadar Risk Manager que esteja conectado a um console IBM Security QRadar.

Se você precisar alterar as configurações de rede, você deverá, em seguida, concluir estas tarefas na seguinte ordem:

1. Remova oQRadar Risk Manager como um host gerenciado.
2. Altere as configurações de rede.
3. Leia QRadar Risk Manager como host gerenciado.

Removendo um host gerenciado

É possível remover o host gerenciado do IBM Security QRadar Risk Manager do console IBM Security QRadar para alterar as configurações de rede ou se houver um problema com a guia **Riscos**.

Procedimento

1. Abra seu navegador da web.
2. Digite a URL `https://<IP Address>`, en que <IP Address> é o endereço IP do console QRadar.
3. Digite seu nome de usuário e senha.

   Para obter informações de login padrão, consulte Tabela 2 na página 6.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. Clique na guia **Visualização do sistema**.
6. Clique com o botão direito do mouse no host gerenciado que deseja excluir e selecione **Excluir**. Repita para cada host gerenciado que não seja do Console até que todos os hosts sejam excluídos.
7. Clique em **Salvar**.
8. Feche o editor de implementação.
9. Na guia **Admin**, clique em **Implementar Mudanças**.

Alterando as configurações de rede

É possível alterar as configurações de rede de um dispositivo IBM Security QRadar Risk Manager que esteja conectado a um console IBM Security QRadar.

Antes de Iniciar

Você deve remover o host gerenciado do QRadar Risk Manager do console QRadar para que possa alterar as configurações de rede.

Procedimento

1. Usando SSH, efetue login no QRadar Risk Manager como usuário raiz.
2. Digite o comando, `qchange_netsetup`.
3. Selecione uma versão do protocolo da Internet. Selecione **Avançar** e pressione Enter. Dependendo de sua configuração de hardware, a janela exibe até um máximo de quatro interfaces. Cada interface com um link físico é denotada com um símbolo de mais (+).

© Copyright IBM Corp. 2012, 2014

4. Selecione a interface que você deseja especificar como a interface de gerenciamento. Selecione **Avançar** e pressione Enter.
5. Insira as informações para o nome do host, endereço IP, máscara de rede, gateway, DNS primário, DNS secundário, IP público e servidor de email. Para obter informações de rede, consulte "Informações de parâmetro de rede para o IPv4" na página 6.
6. Digite uma senha para configurar a senha raiz do QRadar Risk Manager.
7. Selecione **Avançar** e pressione Enter.
8. Redigite sua nova senha para confirmar. Selecione **Concluir** e pressione Enter. Esse processo geralmente leva vários minutos.

Lendo o QRadar Risk Manager como um host gerenciado

Será possível ler o QRadar Risk Manager como host gerenciado depois de ele ser removido.

Procedimento

1. Abra seu navegador da web.
2. Digite a URL `https://<IP Address>`, en que <IP Address> é o endereço IP do console QRadar.
3. Digite seu nome de usuário e senha.

   Para obter informações de login padrão, consulte Tabela 2 na página 6.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. Clique na guia **Visualização do sistema**.
6. No menu, selecione **Ações** > **Incluir um host gerenciado**.
7. Clique em **Avançar**.
8. Inserir valores na janela Incluir novo host gerenciado.
9. Clique em **Avançar**.
10. Clique em **Concluir**. O processo de inclusão do QRadar Risk Manager pode levar vários minutos para ser concluído.
11. Feche o editor de implementação.
12. Na guia **Admin**, clique em **Implementar Mudanças**.

Capítulo 6. Backup e restauração de dados

É possível usar um script da interface da linha de comandos (CLI) para fazer backup dos dados que são armazenados nos hosts gerenciados do console IBM Security QRadar.

É possível usar o script da CLI da para restaurar o IBM Security QRadar Risk Manager após uma falha de dados ou falha de hardware no dispositivo.

Um script de backup é incluído no QRadar Risk Manager, que pode ser programado usando crontab. O script cria automaticamente um archive diário dos dados do QRadar Risk Manager às 3h. Por padrão, o QRadar Risk Manager mantém os cinco últimos backups. Se você tiver rede ou armazenamento anexado, deverá criar uma tarefa cron para copiar os archives de fundo do QRadar Risk Manager para um local de armazenamento de rede.

O archive de backup inclui os seguintes dados:

- Configurações do dispositivo do QRadar Risk Manager
- Dados de conexão
- Dados de topologia
- Perguntas do Monitor de Política
- Tabelas de banco de dados do QRadar Risk Manager

Para obter informações sobre migração da liberação de manutenção 5 do QRadar Risk Manager Maintenance para a liberação atual, consulte o *Guia de migração do IBM Security QRadar Risk Manager*.

Pré-requisitos para backup e restauração de dados

Deve-se entender como ocorre o backup dos dados, como são armazenados e arquivados antes de poder fazer backup e restaurar seus dados.

Local de backup de dados

O backup de dados ocorre no diretório local `/store/qrm_backups`. Seu sistema pode incluir uma montagem `/store/backup` de um SAN externo ou serviço NAS. Os serviços externos fornecem retenção de dados offline de longo prazo. O armazenamento de longo prazo pode ser requerido por regulamentos de conformidade, como padrões Payment Card Industry (PCI).

Versão do dispositivo

A versão do dispositivo que criou o backup no archive está armazenada. Um backup somente poderá ser restaurado em um dispositivo QRadar Risk Manager se for da mesma versão.

Frequência de backup de dados e informações de archive

Backups diários de dados são criados às 3h. Somente os últimos cinco arquivos de backup são armazenados. Um archive de backup será criado se houver espaço livre suficiente no QRadar Risk Manager.

© Copyright IBM Corp. 2012, 2014

Formato dos arquivos de backup

Use o seguinte formato para salvar arquivos de backup: backup-<target date>-<timestamp>.tgz

Em que:

<data prevista> é a data em que o arquivo de backup foi criado.

O formato da data de destino é <dia>_<mês>_<ano>. <registro de data e hora> é o horário em que o arquivo de backup foi criado. O formato do registro de data e hora é <hora>_<minuto>_<segundo>.

Fazendo backup de seus dados

O backup automático ocorre diariamente, às 3h da manhã, ou é possível iniciar o processo de backup manualmente.

Procedimento

1. Usando SSH, efetue login no console do QRadar como usuário-raiz.
2. Usando SSH a partir do console do QRadar, efetue login no QRadar Risk Manager como usuário-raiz.
3. Inicie um backup do QRadar Risk Manager digitando /opt/qradar/bin/dbmaint/risk_manager_backup.sh

Resultados

O script que é usado para iniciar o processo de backup pode levar vários minutos para iniciar.

Após o script concluir o processo de backup, é exibida a mensagem a seguir:

```
Ter 11 de set 10:14:41 EDT 2012
- Backup do Risk Manager concluído,
wrote /store/qrm_backups/backup-2012-09-11-10-14-39.tgz
```

Restaurando dados

É possível usar um script de restauração para restaurar dados a partir de um backup do QRadar Risk Manager.

Antes de Iniciar

O dispositivo QRadar Risk Manager e o archive de backup devem ser da mesma versão do QRadar Risk Manager. Se o script detectar uma diferença de versão entre o archive e o host gerenciado do QRadar Risk Manager, será exibido um erro.

Sobre Esta Tarefa

Use o script de restauração para especificar o archive que você está restaurando para o QRadar Risk Manager. Esse processo requer que você pare os serviços no QRadar Risk Manager. Parar os serviços desconecta todos os usuários do QRadar Risk Manager e para vários processos.

A tabela a seguir descreve os parâmetros que é possível usar para restaurar um archive de backup.

Tabela 3. Parâmetros usados para restaurar um archive de backup para o QRadar Risk Manager

Opção	Descrição
-f	Sobrescreve todos os dados existentes do QRadar Risk Manager em seu sistema com os dados do arquivo de restauração. A seleção desse parâmetro permite que o script sobrescreva quaisquer configurações existentes do dispositivo no Gerenciamento de Origem de Configuração com as configurações do dispositivo do arquivo de backup.
-w	Não exclua diretórios antes de restaurar os dados do QRadar Risk Manager.
-h	A ajuda para o script de restauração.

Procedimento

1. Usando SSH, efetue login no console QRadar SIEM como usuário-raiz.
2. Usando SSH, a partir do console QRadar SIEM, efetue login no QRadar Risk Manager como usuário-raiz.
3. Pare o contexto do host digitando `service hostcontext stop`.
4. Digite o seguinte comando para restaurar um archive de backup para o QRadar Risk Manager: `/opt/qradar/bin/risk_manager_restore.sh -r /store/qrm_backups/<backup>`. Em que `<backup>` é o archive do QRadar Risk Manager que você deseja restaurar.

   Por exemplo, backup-2012-09-11-10-14-39.tgz.
5. Inicie o contexto do host digitando `service hostcontext start`.

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

A IBM pode não oferecer os produtos, serviços ou recursos discutidos neste documento 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 usados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá se usado em substituição a este produto, programa ou serviço. Porém, é de responsabilidade do usuário a avaliação e a verificação da operação de qualquer produto, programa ou serviço que não seja da IBM.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento deste documento não lhe concede qualquer licença para estas 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 consultas sobre licenças a respeito de informações do conjunto de caracteres de byte duplo (DBCS), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie consultas, 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 ao Reino Unido ou a qualquer país em que tais disposições não estejam de acordo com a legislação local:

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA" SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Estas informações podem incluir imprecisões técnicas ou erros tipográficos. Alterações são periodicamente feitas nas informações aqui existentes e essas alterações serão incorporadas em novas edições da publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar o(s) produto(s) e/ou o(s) programa(s) descrito(s) nesta publicação, sem aviso prévio.

© Copyright IBM Corp. 2012, 2014

Referências nestas informações a Web sites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses Web sites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e o usão desses websites é de inteira responsabilidade do Cliente.

A IBM pode usar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o cliente.

Qualquer pessoa detentora de uma licença deste programa que desejar obter informações sobre ele com o objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações que foram trocadas, deve 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 apropriados, 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 obtidos em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais poderão variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão as mesmas em sistemas disponíveis em geral. Além disso, algumas medidas foram estimadas por meio de extrapolação. Os resultados reais podem variar. Usuários deste documento devem verificar os dados aplicáveis para seus ambientes específicos.

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 esses produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Perguntas sobre os recursos de produtos não IBM devem ser endereçadas aos fornecedores desses produtos.

Todas as declarações, referentes a futuros planos ou intenções da IBM, estão sujeitas à alteração ou remoção sem aviso prévio e representam apenas metas e objetivos.

Todos os preços IBM mostrados são preços de varejo atuais sugeridos pela IBM e estão sujeitos a alteração sem aviso prévio. Os preços do revendedor podem variar.

Estas informações contêm exemplos de dados e relatórios usados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer similaridade com nomes e endereços usados por uma empresa real é mera coincidência.

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

Marcas Comerciais

IBM, o logotipo IBM e ibm.com são marcas ou marcas comerciais 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 ™), esses símbolos indicarão marcas registradas ou de direito consuetudinário dos Estados Unidos, de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou marcas comerciais de direito consuetudinário em outros países. Uma lista atual de marcas registradas da IBM está disponível na web em Informações de copyright e de marca registrada (www.ibm.com/legal/copytrade.shtml).

Adobe e Acrobat e todas as marcas comerciais baseadas em Adobe são marcas registradas ou marcas comerciais da Adobe Systems Incorporated nos Estados Unidos, em outros países ou ambos.

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros países.

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

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

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

Considerações de política de privacidade

Os produtos de software IBM, incluindo soluções de software como serviço, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações sobre o uso do produto, para ajudar a melhorar a experiência do usuário final, customizar as interações com o usuário final ou para outros propósitos. Em muitos 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, as informações específicas sobre o uso de cookies desta oferta serão configuradas abaixo.

Dependendo das configurações implementadas, essa Oferta de software poderá usar cookies de sessão que coletam o ID da sessão de cada usuário para fins 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 capacidade de coletar, como cliente, informações pessoalmente identificáveis dos usuários finais por meio de cookies e outras tecnologias, deve-se consultar seu próprio conselho jurídico a respeito das leis aplicáveis a essa coleta de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter mais informações sobre o uso das diversas tecnologias, incluindo cookies, para esses propósitos, consulte a Política de Privacidade da IBM no endereço http://www.ibm.com/privacy e a Declaração de Privacidade Online da IBM em http://www.ibm.com/privacy/details, a seção denominada “Cookies, web beacons e outras tecnologias” e “Declaração de privacidade de software como um serviço e de produtos de software IBM" no endereço http://www.ibm.com/software/info/product-privacy.

Índice Remissivo

© Copyright IBM Corp. 2012, 2014