IBM Security QRadar Risk Manager
Versão 7.2.5

Guia de Instalação

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 19.

Informações do produto

Esse documento se aplica ao IBM QRadar Security Intelligence Platform V7.2.5 e às liberações subsequentes a menos que seja substituído por uma versão atualizada desse documento.

Índice

Introdução à Instalação do IBM Security QRadar Risk Manager

Estas informações são destinadas ao uso com 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 em sua rede.

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

Os dispositivos QRadar Risk Manager são pré-instalados com software e um sistema operacional Red Hat Enterprise Linux. Você também pode 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 localizar a documentação do produto do IBM Security QRadar na web, incluindo toda a documentação traduzida, acesse o IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Para obter informações sobre como acessar a documentação mais técnica na biblioteca dos produtos QRadar, consulte Acessando o IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

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?uid=swg21616144).

Declaração de boas práticas de segurança

A segurança do sistema de TI envolve proteger sistemas e informações por meio de prevenção, detecção e resposta 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 legal abrangente, que envolverá, necessariamente, procedimentos operacionais adicionais e poderão

requerer outros sistemas, produtos ou serviços para serem 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.

Observação:

O uso deste Programa pode envolver diversas leis ou regulamentos, incluindo aqueles relacionados a privacidade, proteção de dados, empregabilidade, e armazenamento e comunicações eletrônicas. O IBM Security QRadar pode ser usado apenas com propósitos legais e de forma legal. O cliente concorda em usar esse programa conforme, e assume todas as responsabilidades de obedecer a, leis aplicáveis, regulamentos e políticas. O Licenciado declara que obterá ou que obteve quaisquer consentimentos, permissões ou licenças necessárias para permitir o uso legal do IBM Security QRadar.

Capítulo 1. Preparar para instalar o IBM Security QRadar Risk Manager

Você instala um dispositivo IBM Security QRadar Risk Manager como um host gerenciado em seu IBM Security QRadar SIEM Console. Somente um QRadar Risk Manager pode existir em um QRadar Console.

O QRadar Console e o QRadar Risk Manager usam o mesmo processo de instalação e imagem ISO. Depois de instalar o console do QRadar e o QRadar Risk Manager, inclua o QRadar Risk Manager como um host gerenciado usando a ferramenta **Gerenciamento de Sistema e Licença** na guia **Admin**. Um dispositivo QRadar Risk Manager é pré-instalado com 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 IBM Security QRadar SIEM Console antes de instalar o IBM Security QRadar Risk Manager. Como uma melhor prática, instale o QRadar SIEM e o QRadar Risk Manager na mesma comutação de rede.

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

Como o QRadar Risk Manager é um dispositivo de 64 bits, certifique-se de ter feito o download do software de instalação correto 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

Firewalls entre o IBM Security QRadar SIEM Console e o IBM Security QRadar Risk Manager devem permitir tráfego em determinadas portas.

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

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

Recursos não suportados no IBM Security QRadar Risk Manager

É importante estar ciente dos recursos que não são suportados pelo 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 QRadar Risk Manager, é necessário acessar os componentes de hardware a seguir:

- Monitor e teclado
- Fonte de alimentação ininterrupta (UPS)

Dispositivos ou sistemas do 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

Software adicional é necessário antes de você 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. Instalar dispositivos IBM Security QRadar Risk Manager

Uma implementação do IBM Security QRadar Risk Manager inclui um dispositivo IBM Security QRadar SIEM Console e QRadar Risk Manager como um host gerenciado.

A instalação do QRadar Risk Manager envolve as etapas a seguir:

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 dispositivo QRadar Risk Manager, entre em contato com o Suporte ao Cliente (www.ibm.com/support/).

Para obter informações, consulte *IBM Security QRadar Hardware Installation Guide*.

Procedimento

1. 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.
5. Digite yes para aceitar o contrato 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 Security QRadar Risk Manager usa as informações de login padrão para a URL, nome de usuário e senha.

Você acessa o QRadar Risk Manager através do IBM Security QRadar SIEM Console. Use as informações na tabela a seguir quando efetuar login no QRadar Console.

Tabela 2. Informações de login padrão para QRadar Risk Manager

Informações de login	Padrão
URL	`https://<IP address>`, em que *<IP address>* é o endereço IP do QRadar Console.
Nome de usuário	admin
Senha	A senha que é designada ao 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 necessárias ao instalar o IBM Security QRadar Risk Manager ou ao alterar as configurações de rede.

Informações de rede são requeridas ao instalar ou reinstalar o QRadar Risk Manager ou ao precisar alterar as 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

Você pode 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.

Incluindo o IBM Security QRadar Risk Manager no IBM Security QRadar SIEM Console

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

Antes de Iniciar

Se desejar ativar a compactação, a versão mínima para cada host gerenciado deve ser QRadar Console 7.1 ou 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 QRadar Console para um host ativado para NAT. Deve-se alterar o console antes de incluir o host gerenciado em sua implementação. Para obter informações adicionais, 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 QRadar Console.
3. Digite seu nome de usuário e senha.
4. Clique na guia **Admin**.
5. Na área de janela **Configuração do Sistema**, clique em **Gerenciamento de Sistema e Licença**.
6. Na janela Gerenciamento de Sistema e Licença, clique em **Ações de Implementação** e, em seguida, selecione **Incluir Host**.
7. Clique em **Avançar**.
8. Inserir valores para o parâmetros a seguir:

Opção	Descrição
IP do Host	O endereço IP do QRadar Risk Manager.
Senha do Host	A senha raiz para o host.
Confirmar Senha do Host	Confirmação para sua senha.
Conversão de Endereço de Rede	Para ativar NAT para um host gerenciado, a rede ativada para NAT deve estar usando tradução estática NAT. Para obter informações adicionais, consulte o *Guia de administração do IBM Security QRadar SIEM*.

Opção	Descrição
Criptografar Host	Cria um túnel de criptografia SSH para o host. Para ativar a criptografia entre dois hosts gerenciados, cada host gerenciado deve estar executando o QRadar Console 7.1 ou o QRadar Risk Manager7.1.
Compactação de Criptografia	Ativa a compactação de dados entre dois hosts gerenciados.

9. Se você tiver marcado a caixa de seleção **Conversão de Endereço de Rede**, deverá inserir valores para os parâmetros NAT:

Opção	Descrição
IP Público	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.
Grupo NAT	A rede que você deseja que este host gerenciado use. Se o host gerenciado estiver na mesma sub-rede do QRadar Console, selecione o console da rede ativado para NAT. Se o host gerenciado não estiver na mesma sub-rede do QRadar Console, selecione o host gerenciado da rede ativado para NAT.

10. Clique em **Incluir**. Este processo pode levar vários minutos para ser concluído. Se a sua implementação incluir mudanças, você deverá implementar todas as mudanças.
11. Clique em **Implementar Mudanças** na guia **Administrador**.

O que Fazer Depois

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

Limpando o cache do navegador da web

Você deve limpar o cache do navegador da web antes de poder acessar a guia **Riscos** no IBM Security QRadar SIEM Console.

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 QRadar Console 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 Risco não estiver sendo exibida adequadamente ou estiver inacessível, remova e reinclua o IBM Security QRadar Risk Manager como um host gerenciado.

Removendo um host gerenciado

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

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 do usuário raiz que foi inserida durante a instalação.
2. Clique na guia **Admin**.
3. Na área de janela **Configuração do Sistema**, clique em **Gerenciamento de Sistema e Licença**.
4. Na tabela de host, clique no host QRadar Risk Manager que deseja remover e clique em **Ações de Implementação** > **Remover Host**.
5. Na barra de menus da guia **Administrador**, clique em **Implementar Mudanças**.
6. Atualize seu navegador da web.

Incluindo novamente o IBM Security QRadar Risk Manager como um host gerenciado

Você pode incluir novamente o IBM Security QRadar Risk Manager como um host gerenciado depois dele ser removido.

Procedimento

1. Na guia **Admin**, clique em **Gerenciamento de Sistema e Licença** > **Ações de Implementação** > **Incluir Host**.
2. Insira o endereço IP e a senha do Host.
3. Clique em **Incluir**.

   Você deve aguardar vários minutos enquanto o host gerenciado é incluído.
4. Feche a janela Gerenciamento de Sistema e Licença.
5. Na barra de ferramentas da guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.
6. Clique em **OK**.

Capítulo 3. Reinstalar o IBM Security QRadar Risk Manager a partir da partição de recuperação

Ao reinstalar o IBM Security QRadar Risk Manager a partir do IBM Security QRadar SIEMIBM Security QRadar SIEM Console ISO na partição de recuperação, seu sistema será restaurado 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 a partir do novo QRadar Risk Manager nos dispositivos QRadar Risk Manager. Ao instalar o QRadar Risk Manager, o instalador (QRadar Console ISO) é copiado para a 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 QRadar Console e o QRadar Risk Manager usam o mesmo arquivo de instalação ISO, o nome QRadar Console ISO 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 escolher reinstalar o QRadar Console ISO, 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 IBM Security QRadar Risk Manager usando a reinstalação do Factory

Você pode reiniciar e reinstalar seu dispositivo IBM Security QRadar Risk Manager usando o opção de instalação do 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. Você pode localizar a chave nesses locais:

- 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 dispositivo QRadar Risk Manager, entre em contato com o Suporte ao Cliente (www.ibm.com/support/).

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

Procedimento

1. Reinicialize seu dispositivo QRadar Risk Manager.
2. Selecione **reinstalação de factory**.
3. Digite `comprimir` para continuar. O disco rígido é particionado e reformatado, o S.O. 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 o 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. Siga as instruções no assistente.

   Esse processo geralmente leva vários minutos.
9. Pressione `Enter` para selecionar `OK`.
10. Pressione `Enter` para selecionar `OK`.

Capítulo 4. 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 IBM Security QRadar SIEM Console.

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 IBM Security QRadar Risk Manager do IBM Security QRadar SIEM Console para alterar as configurações de rede ou se houver um problema com a guia **Riscos**.

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 do usuário raiz que foi inserida durante a instalação.
2. Clique na guia **Admin**.
3. Na área de janela **Configuração do Sistema**, clique em **Gerenciamento de Sistema e Licença**.
4. Na tabela de host, clique no host QRadar Risk Manager que deseja remover e clique em **Ações de Implementação** > **Remover Host**.
5. Na barra de menus da guia **Administrador**, clique em **Implementar Mudanças**.
6. Atualize seu navegador da web.

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 IBM Security QRadar SIEM Console.

Antes de Iniciar

Você deve remover o host gerenciado pelo QRadar Risk Manager a partir do QRadar Console antes de mudar as configurações de rede.

Procedimento

1. Utilizando o SSH, efetue login no QRadar Risk Manager como o 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 (+).
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 sua 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.

Incluindo novamente o IBM Security QRadar Risk Manager como um host gerenciado

Você pode incluir novamente o IBM Security QRadar Risk Manager como um host gerenciado depois dele ser removido.

Procedimento

1. Na guia **Admin**, clique em **Gerenciamento de Sistema e Licença** > **Ações de Implementação** > **Incluir Host**.
2. Insira o endereço IP e a senha do Host.
3. Clique em **Incluir**.

   Você deve aguardar vários minutos enquanto o host gerenciado é incluído.
4. Feche a janela Gerenciamento de Sistema e Licença.
5. Na barra de ferramentas da guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.
6. Clique em **OK**.

Capítulo 5. Backup e restauração de dados

É possível usar um script da interface com a linha de comandos (CLI) para fazer backup de dados armazenados nos hosts gerenciados pelo IBM Security QRadar SIEM Console.

É possível usar o script CLI 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 planejado usando crontab. O script cria automaticamente um archive diário dos dados do QRadar Risk Manager às 3h00. 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 do QRadar Risk Manager para um local de armazenamento de rede.

O archive de backup inclui os seguintes dados:

- Configurações do dispositivo 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 do QRadar Risk Manager Maintenance Liberação 5 para esta liberação atual, consulte o *IBM Security QRadar Risk Manager Migration Guide*.

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 pode ser restaurado em um dispositivo IBM Security 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 é criado se houver espaço livre suficiente no QRadar Risk Manager.

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. Utilizando o SSH, efetue login no IBM Security QRadar SIEM Console como o usuário raiz.
2. Usando SSH a partir do QRadar Console, efetue login no QRadar Risk Manager como o 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. Os 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 no 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. Utilizando o SSH, efetue login no IBM Security QRadar SIEM Console como o usuário raiz.
2. Usando SSH a partir do QRadar SIEM Console, efetue login no QRadar Risk Manager como o usuário raiz.
3. Pare o contexto do host digitando `service hostcontext stop`.
4. Digite o comando a seguir 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.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur 138-146
Botafogo
Rio de Janeiro, RJ
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual
Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local:

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

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão

incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

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

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

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

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

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

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

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

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

Os preços da IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso prévio. Os preços do revendedor podem variar.

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

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

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca comercial da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca comercial (® ou ™), estes símbolos indicarão marcas comerciais dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atual de marcas comerciais da IBM está disponível na web em Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

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

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

Linux é uma marca comercial 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