IBM Security QRadar SIEM
Versão 7.2.5

Guia de Administração

Nota

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 341.

Informações do produto

Este documento aplica-se ao IBM QRadar Security Intelligence Platform V7.2.5 e às liberações subsequentes, a não ser que seja substituído por uma versão atualizada.

Índice

Introdução à administração do produto QRadar

Administradores usam IBM® Security QRadar SIEM para gerenciar paineis, ofensas, atividade de log, atividade de rede, ativos e relatórios.

Público-Alvo

Este guia destina-se a todos os usuários do QRadar SIEM responsáveis pela investigação e pelo gerenciamento da segurança de rede. Este guia assume que você tenha acesso ao QRadar SIEM e conhecimento de sua rede corporativa e tecnologias de rede.

Documentação técnica

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

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

Entrando em contato com o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte a Nota Técnica de Suporte e Download (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Declaração de boas práticas de segurança

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

Observe que:

O uso deste Programa pode envolver diversas leis ou regulamentos, incluindo aqueles relacionados à privacidade, proteção de dados, empregabilidade, e comunicações e armazenamento eletrônicos. O IBM Security QRadar pode ser usado apenas para propósitos legais e de maneira legal. O cliente concorda em usar este Programa de acordo com leis, regulamentos e políticas e assume toda a

responsabilidade pelo seu cumprimento. O licenciado declara que obterá ou obteve quaisquer consentimentos, permissões ou licenças necessárias para permitir o uso legal do IBM Security QRadar.

Capítulo 1. O que há de novo para administradores em QRadar V7.2.5

O IBM Security QRadar V7.2.5 apresenta segmentação de domínios, melhor autenticação e autorização LDAP, coleta centralizada de arquivos de log, melhor gerenciamento de chaves SSH e mais recursos.

Segmentação de domínio

Agora o QRadar suporta a segmentação de domínios, com base nas seguintes origens de entrada: coletores de eventos e de fluxo, origens de log, grupos de origens de log, origens de fluxo e propriedades customizadas. É possível usar perfis de segurança para conceder privilégios de domínio e assegurar que as restrições de domínio sejam completamente respeitadas em todo o sistema IBM Security QRadar.

 Saiba mais...

Autorização LDAP

É possível usar provedores LDAP (Lightweight Directory Access Protocol) para autenticação. O QRadar lê as informações do usuário e da função a partir do servidor LDAP, com base nos critérios de autorização definidos.

 Saiba mais...

Vários repositórios LDAP

É possível configurar o QRadar para mapear entradas de vários repositórios LDAP em um único repositório virtual.

 Saiba mais...

Coleta centralizada de arquivos de log

Os arquivos de log do QRadar contêm informações detalhadas sobre a implementação, como nomes de host, endereços IP e endereços de email. É possível coletar simultaneamente os arquivos de log de um ou mais sistemas host diretamente a partir do QRadar.

 Saiba mais...

Melhoria no gerenciamento de chaves SSH

Agora as chaves SSH são distribuídas durante a implementação do QRadar. Ao fazer upgrade para o QRadar V7.2.5, as chaves SSH existentes nos hosts gerenciados são substituídas. A remoção ou alteração das chaves pode interromper a comunicação entre o QRadar Console e os hosts gerenciados, o que pode resultar em perda de dados.

Funcionamento do sistema

Agora é possível visualizar todas as notificações do sistema e outras informações sobre o funcionamento do host do QRadar em um só lugar.

 Saiba mais...

Gerenciamento de implementação

É possível incluir hosts gerenciados na implementação do QRadar ao usar as telas de gerenciamento do QRadar no QRadar.

O novo menu de **Ações de implementação** oferece as mesmas opções que o **Editor de implementação**, exceto para instalações de software. **Ações de implementação** é baseada na web e não depende de um cliente Java™.

 Saiba mais...

Capítulo 2. Visão geral da administração do QRadar

Os administradores usam a guia **Admin** no IBM Security QRadar SIEM para gerenciar paineis, ofensas, atividades de log, atividades de rede, ativos e relatórios.

Esta visão geral inclui informações gerais sobre como acessar e usar a interface com o usuário e a guia **Admin**.

Navegadores da web suportdos

Para os recursos nos produtos IBM Security QRadar funcionarem de forma adequada, você deve usar um navegador da web suportado.

Quando 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 para Produtos QRadar

Navegador da Web	Versões suportadas
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer de 32 bits e 64 bits, com o modo de documento e o modo de navegador ativados	9.0 10.0
Google Chrome	A versão atual a partir da data de liberação da versão do IBM Security QRadar que você instalou.

Visão geral da guia Administração

A guia **Admin** fornece várias opções de menu e guia que permitem configurar o QRadar.

Deve-se ter privilégios administrativos para acessar as funções administrativas. Para acessar as funções administrativas, clique na guia **Admin** na interface com o usuário.

A guia **Admin** também inclui as seguintes opções de menu:

Tabela 2. Opções de menu da guia Administração

Opção do menu	Descrição
Editor de Implementação	Abre a janela Editor de Implementação. Para obter informações adicionais, consulte Capítulo 11, “Editor de implementação”, na página 139.

Tabela 2. Opções de menu da guia Administração (continuação)

Opção do menu	Descrição
Implementar Mudanças	Implementa qualquer mudança na configuração da sessão atual para sua implementação. Para obter informações adicionais, consulte "Implementando mudanças".
Avançado	O menu **Avançado** fornece as seguintes opções: **Limpar Modelo de SIM** – Reconfigura o módulo SIM. Consulte "Reconfigurando o SIM" na página 6. **Implementar Configuração Integral** – Implementa todas as mudanças na configuração. Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.Para obter informações adicionais, consulte "Implementando mudanças".

Implementando mudanças

É possível atualizar suas definições de configuração a partir da guia **Admin**. Suas mudanças são salvas em uma área temporária onde são armazenadas até serem implementadas manualmente.

Sobre Esta Tarefa

Cada vez que você acessa a guia **Admin** e cada vez que fecha uma janela na guia **Admin**, um banner na parte superior da guia **Admin** exibe a seguinte mensagem: `Verificando mudanças implementadas`. Se mudanças implementadas forem localizadas, o banner será atualizado para fornecer informações sobre as mudanças implementadas.

Se a lista de mudanças implementadas for longa, uma barra de rolagem será fornecida. Role pela lista.

A mensagem do banner também sugere qual tipo de mudança de implementação fazer. Escolha uma das duas opções:

- **Implementar Mudanças** - Clique no ícone **Implementar Mudanças** na barra de ferramentas da guia **Admin** para implementar quaisquer mudanças na configuração da sessão atual para sua implementação.
- **Implementar Configuração Integral** - Selecione **Avançado** > **Implementar Configuração Integral** no menu da guia **Admin** para implementar todas as definições de configuração para sua implementação. Todas as mudanças implementadas são então aplicadas em toda a sua implementação.

  Importante: Quando você clicar em **Implementar Configuração Integral**, o QRadar SIEM reiniciará todos os serviços, o que resulta em uma diferença na coleta de dados até a conclusão da implementação.

Depois de implementar as mudanças, o banner limpa a lista de mudanças não implementadas e verifica a área de preparação novamente para ver se há alguma nova mudança não implementada. Se não houver nenhuma presente, a seguinte mensagem será exibida: `Não há mudanças para implementar.`

Procedimento

1. Clique em **Visualizar Detalhes**
2. Escolha uma das seguintes opções:
   a. Para expandir um grupo para exibir todos os itens, clique no sinal de mais (+) ao lado do texto. Quando terminar, é possível clicar no sinal de menos (-).
   b. Para expandir todos os grupos, clique em **Expandir Todos**. Quando terminar, é possível clicar em **Reduzir Todos**.
   c. Clique em **Ocultar Detalhes** para ocultar os detalhes da visualização novamente.
3. Execute a tarefa sugerida:
   a. A partir do menu da guia **Admin**, clique em **Implementar Mudanças**.
   b. No menu da guia **Admin**, clique em **Avançado** > **Implementar Configuração Integral**.

      Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Atualizando detalhes do usuário

É possível acessar detalhes do usuário administrativo por meio da interface com o usuário principal.

Procedimento

1. Clique em **Preferências**
2. Opcional: Atualize os detalhes configuráveis do usuário.

Opção	Descrição
Parâmetro	Descrição
Email	Digite um endereço de email novo
Senha	Digite uma nova senha
Password (Confirm)	Digite a nova senha novamente
Enable Popup Notifications	Mensagens de notificação pop-up do sistema são exibidas no canto inferior direito da interface com o usuário. Para desativar as notificações pop-up, desmarque esta caixa de seleção. Para obter informações adicionais sobre notificações pop-up, consulte o *Guia do Usuário* para seu produto.

3. Clique em **Salvar**.

Reconfigurando o SIM

Use o **Admin** para reconfigurar o módulo SIM. Agora, é possível remover todas as ofensas, endereços IP de origem e informações de endereço IP de destino do banco de dados e do disco.

Sobre Esta Tarefa

Esta opção é útil depois de você ajustar sua implementação para evitar o recebimento de quaisquer informações adicionais positivo falso.

O processo de reconfiguração do SIM pode levar vários minutos, dependendo da quantidade de dados em seu sistema. Se você tentar mover para outras áreas da interface com o usuário do IBM Security QRadar SIEM durante o processo de reconfiguração do SIM, uma mensagem de erro será exibida.

Procedimento

1. Clique na guia **Admin**.
2. No menu **Avançado**, selecione **Limpar Modelo de SIM**.
3. Leia as informações na janela Reconfigurar o Módulo de Dados do SIM.
4. Selecione uma das opções a seguir.

Opção	Descrição
Limpeza Suave	Encerra todas as ofensas no banco de dados. Se você selecionar a opção **Limpeza Suave**, poderá marcar também a caixa de seleção **Desativar todas as ofensas**.
Limpeza Bruta	Limpa todos os dados históricos e atuais do SIM, que incluem ofensas, endereços IP de origem e endereços IP de destino.

5. Se você desejar continuar, marque a caixa de seleção **Tem certeza de que deseja reconfigurar o modelo de dados?**.
6. Clique em **Continuar**.
7. Quando o processo de reconfiguração do SIM for concluído, clique em **Encerrar**.
8. Quando o processo de reconfiguração do SIM for concluído, reconfigure seu navegador.

Monitorando sistemas com SNMP

Monitoramento de dispositivos por meio de pesquisa SNMP.

QRadar SIEM usa o agente Net-SNMP, que suporta vários MIBs de monitoramento de recursos do sistema. Eles podem ser pesquisados pelas soluções Network Management para monitoramento e alerta de recursos do sistema. Para obter mais informações sobre o Net-SNMP, consulte a documentação do Net-SNMP.

Gerenciando Visualizações de Dados Agregados

Um grande volume de agregação de dados pode diminuir o desempenho do sistema. Para melhorar o desempenho do sistema, é possível desativar, ativar ou excluir visualizações de dados agregados. Os gráficos de série temporal, gráficos de relatórios e regras de anomalias usam visualizações de dados agregados.

Sobre Esta Tarefa

Os itens na lista **Exibir** drop-down classificar os dados exibidos.

A Visualização de Dados Agregados é necessária para gerar dados para regras de ADE, os gráficos de série temporal, e relatórios.

Desative ou exclua visualizações se o número máximo de pontos é atingido.

As visualizações duplicadas podem aparecer na coluna **ID de Dados Agregados** porque uma visualização de dados agregados podem incluir várias pesquisas.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Dados Agregados** .
4. Para filtrar a lista de visualizações de dados agregados, escolha uma opção a partir de uma das seguintes opções:
   - Selecione uma opção a partir de uma das seguintes listas: **Visualização**, **Banco de Dados**, **Mostrar** ou **Exibir**.
   - Digite um ID de dados agregados, nome do relatório, nome do gráfico ou nome da procura salva no campo de procura.
5. Para gerenciar uma visualização de dados agregados, selecione a visualização e, em seguida, a ação apropriada a partir da barra de ferramentas:
   - Se você selecionar **Desativar Visualização** ou **Excluir Visualização**, uma janela exibirá as dependências de conteúdo para a visualização de dados agregados. Após desativar ou excluir a visualização de dados agregados, os componentes dependentes não usarão mais os dados agregados.
   - Se você ativar uma visualização de dados agregados desativada, os dados agregados a partir da visualização excluída serão restaurados.

Tabela 3. Visualização Gerenciamento de Dados Agregados descrições de colunas

Coluna	Descrição
ID de dados agregados	Identificador para os dados agregados
Nome da Procura Salva	o nome definido para a procura salva
Column Name	Identificador de coluna
Procuras Times	contagem de Procura
Dados Gravados	O tamanho dos dados gravados
Nome do Banco de Dados	banco de dados onde o arquivo foi gravado
Horário da Última Modificação	Time stamp da última modificação de dados
Contagem Exclusiva Ativada	resultados da procura – True ou False para exibir evento exclusivo e contagens de fluxo em vez de média de contagens ao longo do tempo.

API RESTful

Use a interface de programação de aplicativos (API) Representational State Transfer (REST) para criar consultas HTTP sobre SSL e integrar o IBM Security QRadar a outras soluções.

Permissões de acesso e de função de usuário

Você deve ter permissões de função de usuário administrativo no QRadar para acessar e usar APIs RESTful. Para obter mais informações sobre como gerenciar permissões de função de usuário, consulte o *Guia de Administração do IBM Security QRadar SIEM*.

Acessar a interface com o usuário da documentação técnica da API REST

A interface com o usuário da API fornece descrições e recursos das interfaces API REST a seguir:

Tabela 4. Interfaces da API REST

API REST	Descrição
`/api/ariel`	Consulte bancos de dados, procuras, IDs de procura e resultados da procura.
`/api/asset_model`	Retorna uma lista de todos os ativos no modelo. Também é possível listar todos os tipos de propriedades de ativo e de procuras salvas disponíveis e atualizar um ativo.
`/api/auth`	Efetue logout e invalide a sessão atual.
`/api/help`	Retorna uma lista de recursos da API.
`/api/siem`	Retorna uma lista de todas as ofensas.
`/api/qvm`	Revise e gerencie dados do QRadar Vulnerability Manager.
`/api/reference_data`	Visualiza e gerencia coleções de dados de referência.
`/api/qvm`	Recupera ativos, vulnerabilidades, redes, serviços abertos e filtros. Também é possível criar ou atualizar chamados de correção.
`/api/scanner`	Visualize, crie ou inicie uma varredura remota relacionada a um perfil de varredura.

A interface da documentação técnica da API REST fornece uma estrutura que pode ser usada para reunir o código necessário para implementar as funções do QRadar em outros produtos.

1. Insira a seguinte URL no navegador da web para acessar a interface de documentação técnica: `https://`*`ConsoleIPaddress`*`/api_doc/`.
2. Clique no cabeçalho da API que você deseja acessar, por exemplo, **/ariel**.
3. Clique no cabeçalho do terminal que você deseja acessar, por exemplo, **/databases**.
4. Clique no subcabeçalho Experimental ou Provisório.

   Nota:

   Os terminais da API são anotados como *experimental* ou *estável*.

   Experimental
   Indica que o terminal da API pode não ter sido totalmente testado e pode ser futuramente alterado ou removido sem aviso prévio.

Estável

Indica que o terminal da API foi completamente testado e suportado.

5. Clique em **Experimentar** para receber respostas HTTPS formatadas adequadamente.
6. Revise e reúna as informações necessárias para implementar em sua solução de terceiros.

Fórum e amostras de código da API do QRadar

O fórum da API fornece mais informações sobre a API REST, incluindo as respostas para perguntas mais frequentes e amostras de códigos anotados que podem ser usadas em um ambiente de teste. Para obter mais informações, veja o Fórum da API (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca).

Capítulo 3. Gerenciamento do usuário

Administradores usam o recurso **Gerenciamento de Usuário** na guia **Admin** no IBM Security QRadar para configurar e gerenciar contas de usuário.

Quando você inicialmente configura o QRadar SIEM, você deve criar contas de usuário para todos os usuários que requerem acesso a QRadar SIEM. Depois da configuração inicial, você pode editar contas do usuário para garantir que as informações do usuário é atual. Você também pode incluir e excluir contas do usuário conforme necessário.

Visão geral de gerenciamento do usuário

Uma conta do usuário define o nome do usuário, senha padrão, e o endereço de e-mail para um usuário.

Designe os seguintes itens para cada nova conta de usuário que você criar:

- **função do Usuário** – Determina os privilégios que é concedido ao usuário para acessar funções e informações em QRadar SIEM. QRadar SIEM inclui duas funções de usuário padrão : Admin e Todos. Antes de incluir contas de usuário, você deve criar mais funções de usuário para atender o requisito de permissões específico de seus usuários.
- **perfil de Segurança** – Determina a redes e as fontes de log do usuário recebe acesso. QRadar SIEM inclui um perfil de segurança padrão para usuários administrativos. O perfil de segurança do Administrador inclui acesso a todas as redes e fontes de log. Antes de incluir contas de usuário, você deve criar mais funções de usuário para atender o requisito de permissões específico de seus usuários.

Gerenciador de função

Usando a janela Funções do usuário, é possível criar e gerenciar as funções do usuário.

Criando uma Função de Usuário

Utilize esta tarefa para criar as funções de usuário que são necessárias para sua implementação.

Sobre Esta Tarefa

Por padrão, o sistema fornece uma função de usuário administrativo padrão, que fornece acesso a todas as áreas do QRadar SIEM. Usuários que são designados a uma função de usuário administrativo não podem editar sua própria conta. Esta restrição se aplica à função de usuário Administrador padrão. Outro usuário administrativo deve fazer quaisquer alterações de conta.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Funções do Usuário**.

4. Na barra de ferramentas, clique em **Novo**.
5. Configure os seguintes parâmetros:
   a. No campo **Nome da Função de Usuário**, digite um nome exclusivo para essa função de usuário.
   b. Selecione as permissões que você deseja designar a esta função de usuário. Consulte "Usuário função de acesso e permissões" na página 29.
6. No **Painéis** área, selecione os painéis que você deseja que a função de usuário para acessar o, e clique em **Incluir**.

   Nota:
   a. Um painel não exibe informações se a função do usuário não tiver permissão para visualizar dados do painel.
   b. Se um usuário modificar os painéis exibidos, os painéis definido para a função do usuário aparecer no próximo login.
7. Clique em **Salvar**.
8. Feche a janela Gerenciamento de Função de Usuário.
9. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Editando uma Função de Usuário

É possível editar uma função existente para alterar as permissões que estão designadas à função.

Sobre Esta Tarefa

Para localizar rapidamente a função de usuário que você deseja editar na janela Gerenciamento de Função de Usuário, você pode digitar um nome de função na caixa de texto **Tipo para filtrar**. Esta caixa está localizada acima da área de janela à esquerda.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Funções do Usuário**.
4. Na área de janela esquerda da janela Gerenciamento de Função de Usuário, selecione a função do usuário que você deseja editar.
5. Na área de janela direita, atualize as permissões, conforme necessário. Consulte "Usuário função de acesso e permissões" na página 29.
6. Modifique as opções de **Painéis** para a função do usuário conforme necessário.
7. Clique em **Salvar**.
8. Feche a janela Gerenciamento de Função de Usuário.
9. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Excluindo uma Função de Usuário

Se uma função de usuário não for mais necessária, será possível excluí-la.

Sobre Esta Tarefa

Se as contas do usuário forem designados à função de usuário que você deseja excluir, você deverá redesignar as contas do usuário para uma outra função de usuário. O sistema detecta automaticamente essa condição e solicita que você atualize as contas do usuário.

É possível localizar rapidamente a função de usuário que você deseja excluir na janela Gerenciamento de Função de Usuário. Digite um nome de função na caixa de texto **Tipo para filtrar**, que está localizada acima da área de janela esquerda.

Procedimento

1. Clique na guia **Admin**.
2. No menu **Navegação**, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Funções do Usuário**.
4. Na área de janela esquerda da janela de Gerenciamento de Função de Usuário, selecione a função que você deseja excluir.
5. Na barra de ferramentas, clique em **Excluir**.
6. Clique em **OK**.
   - Se as contas de usuário forem designadas para essa função de usuário, a janela Usuários Estão Designados para Esta Função de Usuário será aberta. Vá para a Etapa 7.
   - Se não houver contas do usuário designadas para esta função, a função de usuário será excluída com êxito. Vá para a Etapa 8.
7. Redesigne as contas do usuário listadas para uma outra função de usuário:
   a. Na caixa de listagem **Função de Usuário para Designar**, selecione uma função de usuário.
   b. Clique em **Confirmar**.
8. Feche a janela Gerenciamento de Função de Usuário.
9. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Gerenciando perfis de segurança

Os perfis de segurança definem quais redes e fontes de log um usuário pode acessar e a precedência de permissão.

Usando a janela Gerenciador de perfis de segurança, é possível visualizar, criar, atualizar e excluir perfis de segurança.

Permissão de precedentes

Este tópico define cada uma das opções de precedência de permissão.

A precedência de permissão determina quais componentes do Perfil de Segurança devem ser consideradas quando o sistema exibe eventos na guia **Atividade de log** e fluxos na guia **Atividade de rede**.

Assegure-se de que você compreendeu as restrições abaixo:

- **Sem restrições** - Essa opção não coloca restrições sobre quais eventos são exibidos na guia **Atividade de log** e quais fluxos são exibidos na guia **Atividade de rede**.

- **Apenas rede** - Essa opção restringe o usuário a visualizar eventos e fluxos que são associados a redes específicas nesse perfil de segurança.
- **Apenas fontes de log** - Essa opção restringe o usuário a visualizar apenas eventos que são associados com fontes de log, especificadas nesse perfil de segurança.
- **Redes E origens do log** - Essa opção permite que o usuário visualize somente eventos e fluxo que estão associados às origens do log e redes especificadas nesse perfil de segurança.

Por exemplo, se um evento estiver associado a uma origem de log o perfil de segurança permite acesso, mas a rede de destino é restrito, o evento é exibido na guia **Atividade do Log**. O evento deve corresponder a ambos os requisitos.

- **Redes OU origens de log** - Essa opção permite que o usuário visualize somente eventos e fluxos que estão associados às origens de log e redes especificadas nesse perfil de segurança.

Por exemplo, se um evento estiver associado a uma origem de log, o perfil de segurança permite acesso, mas a rede de destino é restrita, o evento é exibido na guia **Atividade do Log**. O evento deve corresponder a um requisito.

Criando um Perfil de Segurança

Para incluir contas do usuário, você deve primeiro criar perfis de segurança para atender aos requisitos de acesso específicos de seus usuários.

Sobre Esta Tarefa

QRadar SIEM inclui um perfil de segurança padrão para usuários administrativos. O perfil de segurança do Administrador inclui acesso a todas as redes e fontes de log.

Para selecionar múltiplos itens na janela Gerenciamento de Perfil de Segurança, pressione a tecla CTRL enquanto seleciona cada rede ou cada grupo de redes que desejar incluir.

Se, após incluir fontes de log ou redes, você desejar remover uma ou mais antes de salvar a configuração, poderá selecionar o item e clicar no ícone **Remover (<)**. Para remover todos os itens, clique em **Remover Todos**.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Perfis de Segurança**.
4. Na barra de ferramentas da janela Gerenciamento de Perfil de Segurança, clique em **Novo**.
5. Configure os seguintes parâmetros:
   a. No campo **Nome do Perfil de Segurança**, digite um nome exclusivo para o perfil de segurança. O nome do perfil de segurança deve atender aos seguintes requisitos: mínimo de 3 caracteres e máximo de 30 caracteres.
   b. `Opcional` Digite uma descrição do perfil de segurança. O número máximo de caracteres é 255.
6. Clique na guia **Precedência da Permissão**.

7. Na área de janela Configuração da Precedência da Permissão, selecione uma opção de precedência da permissão. Consulte “Permissão de precedentes” na página 13.
8. Configure as redes que deseja designar ao perfil de segurança:
   a. Clique na guia **Redes**.
   b. Na árvore de navegação na área de janela à esquerda da guia **Redes**, selecione a rede à qual você deseja que esse perfil de segurança tenha acesso.
   c. Clique no ícone **Incluir (>)** para incluir a rede na área de janela Redes Designadas.
   d. Repita para cada rede que você deseja incluir.
9. Configure as fontes de log que deseja designar ao perfil de segurança:
   a. Clique na guia **Fontes de Log**.
   b. A partir da árvore de navegação na área de janela esquerda, selecione o grupo de fontes de log ou a fonte de log à qual você deseja que esse perfil de segurança tenha acesso.
   c. Clique no ícone **Incluir (>)** para incluir a fonte de log na área de janela Fontes de Log Designadas.
   d. Repita para cada fonte de log que você deseja incluir.
10. Clique em **Salvar**.
11. Feche a janela Gerenciamento de Perfil de Segurança.
12. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Editando um Perfil de Segurança

É possível editar um perfil de segurança existente para atualizar quais redes e origens de log um usuário pode acessar e a precedência de permissão.

Sobre Esta Tarefa

Para localizar rapidamente o perfil de segurança que deseja editar na janela de Gerenciamento de Perfil de Segurança, digite o nome do perfil de segurança na caixa de texto **Tipo para Filtrar**. Ele está localizado acima da área de janela esquerda.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Perfis de Segurança**.
4. Na área de janela à esquerda, selecione o perfil de segurança que deseja editar.
5. Na barra de ferramentas, clique em **Editar**.
6. Atualize os parâmetros conforme necessário.
7. Clique em **Salvar**.
8. Se a janela Perfil de Segurança Possui Dados de Séries Temporais abrir, selecione uma das seguintes opções:

Opção	Descrição
Manter Dados Antigos e Salvar	Selecione esta opção para manter os dados de série temporal acumulados anteriormente. Se você escolher essa opção, problemas poderão ocorrer quando os usuários associados a esse perfil de segurança visualizarem gráficos de série temporal.
Ocultar Dados Antigos e Salvar	Selecione esta opção para ocultar dados de série temporal. Se você escolher essa opção, a acumulação de dados série temporal será reiniciada depois que você implementar suas mudanças na configuração.

9. Feche a janela Gerenciamento de Perfil de Segurança.
10. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Duplicando um Perfil de Segurança

Se você deseja criar um novo perfil de segurança que corresponda melhor a um perfil de segurança existente, pode duplicar o perfil de segurança existente e, em seguida, modificar os parâmetros.

Sobre Esta Tarefa

Para localizar rapidamente o perfil de segurança que deseja duplicar na janela Gerenciamento de Perfil de Segurança, é possível digitar o nome do perfil de segurança na caixa de texto **Tipo para filtrar**, que está localizada acima da área de janela esquerda.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema Gerenciamento do usuário**.
3. Clique no ícone **Perfis de Segurança**.
4. Na área de janela à esquerda, selecione o perfil de segurança que deseja duplicar.
5. Na barra de ferramentas, clique em **Duplicar**.
6. Na janela Confirmação, digite um nome exclusivo para o perfil de segurança duplicado.
7. Clique em **OK**.
8. Atualize os parâmetros conforme necessário.
9. Feche a janela Gerenciamento de Perfil de Segurança.
10. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Excluindo um Perfil de Segurança

Se um perfil de segurança não for mais necessário, você poderá excluí-lo.

Sobre Esta Tarefa

Se contas do usuário forem designadas aos perfis de segurança que você deseja excluir, você deverá redesignar as contas do usuário para um outro perfil de segurança. OQRadar SIEM detecta automaticamente essa condição e solicita que você atualize as contas do usuário.

Para localizar rapidamente o perfil de segurança que você deseja excluir na janela Gerenciamento de Perfil de Segurança, você pode digitar o nome do perfil de segurança na caixa de texto **Tipo para filtrar**. Ele está localizado acima da área de janela esquerda.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Perfis de Segurança**.
4. Na área de janela à esquerda, selecione o perfil de segurança que você deseja excluir.
5. Na barra de ferramentas, clique em **Excluir**.
6. Clique em **OK**.
   - Se contas do usuário forem designadas a esse perfil de segurança, a janela Usuários estão Designados a este Perfil de Segurança será aberta. Acesse "Excluindo uma Função de Usuário" na página 12.
   - Se não houver contas do usuário designadas a esse perfil de segurança, o perfil de segurança será excluído com êxito. Acesse "Excluindo uma Função de Usuário" na página 12.
7. Redesigne as contas do usuário listadas para outro perfil de segurança:
   a. Na caixa de listagem **Perfil de Segurança do Usuário para designar**, selecione um perfil de segurança.
   b. Clique em **Confirmar**.
8. Feche a janela Gerenciamento de Perfil de Segurança.
9. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Gerenciamento de conta do usuário

Esse tópico fornece informações sobre gerenciamento de contas do ususário.

Quando inicialmente o sistema é configurado, deve-se criar contas do usuário para cada um de seus usuários. Após configuração inicial, pode ser necessário criar mais contas do usuário e gerenciar as existentes.

Criando uma Conta do Usuário

É possível criar novas contas do usuário.

Antes de Iniciar

Antes de poder criar uma conta do usuário, você deve assegurar que a função de usuário e o perfil de segurança necessários sejam criados.

Sobre Esta Tarefa

Ao criar uma nova conta de usuário, você deve designar credenciais de acesso, uma função de usuário e um perfil de segurança para o usuário. Funções do usuário definem quais ações o usuário tem permissão para executar. Perfis de Segurança definem quais dados o usuário tem permissão para acessar.

É possível criar múltiplas contas do usuário que incluem privilégios administrativos; no entanto, quaisquer contas de usuário de Gerente Administrador podem criar outras contas de usuário administrativo.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Usuários**.
4. Na barra de ferramentas **Gerenciamento do usuário**, clique em **Novo**.
5. Insira os valores para os parâmetros a seguir:
   a. No campo **Nome de Usuário**, digite um nome de usuário exclusivo para o novo usuário. O nome de usuário deve conter um máximo de 30 caracteres.
   b. No campo **Senha**, digite uma senha para o usuário para obter acesso.

      A senha deve atender aos seguintes critérios:
      - Mínimo de 5 caracteres
      - Máximo de 255 caracteres
6. Clique em **Salvar**.
7. Feche a janela Detalhes do Usuário.
8. Feche a janela Gerenciamento do Usuário.
9. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Excluindo uma Conta do Usuário

Se uma conta do usuário não é mais necessária, é possível excluí-la.

Sobre Esta Tarefa

Depois de excluir um usuário, o usuário não possui mais acesso à interface com o usuário. Se o usuário tentar efetuar login, uma mensagem será exibida para informar ao usuário de que o nome do usuário e a senha não são mais válidos. Itens que um usuário excluído criou, como procuras e relatórios salvos, permanecem associados ao usuário excluído.

Para localizar rapidamente a conta do usuário que você deseja excluir na janela Gerenciamento do Usuário, você pode digitar o nome do usuário na caixa de texto **Procurar Usuário** na barra de ferramentas.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Usuários**.
4. Selecione o usuário que você deseja excluir.
5. Na barra de ferramentas, clique em **Excluir**.

6. Clique em **OK**.
7. Feche a janela Gerenciamento do Usuário.

Desativando uma conta do usuário

É possível desativar uma conta do usuário para restringir um usuário de acessar o QRadar. A opção para desativar uma conta do usuário revoga provisoriamente o acesso de um usuário sem excluir a conta.

Sobre Esta Tarefa

Se o usuário com a conta desativada tentar efetuar login, uma mensagem será exibida para informá-lo que o nome de usuário e a senha não são mais válidos. Os itens que o usuário criou, como procuras e relatórios salvos, permanecem associados ao usuário.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Usuários**.
4. Na área de janela Gerenciar usuários, clique na conta do usuário que deseja desativar.
5. Na janela Detalhes do usuário, selecione **Desativado** na lista **Função de usuário**.
6. Clique em **Salvar**.
7. Feche a janela Detalhes do Usuário.
8. Feche a janela Gerenciamento do Usuário.
9. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Gerenciador de autenticação

Esse tópico fornece informação e instrução de como configurar a autenticação.

QRadar SIEM suporta vários tipos de autenticação. Você pode configurar a autenticação para validar usuários e senhas.

Visão Geral da Autenticação

Quando a autenticação é configurada e um usuário insere um nome de usuário inválido e senha combinação, uma mensagem será exibida para indicar que o login era inválido.

Se o usuário tenta acessar o sistema várias vezes com informações inválidas, o usuário deve aguardar o período de tempo configurado antes de uma outra tentativa de acessar o sistema novamente. Você pode configurar definições do Console para determinar o número máximo de logins com falha, e outras configurações relacionadas. Para obter informações adicionais sobre como configurar as definições do Console para autenticação, consulte Capítulo 6, “Configurar QRadar”, na página 65 “Configurando as Definições do Console” na página 100.

Um usuário administrativo pode acessar o QRadar SIEM por meio de um módulo de autenticação do fornecedor ou utilizando a senha Admin local. As funções a

senha Admin se você configurar e ativado um módulo de autenticação do fornecedor. No entanto, você não pode alterar a senha Admin enquanto o módulo de autenticação está ativo. Para alterar a senha Admin, você deve temporariamente desativar o módulo de autenticação do fornecedor, reconfigure a senha e, em seguida, reconfigure o módulo de autenticação do fornecedor.

QRadar SIEM suporta os seguintes tipos de autenticação do usuário :

- **Autenticação de sistema** - Os usuários são autenticados localmente. Este é o tipo de autenticação padrão.
- **Autenticação RADIUS** - Os usuários são autenticados por um servidor Remote Authentication Dial-in User Service (RADIUS). Quando um usuário tentar efetuar login, QRadar SIEM criptografa a senha somente, e redireciona o nome do usuário e a senha para o servidor RADIUS para autenticação.
- **Autenticação TACACS** – Os usuários são autenticados por um servidor Terminal Access Controller Access Control System (TACACS). Quando um usuário tentar efetuar login, QRadar SIEM criptografa o nome de usuário e a senha, e redireciona essas informações para o servidor TACACS para autenticação. utilizar Secure Cisco ACS Authentication TACACS Express como um servidor TACACS. QRadar SIEM suporta até Cisco Secure ACS Express 4,3.
- **Active Directory** – Os usuários são autenticados por um servidor LDAP (Lightweight Directory Access Protocol) que utiliza Kerberos.
- **LDAP** – Os usuários são autenticados por um servidor LDAP Nativo.

Lista de verificação de tarefas de pré-requisito de tipo de autenticação

Tarefas de pré-requisito são necessárias antes da configuração de RADIUS, TACACS, Active Directory ou LDAP como o tipo de autenticação.

Antes de poder configurar o RADIUS, TACACS, Active Directory, ou LDAP como o tipo de autenticação, você deve concluir as seguintes tarefas:

- Configure o servidor de autenticação antes de você configurar a autenticação em QRadar. Para obter informações adicionais, consulte a documentação do servidor
- Certifique-se de que o servidor tenha as contas de usuário apropriadas e os níveis de privilégio para se comunicar com QRadar. Para obter informações adicionais, consulte a documentação do servidor.
- Certifique-se de que a hora do servidor de autenticação está sincronizada com a hora do servidor. QRadar Para obter informações adicionais sobre tempo de configuração, consulte Capítulo 6, “Configurar QRadar”, na página 65.
- Certifique-se de que todos os usuários tenham apropriado contas do usuário e funções para permitir a autenticação com os servidores do fornecedor.

Configurando autenticação do sistema

É possível configurar a autenticação local em seu sistema. QRadar

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema** > **Gerenciamento do usuário**.
3. Clique no ícone **Autenticação**.
4. Na caixa de seleção **Módulo de Autenticação** selecione **Sistema de Autenticação**.

5. Clique em **Salvar**.

Configurando autenticação RADIUS

É possível configurar a autenticação RADIUS em seu sistema. QRadar

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema Gerenciamento do usuário**.
3. Clique no ícone **Autenticação**.
4. Na caixa de listagem **Módulo de Autenticação**, selecione **Autenticação RADIUS**.
5. Configure os parâmetros:
   a. No campo **Servidor RADIUS** , digite o nome do host ou endereço IP do servidor RADIUS.
   b. No campo **Porta do RADIUS** , digite a porta do servidor RADIUS.
   c. Na caixa de listagem **Tipo de autenticação**, selecione o tipo de autenticação que você deseja executar.

      Escolha uma das seguintes opções:

Opção	Descrição
CHAP	CHAP (Challenge Handshake Authentication Protocol) estabelece uma conexão protocolo ponto a ponto (PPP) entre o usuário e o servidor.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol (MSCHAP) autentica as estações de trabalho Windows remotas.
ARAP	Apple Remote Access Protocol (ARAP) AppleTalk estabelece a autenticação para o tráfego de rede.
PAP	o Password Authentication Protocol (PAP) envia texto limpo entre o usuário e o servidor.

   d. No campo **Segredo Compartilhado** , digite o segredo compartilhado que utiliza para criptografar senhas QRadar SIEM RADIUS para transmissão do servidor RADIUS.
6. Clique em **Salvar**.

Configurando a Autenticação do TACACS

Você pode configurar a autenticação TACACS em seu sistema. QRadar

Procedimento

1. Clique na guia **Admin**.
2. No menu **de navegação**, clique em **Configuração do sistema** > **gerenciador de usuário**.
3. Clique no ícone **Autenticação**.
4. Na caixa de listagem **Módulo de autenticação**, selecione **Autenticação do TACACS**.

5. Configure os parâmetros:
   a. No campo **Servidor TACACS**, digite o nome do host ou endereço IP do servidor TACACS.
   b. No campo **Porta do TACACS**, digite a porta do servidor TACACS.
   c. Na caixa de listagem **Tipo de autenticação**, selecione o tipo de autenticação que você deseja executar.

      Escolha uma das seguintes opções:

Opção	Descrição
ASCII	O ASCII (American Standard Code for Information Interchange) envia o nome do usuário e senha em texto limpo, não criptografado.
PAP	o Password Authentication Protocol (PAP) envia texto limpo entre o usuário e o servidor. Este é o tipo de autenticação padrão.
CHAP	CHAP (Challenge Handshake Authentication Protocol) estabelece uma conexão protocolo ponto a ponto (PPP) entre o usuário e o servidor.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol (MSCHAP) autentica as estações de trabalho Windows remotas.
MSCHAP2	Microsoft Challenge Handshake Authentication Protocol versão 2 (MSCHAP2) autentica as estações de trabalho Windows remotas usando autenticação mútua.
EAPMD5	A Autenticação de protocolo extensível do protocolo MD5 (EAPMD5), usa MD5 para estabilizar uma conexão PPP.

   d. No campo **Segredo Compartilhado**, digite o segredo compartilhado que o QRadar SIEM usa para criptografar senhas de TACACS para transmissão para o servidor TACACS.
6. Clique em **Salvar**.

Configurando a autenticação do Active Directory

É possível configurar a autenticação Active Directory em seu IBM Security QRadar sistema.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do Sistema** e, em seguida, clique no ícone **Autenticação**.
3. caixa de listagem **Módulo de autenticação** selecione o **Diretório ativo**.

   Configure os seguintes parâmetros:

Parâmetro	Descrição
URL do Servidor	Digite a URL utilizada para conectar-se ao servidor LDAP, por exemplo, ldaps://*host*:*port*.
Contexto do LDAP	Digite o contexto LDAP que você deseja utilizar, por exemplo, DC=QRADAR,DC=INC.
Domínio LDAP	Redigite a chave que deseja utilizar para criptografia, por exemplo.

4. Clique em **Salvar**.

Autenticação LDAP

É possível configurar o QRadar para usar provedores Lightweight Directory Access Protocol (LDAP) suportados para autenticação e autorização do usuário.

O QRadar lê as informações do usuário e da função a partir do servidor LDAP, com base nos critérios de autorização definidos.

Autenticação

A autenticação estabelece a prova de identidade para qualquer usuário que tentar efetuar login no servidor QRadar. Quando um usuário efetua login, o nome e a senha do usuário são enviados para o diretório LDAP, para verificar se as credenciais estão corretas. Para enviar estas informações com segurança, configure a conexão do servidor LDAP para usar a criptografia Secure Socket Layer (SSL) ou Segurança da Camada de Transporte (TLS).

Use a conexão anônima para criar uma sessão com o servidor de diretório LDAP que não requer o fornecimento de informações de autenticação.

A conexão autenticada requer que a sessão tenha uma combinação válida de nome de usuário e senha. Uma conexão autenticada bem-sucedida autoriza o usuário autenticado a ler a lista de usuários e funções do diretório LDAP durante a sessão.

Para maior segurança, certifique-se de que o ID de usuário usado para a conexão de ligação não tenha permissões para fazer mais nada além de ler o diretório LDAP.

Autorização

Autorização é o processo de determinar quais permissões de acesso um usuário possui. Os usuários estão autorizados a executar tarefas com base em suas designações de funções.

Você deve ter uma conexão de ligação válida com o servidor LDAP antes de poder selecionar configurações de autorização.

Local Os servidores LDAP são usados apenas para a autenticação de usuários. A combinação de nome de usuário e senha é verificada para cada usuário que efetua login, mas nenhuma informação de autorização é trocada entre o servidor LDAP e o servidor QRadar. Caso tenha escolhido a autorização **Local**, crie cada usuário no console do QRadar.

Atributos do usuário
Forma um filtro de procura usado quando os usuários são autenticados.

Você deve especificar um atributo de função do usuário e um atributo de perfil de segurança. Os atributos que podem ser usados são recuperados do servidor LDAP, com base nas configurações de conexão.

Grupo Os usuários herdam as permissões de acesso baseadas em função depois de fazerem a autenticação com o servidor LDAP.

As listas de membros do grupo LDAP são recuperadas com base nos atributos configurados no **Campo de Membro de Grupo**. Todos os usuários nesses grupos herdam permissões com base no que é permitido pela função do QRadar. É possível configurar grupos separados para autorizar ou negar permissões para perfis de segurança e funções de usuário.

Os valores do atributo do usuário fazem distinção entre maiúsculas e minúsculas. O mapeamento de nomes de grupos para funções de usuário e perfis de segurança também faz distinção entre maiúsculas e minúsculas.

Sincronização de dados

Caso tenha optado por usar a autenticação que é baseada em grupos ou atributos do usuário, as informações do usuário serão automaticamente importadas do servidor LDAP para o console do QRadar. Cada grupo que é configurado no servidor LDAP deve ter uma função do usuário ou um perfil de segurança correspondente configurado no console do QRadar. Para cada grupo correspondente, os usuários serão importados e receberão permissões baseadas nessa função de usuário ou nesse perfil de segurança.

Por padrão, a sincronização ocorre a cada 24 horas. O tempo para a sincronização é baseado na última execução. Por exemplo, caso a sincronização seja executada manualmente às 23h45 e o intervalo de sincronização seja definido como 8 horas, a próxima sincronização ocorrerá às 7h45. Caso haja uma mudança nas permissões de acesso de um usuário que está conectado durante a execução da sincronização, a sessão se tornará inválida. O usuário é redirecionado à tela de login com a próxima solicitação.

Para sincronizar dados manualmente, siga estas etapas:

1. Na guia **Administrador**, clique em **Configuração do Sistema** e, em seguida, clique em **Autenticação**.
2. Na lista **Módulo de Autenticação**, selecione **LDAP**.
3. Clique em **Gerenciar Sincronização** e, em seguida, clique em **Executar Sincronização Agora**.

Configurando a Autenticação LDAP

É possível configurar o sistema IBM Security QRadar para usar a criptografia SSL ou a autenticação TLS ao se conectar ao servidor LDAP.

Antes de Iniciar

Se você planeja usar a criptografia SSL ou a autenticação TLS com o servidor LDAP, deverá importar o certificado SSL ou TLS do servidor LDAP para o diretório `/opt/qradar/conf/trusted_certificates` no console do QRadar. Para obter mais informações sobre como configurar os certificados, consulte "Configurando certificados SSL ou TLS" na página 29.

Caso esteja usando a autorização de grupo, configure uma função de usuário ou um perfil de segurança do QRadar no console do QRadar para cada grupo LDAP usado pelo QRadar. Cada função de usuário do QRadar ou perfil de segurança deve ter pelo menos um grupo de aceitação. O mapeamento de nomes de grupos para funções de usuários e perfis de segurança faz distinção entre maiúsculas e minúsculas.

Sobre Esta Tarefa

A tabela a seguir mostra os parâmetros que são necessários para configurar um provedor de autenticação LDAP.

Tabela 5. Parâmetros do provedor de autenticação LDAP

Parâmetro	Descrição
URL do Servidor	O nome DNS ou endereço IP do servidor LDAP. A URL deve incluir um valor de porta. Por exemplo, `ldap://<host_name>:<port>` ou `ldap://<ip_address>:<port>`.
Conexão SSL	Caso a criptografia SSL esteja ativada, o valor no campo **URL do Servidor** deve especificar uma conexão segura, por exemplo, `ldaps://secureldap.mydomain.com:636`.
Autenticação TLS	A criptografia TLS (Segurança da Camada de Transporte) para conexão com o servidor LDAP é negociada como parte do protocolo LDAP normal e não requer uma designação de protocolo ou porta especial no campo **URL do Servidor**.
Procurar base inteira	Selecione **True** para procurar todos os subdiretórios do Nome de Diretório (DN) especificado. Selecione **False** para procurar apenas o conteúdo imediato do DN Base. Os subdiretórios não serão pesquisados.
Campo do usuário LDAP	O identificador de campo do usuário no qual você deseja procurar. Você pode especificar vários campos do usuário em uma lista separada por vírgula para permitir que os usuários autentiquem em relação a vários campos. Por exemplo, ao especificar **uid,mailid**, um usuário poderá ser autenticado fornecendo seu ID de usuário ou seu ID de correio.
DN base	O DN do nó no qual a procura por um usuário deve começar. O DN base se torna o local de início para o carregamento de usuários e grupos. Por motivos de desempenho, o DN base deve ser o mais específico possível. Por exemplo, se todas as suas contas e grupos de usuários estiverem no servidor de diretórios na pasta `Usuários` e seu nome de domínio for `ibm.com`, o valor do DN base será `cn=Users,dc=ibm,dc=com`.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do Sistema** > **Gerenciamento do Usuário** e clique no ícone **Autenticação**.
3. Na caixa de listagem **Módulo de Autenticação**, selecione **LDAP**.
4. Clique em **Incluir** e preencha os parâmetros básicos de configuração.
5. Em **Configurações de Conexão**, selecione o tipo de conexão de ligação.

6. Se você estiver usando uma ligação autenticada, forneça as informações de autenticação. Por exemplo, se o nome de login for admin e o domínio for ibm.com, o **DN de Login** será `cn=admin,dc=ibm,dc=com`.
7. Clique em **Testar conexão** para testar as informações de conexão. Você deve ter uma conexão bem-sucedida com o servidor LDAP antes de poder continuar com as etapas restantes.
8. Selecione o método de autorização a ser usado.
   - Caso deseje que o servidor LDAP verifique apenas as informações de nome de usuário e senha, escolha **Local**. Nenhuma informação de autorização é trocada entre o servidor LDAP e o console do QRadar.
   - Caso deseje especificar quais atributos podem ser usados para determinar os níveis de autorização, escolha **Atributos do usuário**.
   - Caso deseje que os usuários herdem permissões de acesso baseadas em função após a autenticação com o servidor LDAP, escolha **Grupo**.
9. Se você estiver usando a autorização **Grupo**, especifique a aceitação e a negação dos grupos de privilégios.
   a. No **Campo de Membro do Grupo**, forneça o atributo LDAP que é usado para definir a associação do grupo de usuários.
   b. Clique no ícone de mais (+) ou menos (-) para incluir ou remover grupos de privilégios. As opções de privilégios de função do usuário controlam a quais componentes do QRadar o usuário tem acesso. As opções de privilégios do perfil de segurança controlam os dados do QRadar aos quais cada usuário tem acesso.
10. Clique em **Salvar**.
11. Clique em **Gerenciar sincronização** para trocar informações sobre autenticação e autorização entre o servidor LDAP e o console do QRadar.
    a. Se você estiver configurando a conexão LDAP pela primeira vez, clique em **Executar Sincronização Agora** para sincronizar os dados.
    b. Especifique a frequência para sincronização automática.
    c. Clique em **Fechar**.
12. Repita as etapas para incluir mais servidores LDAP e clique em **Salvar** quando concluir.

Vários repositórios LDAP

É possível configurar o IBM Security QRadar para mapear entradas de vários repositórios LDAP em um único repositório virtual.

Caso haja vários repositórios configurados, os usuários devem especificar o nome de domínio ao efetuarem login, para indicar qual repositório deve ser usado para autenticação.

Por exemplo, um sistema QRadar possui dois repositórios LDAP configurados. Repository_1 está configurado para usar o domínio `ibm.com` e Repository_2 está configurado para usar o domínio `ibm.ca.com`. Quando um usuário tenta efetuar login, ele deve especificar o nome de domínio no campo de nome de usuário, como `ibm.ca.com\username`.

As informações sobre o usuário são automaticamente importadas do servidor LDAP para repositórios que usam atributos do usuário ou autorização de grupo. Para repositórios que usam autorização local, você deve criar usuários diretamente no sistema QRadar.

Exemplo: configuração de acesso menos privilegiado

Conceda aos usuários apenas o acesso mínimo necessário para execução de suas tarefas diárias.

Você pode designar privilégios diferentes para dados do QRadar e recursos do QRadar. É possível fazer isso especificando diferentes grupos de aceitação e negação para perfis de segurança e funções do usuário. Aceite privilégios de designação de grupo e negue privilégios de restrição de grupos.

Vamos ver um exemplo. Sua empresa contratou um grupo de estudantes estagiários. John está em seu último ano de um programa especializado de cyber segurança na universidade local. Foi solicitado que ele monitorasse e revisasse as vulnerabilidades de rede conhecidas e preparasse um plano de correção, com base nas descobertas. As informações sobre as vulnerabilidades de rede da empresa são confidenciais.

Como administrador do QRadar, você deve garantir que os estagiários estudantes tenham acesso limitado aos dados e sistemas. A maioria dos estagiários deve ter o acesso negado ao QRadar Vulnerability Manager, mas a designação especial de John requer que ele tenha esse acesso. A política de sua organização é que os estagiários nunca tenham acesso à API do QRadar.

A tabela a seguir mostra que John deve ser membro dos grupos **company.interns** e **qvm.interns** para ter acesso ao QRadar Risk Manager e ao QRadar Vulnerability Manager.

Tabela 6. Grupos de privilégios de funções de usuários

Função de usuário	Aceitar	Negar
Admin	qradar.admin	company.firedemployees
QVM	qradar.qvm qvm.interns	company.firedemployees qradar.qrm company.interns
QRM	qradar.qrm company.interns	company.firedemployees

A tabela a seguir mostra que o perfil de segurança de **qvm.interns** impede que John acesse a API do QRadar.

Tabela 7. Grupos de privilégios de perfis de segurança

Perfil de segurança	Aceitar	Negar
QVM	qradar.secprofile.qvm	company.firedemployees
API	qradar.secprofile.qvm.api	company.firedemployees qradar.secprofile.qvm.interns

Exibindo texto de ajuda instantânea para informações de LDAP

Você cria um arquivo de configuração de propriedades do LDAP para exibir informações do usuário LDAP como texto de ajuda instantânea. Esse arquivo de configuração consulta o banco de dados LDAP para obter informações sobre o usuário LDAP que está associado aos eventos, ofensas ou ativos.

Antes de Iniciar

O servidor da web deve ser reiniciado após a criação das propriedades do LDAP. Considere planejar esta tarefa durante uma janela de manutenção quando nenhum usuário ativo estiver com login efetuado no sistema.

Sobre Esta Tarefa

O exemplo a seguir lista as propriedades que você pode incluir em um arquivo de configuração `ldap.properties`.

```
ldap.url=ldap://LDAPserver.example.com:389
ldap.authentication=simple
ldap.userName=user.name
ldap.password=your.encrypted.password
ldap.basedn=O=IBM,C=US ldap.filterString=(&(objectclass=user)(samaccountname=%USER%))
ldap.attributes.displayName=Name
ldap.attributes.email=Email
ldap.attributes.employeeID=EmployeeID
ldap.attributes.department=Department
```

Procedimento

1. Use SSH para efetuar login no IBM Security QRadar como um usuário raiz.
2. Para criptografar a senha do usuário LDAP, execute o script `/opt/qradar/bin/runjava.sh com.q1labs.core.util.PasswordEncrypt [password]`.
3. Use um editor de texto para criar o arquivo de configuração `/opt/qradar/conf/ldap.properties`.
4. Especifique as informações de local e autenticação para acessar o servidor LDAP remoto.
   a. Especifique a URL do servidor LDAP e o número da porta.

      Use `ldaps://` ou `ldap://` para conectar ao servidor remoto, por exemplo, `ldap.url=ldaps://LDAPserver.example.com:389`.
   b. Digite o método de autenticação que é usado para acessar o servidor LDAP.

      Os administradores podem usar o método de autenticação simples, por exemplo, `ldap.authentication=simple`.
   c. Digite o nome do usuário que tem permissões para acessar o servidor LDAP, por exemplo, `ldap.userName=user.name`.
   d. Para autenticar no servidor LDAP remoto, digite a senha de usuário LDAP criptografada do usuário, por exemplo, `ldap.password=password`.
   e. Digite o DN base usado para procurar o servidor LDAP dos usuários, por exemplo, `ldap.basedn=BaseDN`.
   f. Digite um valor para ser usado pelo filtro de parâmetro de procura no LDAP.

      Por exemplo, no IBM Security QRadar, ao passar o mouse sobre `ldap.filterString=(&(objectclass=user)(samaccountname=%USER%))`, o valor `%USER%` é substituído pelo nome do usuário.
5. Digite um ou mais atributos a serem exibidos no texto de ajuda instantânea.

   Você deve incluir pelo menos um atributo LDAP. Cada valor deve usar este formato: `ldap.attributes.AttributeName=Descriptive text to show in UI.`
6. Verifique se há permissão no nível de leitura para o arquivo de configuração `ldap.properties`.
7. Efetue login no QRadar como administrador.
8. Na guia **Administrador**, selecione **Avançado** > **Reiniciar servidor da web**.

Resultados

Os administradores podem passar o mouse sobre o campo **Nome do Usuário** nas guias **Atividade de Log** e **Infrações** ou passar o mouse sobre o campo **Último Usuário** na guia **Ativos** para exibir mais informações sobre o usuário LDAP.

Configurando certificados SSL ou TLS

Se usar um servidor de diretório LDAP para autenticação do usuário e desejar ativar a criptografia SSL ou a autenticação TLS, você deverá configurar seu certificado SSL ou TLS.

Procedimento

1. Utilizando o SSH, efetue login no para o system como o usuário root.
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`
2. Digite o seguinte comando para criar o diretório `/opt/qradar/conf/trusted_certificates/` :

   ```
   mkdir -p /opt/qradar/conf/trusted_certificates
   ```
3. Copie o certificado SSL ou TLS do servidor LDAP para o `/opt/qradar/conf/trusted_certificates` diretório em seu sistema.
4. Verifique se a extensão do nome do arquivo de certificado é `.cert`, o que indica que o certificado é confiável. O sistema QRadar carrega apenas arquivos `.cert`.

Usuário função de acesso e permissões

Utilize a janela Gerenciamento de Função de Usuário parâmetros para restringir o acesso a recursos do IBM Security QRadar .

A tabela a seguir descreve os parâmetros da janela Gerenciamento de Função de Usuário .

Tabela 8. Descrição da janela Gerenciamento de Função de Usuário parâmetros

Parâmetro	Descrição
Nome da função do usuário	Um nome exclusivo para a função.
Admin	Concede acesso administrativo para a interface com o usuário. Você pode conceder permissões: Admin específico **Gerenciador do Administrador** Concede acesso administrativo para a interface com o usuário. Você concede permissões específicas de Administrador. **Configuração de Redes e Serviços Remotos** Concede permissão para configurar redes remotas e serviços na guia **Admin** . **Administrador do Sistema** Concede permissão para acessar todos os domínios da interface com o usuário. Os usuários que têm esse acesso não pode editar outras contas do administrador.

Tabela 8. Descrição da janela Gerenciamento de Função de Usuário parâmetros (continuação)

Parâmetro	Descrição
Ofensas	Concede o acesso a todas as funções na guia **Ofensas** . Você pode conceder permissões específicas : **Designar Crimes a Usuários** Concede permissão para designar ofensas a outros usuários. **Manter Regras Customizadas** Concede permissão para criar e editar regras customizadas. **Gerenciar Motivos de Encerramento de Crime** Concede permissão para gerenciar ofensas de razões de fechamento. **Visualizar Regras Customizadas** Concede permissão para visualizar regras customizadas. Se concedidas a uma função de usuário que não terá também a permissão **Manter regras customizadas** , a função do usuário não pode criar ou editar regras customizadas.
Atividade do Log	Concede acesso a funções na guia **Atividade de Log** . Você também pode conceder permissões específicas : **Manter Regras Customizadas** Concede permissão para criar ou editar regras que são exibidos na guia **Atividade de Log** . **Gerenciar Série Temporal** Concede permissão para configurar e visualizar gráficos de dados série temporal. **Propriedades de Eventos Definidas pelo Usuário** Concede permissão para criar propriedades de evento customizado. Para obter informações adicionais sobre propriedades de eventos customizados, consulte a *Guia do Usuário* para seu produto. **Visualizar Regras Customizadas** Concede permissão para visualizar regras customizadas. Se concedidas a uma função de usuário que não terá também a permissão **Manter regras customizadas** , a função do usuário não pode criar ou editar regras customizadas.

Tabela 8. Descrição da janela Gerenciamento de Função de Usuário parâmetros (continuação)

Parâmetro	Descrição
Recursos	**Nota:** Esta permissão é exibida somente se IBM Security QRadar Vulnerability Manager for instalado em seu sistema. Concede acesso à função na guia **Ativos** . Você pode conceder permissões específicas : **Desempenhe VA Varreduras** Concede permissão para concluir varreduras de avaliação de vulnerabilidades. Para obter informações adicionais sobre de avaliação de vulnerabilidades, consulte a guia *Gerenciando Avaliação de Vulnerabilidades*. **Remover Vulnerabilidades** Concede permissão para remover as vulnerabilidades de ativos. **Servidor Discovery** Concede permissão para descobrir servidores. **Visualização VA Data** Concede permissão aos dados de avaliação de vulnerabilidades. Para obter informações adicionais sobre de avaliação de vulnerabilidades, consulte o *Gerenciando guia Avaliação de Vulnerabilidades.*

Tabela 8. Descrição da janela Gerenciamento de Função de Usuário parâmetros (continuação)

Parâmetro	Descrição
Atividade da Rede	Concede acesso a todas as funções na guia **Atividade de Rede** . Você pode conceder acesso específico para as seguintes permissões: **Manter Regras Customizadas** Concede permissão para criar ou editar regras que são exibidos na guia **Atividade de Rede** . **Gerenciar Série Temporal** Concede permissão para configurar e visualizar gráficos de dados série temporal. **Propriedades de Fluxo Definidas pelo Usuário** Concede permissão para criar propriedades do fluxo customizado. **Visualizar Regras Customizadas** Concede permissão para visualizar regras customizadas. Se a função do usuário não terá também a permissão **Manter regras customizadas** , a função do usuário não pode criar ou editar regras customizadas. **Visualizar Conteúdo do Fluxo** Concede permissão para acesso ao fluxo de dados.
Relatórios	Concede permissão para acesso a todas as funções no guia **Relatórios** . Você pode conceder aos usuários permissões específicas : **Distribuir Relatórios por E-mail** Concede permissão para distribuírem relatórios por meio de email. **Manter Gabaritos** Concede permissão para editar os modelos de relatório.
Gerenciador de Vulnerabilidade	Concede permissão para QRadar Vulnerability Manager função. IBM Security QRadar Vulnerability Manager deve ser ativada. Para obter informações adicionais, consulte *IBM Security QRadar Vulnerability Manager User Guide*.

Tabela 8. Descrição da janela Gerenciamento de Função de Usuário parâmetros (continuação)

Parâmetro	Descrição
Forense	Concede permissões para os recursos do QRadar Incident Forensics. **Crie casos no Resposta a Insidentes** Concede permissões para criar casos para coleções de documentos importados e arquivos pcap.
Clique com o botão direiro em extensões IP	Concede permissão para opções incluídas no menu de atalho.
Configuração de plataforma	Concede permissão para serviços **Configuração de Plataforma** . **Descartar Notificações do Sistema** Concede permissão para oculte notificações do sistema da guia **Mensagens** . **Visualizar Notificações do Sistema** Concede permissão para visualizar as notificações do sistema a partir da guia **Mensagens** .

Parâmetros de perfil de segurança

A tabela a seguir fornece descrições dos parâmetros da janela Gerenciamento de perfil de segurança

Tabela 9. Parâmetros da janela Gerenciamento de perfil de segurança

Parâmetro	Descrição
Nome do perfil de segurança	Digite um nome exclusivo para o perfil de segurança. O nome do perfil de segurança deve atender aos requisitos a seguir: • Mínimo de 3 caracteres • Máximo de 30 caracteres
Descrição	`Opcional.` Digite uma descrição do perfil de segurança. O número máximo de caracteres é 255.

Parâmetros da janela de gerenciamento do usuário

A tabela a seguir fornece descrições dos parâmetros da janela de gerenciamento do usuário:

Tabela 10. Parâmetros da janela de gerenciamento do usuário

Parâmetro	Descrição
Nome de usuário	Exibe o nome do usuário desta conta do usuário.
Descrição	Exibe a descrição da conta do usuário.
e-mail	Exibe o endereço de e-mail desta conta do usuário.

Tabela 10. Parâmetros da janela de gerenciamento do usuário (continuação)

Parâmetro	Descrição
Função de usuário	Exibe a função do usuário que está designada a esta conta de usuário. Funções do usuário definem quais ações o usuário tem permissão para executar.
Perfil de Segurança	Exibe o perfil de segurança que é designado a esta conta de usuário. Perfis de Segurança definem quais dados o usuário tem permissão para acessar.

Barra de ferramentas da janela de gerenciamento do usuário

Barra de ferramentas da janela de gerenciamento de funções do usuário

A tabela a seguir fornece descrições das funções da barra de ferramentas da janela Gerenciamento do usuário

Tabela 11. Funções da barra de ferramentas da janela de gerenciamento do usuário

Função	Descrição
Novo	Clique neste ícone para criar uma conta do usuário. Para obter informações adicionais sobre como criar uma conta de usuário, consulte “Criando uma Conta do Usuário” na página 17.
Editar	Clique nesse ícone para editar a conta de usuário selecionada.
Excluir	Clique nesse ícone para excluir a conta de usuário selecionada.
Procurar Usuários	Nesta caixa de texto, você pode digitar uma palavra-chave e, em seguida, pressione Enter para localizar uma conta de usuário específica.

Parâmetros da janela Detalhes do Usuário

Parâmetros da janela Detalhes do Usuário

A tabela a seguir fornece descrições dos parâmetros: janela Detalhes do Usuário

Tabela 12. Parâmetros da janela Detalhes do Usuário

Parâmetro	Descrição
Nome de usuário	Digite um nome de usuário exclusivo para o novo usuário. O nome de usuário deve conter no máximo 30 caracteres.
e-mail	Digite o endereço de e-mail do usuário. O endereço de e-mail deve atender aos seguintes requisitos: • Deve ser um endereço de e-mail válido • Mínimo de 10 caracteres • Máximo de 255 caracteres

Tabela 12. Parâmetros da janela Detalhes do Usuário (continuação)

Parâmetro	Descrição
Senha	Digite uma senha para o usuário para obter acesso. A senha deve atender aos seguintes critérios: • Mínimo de 5 caracteres • Máximo de 255 caracteres
Confirme a senha	Digite a senha novamente para confirmação.
Descrição	`Opcional.` Digite uma descrição para a conta do usuário. O número máximo de caracteres é 2.048.
Função de usuário	Na caixa de listagem, selecione a função do usuário que você deseja designar para este usuário. Para incluir, editar ou excluir as funções de usuário, você pode clicar no link **Gerenciar Funções do Usuário**. Para obter informações sobre funções de usuário, consulte "Gerenciador de função" na página 11.
Perfil de Segurança	Na caixa de listagem, selecione o perfil de segurança que você quer designar para este usuário. Para incluir, editar ou excluir perfis de segurança, você pode clicar no link **Gerenciar Perfis de Segurança**. Para obter informações sobre perfis de segurança, consulte "Gerenciando perfis de segurança" na página 13.

Capítulo 4. Gerenciamento de licenças e sistema

É possível gerenciar as licenças, alta disponibilidade (HA) e os sistemas em sua implementação.

Você deve alocar uma licença para cada sistema em sua implementação, incluindo dispositivos de software.QFlow e QRadar Event Collectors não requer uma licença.

Quando você instala um QRadar do sistema, uma chave de licença padrão fornece a você acesso à interface com o usuário para cinco semanas. Antes da expiração da licença padrão, você deve alocar uma chave de licença para seu sistema. Você também pode incluir licenças para ativar produtos QRadar , como QRadar Vulnerability Manager.

Há um período de carência de 14 dias para realocar uma licença. Você pode desbloquear uma licença se a chave for transferida por upload, após um host é corrigido com uma correção, ou após uma chave desbloquear é transferido por upload. Após o período de carência passar, a licença é bloqueada para o sistema.

Se o seu status de licença for **inválido**, a licença deve ser substituída. O status pode indicar que a licença foi alterada sem autorização.

Uma licença removida permanece até que você implemente a alteração de licença.

Janela Visão geral de Gerenciamento e Licença do Sistema

Você pode utilizar a janela System and License Management para gerenciar suas chaves de licenças, reiniciar ou encerrar o sistema, e configurar as configurações de acesso.

A barra de ferramentas na janela System and License Management fornece as seguintes funções:

Tabela 13. Funções de Gerenciamento e Licensa do Sistema na barra de tarefas

Função	Descrição
Alocar Licença para Sistema	Use esta função para alocar uma licença para o sistema. Se você selecionar **Licenças** a partir da lista de opções **Exibir** na caixa de listagem Detalhes de Implementação, as funções a seguir estão disponíveis no menu **Ações** :
Fazer Upload da Licença	Use esta função para fazer upload de uma licença para o Console. Para obter informações adicionais, consulte “Fazendo Upload de uma Chave de Licença” na página 40.
Ações (Licença)	Se **Licenças** for selecionada a partir da caixa de seleção **Exibir** no painel detalhes de implementação, as funções a seguir estarão disponíveis no menu **Ações**: Se você selecionar **Reverter Alocação** em uma licença implementada dentro do período de carência de alocação, que é 14 dias após a implementação, o estado da licença é alterado para **Desbloqueado** para que seja possível realocar a licença para um outro sistema.

Tabela 13. Funções de Gerenciamento e Licensa do Sistema na barra de tarefas (continuação)

Função	Descrição
Ações (Sistema)	Se **Sistemas** da caixa de listagem **Exibir** for selecionada nos detalhes de implementação da janela, as funções a seguir estarão disponíveis no menu **Ações**. • **Visualizar sistema** – Selecionar um sistema, e, em seguida, selecione esta opção para exibir a janela Detalhes do Sistema. Para obter informações adicionais, consulte "Visualizando Detalhes do Sistema" na página 43. • **Reverter Alocação** – Selecione esta opção para desfazer alterações de licença. A configuração será revertido para o último implementado de alocação de licença. Se você selecionar **Reverter Alocação** em uma licença implementada dentro do período de carência de alocação, que é 14 dias após a implementação, o estado da licença é alterado para **Desbloqueado** para que seja possível realocar a licença para um outro sistema. • **Gerenciar Sistema** – Selecionar um sistema, e, em seguida, selecione esta opção para abrir a janela Configuração do sistema , que pode ser utilizado para configurar regras de firewall, funções de interface, senhas, e a hora do sistema. Para obter informações adicionais, consulte "Gerenciamento da configuração de acesso" na página 48. • **Reiniciar Servidor da Web** – Selecione essa opção para reiniciar a interface com o usuário, quando necessário. Por exemplo, você pode ser solicitado a reiniciar sua interface com o usuário depois de instalar um novo protocolo que apresenta os componentes da interface com o usuário novo. • **Encerramento do Sistema** – Selecionar um sistema e, em seguida, selecione esta opção para encerrar o sistema. Para obter informações adicionais, consulte "Encerrando um Sistema" na página 46. • **Encerramento do Sistema** – Selecionar um sistema e, em seguida, selecione esta opção para encerrar o sistema. Para obter informações adicionais, consulte "Reiniciando um Sistema" na página 45.

Quando você selecionar **Licenças** a partir da lista de opções **Exibir** na área de janela Detalhes de Implementação, a janela System and License Managementexibe as seguintes informações:

Tabela 14. Janela de parâmetros Gerenciador de Licença e Sistema. – visualizar licenças.

Parâmetro	Descrição
Nome do host	Exibe o nome do host do sistema que está alocada para esta licença.
IP do Host	Exibe o endereço IP do sistema que é alocada para esta licença.
Tipo de Dispositivo	Exibe o tipo de dispositivo do sistema que é alocada para esta licença.
Identidade da Licença	Exibe o nome do IBM Security QRadar do produto dessa licença fornece.

Tabela 14. Janela de parâmetros Gerenciador de Licença e Sistema. – visualizar licenças (continuação).

Parâmetro	Descrição
Status da Licença	Exibe o status da licença que está alocada para esse sistema. Os status incluem: • **Não alocada** – Indica que esta licença não está alocada para um sistema. • **Não implementada** - Indica que esta licença está alocada para um sistema, mas não é possível implementar a mudança de alocação. Isso significa que a licença não está ativa em sua implementação ainda. • **Implementada** – Indica que essa licença é alocada e ativa em sua implementação. • **Desbloqueada** – Indica que essa licença foi desbloqueada. É possível desbloquear uma licença caso ela tenha sido implementada nos últimos 10 dias. Esse é o período de carência padrão para realocar uma licença. Após o período de carência passar, a licença é bloqueada para o sistema. Se você deve desbloquear uma licença após esse período, entre em contato com o Suporte ao Cliente. • **Nome** – Indica que esta licença não é válida e deve ser substituída. Esse status pode indicar que a licença foi alterada sem autorização.
Data de Expiração da Licença	Exibe a data de expiração desta licença.
Limite de Taxa do Evento	Exibe a taxa de eventos limite sua licença permite.
Limite de Taxa de Fluxo	Exibe a taxa de fluxo limitar sua licença permite.

Lista de verificação de gerenciamento de licenças

Utilize as opções disponíveis na janela Gerenciamento de Sistema e Licença para gerenciar suas chaves de licença.

Uma chave de licença padrão fornece a você acesso à interface com o usuário por cinco semanas. Você deve alocar uma chave de licença para seu sistema.

Deve-se configurar o sistema QRadar antes de os usuários poderem usar as ferramentas. Comece obtendo uma chave de licença. Após ter uma chave de licença, você deverá fazer seu upload no console e alocá-la para um sistema.

Durante a configuração inicial de um sistema, deve-se concluir as seguintes tarefas:

Procedimento

1. Obtenha uma chave de licença por um dos seguintes métodos:
   - Para obter uma chave de licença nova ou atualizada, entre em contato com seu representante de vendas local.

- Para todas as outras questões técnicas, entre em contato com o Suporte ao Cliente.

2. Faça upload de sua chave de licença.

   Quando você faz upload de uma chave de licença, ela é listada na janela Gerenciamento de Sistema e Licença, mas permanece não alocada. Para obter informações adicionais, consulte "Fazendo Upload de uma Chave de Licença"
3. Aloque sua licença para um sistema ou aloque um sistema para sua licença.
4. Para implementar suas mudanças, no menu da guia **Admin**, clique em **Avançado** > **Implementar Configuração Integral**.

   Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Fazendo Upload de uma Chave de Licença

Você deve fazer upload de uma chave de licença para o Console quando instala um novo sistema QRadar, atualiza uma licença expirada ou inclui um produto QRadar, tal como o QRadar Vulnerability Manager, em sua implementação.

Antes de Iniciar

Escolha uma das opções a seguir para obter assistência com sua chave de licença:

1. Para obter uma chave de licença nova ou atualizada, entre em contato com seu representante de vendas local.
2. Para todas as outras questões técnicas, entre em contato com o Suporte ao Cliente.

Sobre Esta Tarefa

Se você efetuar login na interface com o usuário e a chave de licença do Console expirou, você será automaticamente direcionado para a janela Gerenciamento de Sistema e Licença. Você deve fazer upload de uma chave de licença antes que possa continuar. Se um de seus sistemas não do Console incluir uma chave de licença expirada, uma mensagem será exibida quando você efetuar login, indicando que um sistema requer uma nova chave de licença. Você deve acessar a janela Gerenciamento de Sistema e Licença para atualizar essa chave de licença.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na barra de ferramentas, clique em **Fazer Upload da Licença**.
5. Na caixa de diálogo, clique em **Selecionar Arquivo**.
6. Na janela Upload de Arquivo, localize e selecione a chave de licença.
7. Clique em **Abrir**.
8. Clique em **Fazer Upload**.

Resultados

A licença é transferida por upload para o Console e é exibida na janela Gerenciamento de Sistema e Licença. Por padrão, a licença não está alocada.

O que Fazer Depois

"Alocando um sistema para uma licença" na página 45

Alocando uma licença para um sistema

Utilize as opções na janela System and License Management para alocar uma licença.

Sobre Esta Tarefa

Quando você instala um QRadar do sistema, uma chave de licença padrão fornece a você acesso à interface com o usuário para cinco semanas. Antes da expiração da licença padrão, você deve alocar uma chave de licença para seu sistema. Você também pode incluir licenças para ativar os produtos QRadar, como QRadar Vulnerability Manager.

Status de Licença exibe o status da licença que é alocada para esse sistema. Os status incluem:

- Não alocada - Indica que esta licença não está alocada para um sistema.
- Não implementada - Indica que essa licença está alocada para um sistema, mas você não implementou a mudança de alocação. Isso significa que a licença não está ativa em sua implementação ainda.
- Implementada - Indica que essa licença está alocada e ativa em sua implementação.
- Desbloqueada - Indica que essa licença foi desbloqueada. Você pode desbloquear uma licença se tiver sido implementada nos últimos 14 dias. Esse é o período de carência padrão para realocar uma licença. Após o período de carência passar, a licença é bloqueada para o sistema. Se você deve desbloquear uma licença após esse período, entre em contato com o Suporte ao Cliente.
- Inválida - Indica que esta licença não é válida e deve ser substituída. Esse status pode indicar que sua licença foi alterada sem autorização.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Licenças**.
5. Selecione um sistema disponível.
6. Clique em **Sistema para Alocar Licença**.
7. Opcional: Para filtrar a lista de licenças, digite uma palavra-chave na caixa de procura **Upload da Licença**.
8. Na lista de licenças, selecione uma licença.
9. Selecione um sistema.
10. Clique em **Alocar Licença para Sistema**.

Revertendo uma Alocação

É possível reverter uma licença alocada dentro do período de carência de 14 dias.

Sobre Esta Tarefa

Depois que você aloca uma licença para um sistema e antes de implementar suas mudanças na configuração, é possível desfazer a alocação de licença. Ao desfazer a alocação de licença, a licença que foi alocada e implementada pela última vez no sistema é mantida.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Licenças**.
5. Selecione a licença que você deseja reverter.
6. Clique em **Ações** > **Reverter Alocação**.

Visualizando Detalhes da Licença

Uma chave de licença fornece informações e reforça os limites e habilidades em um sistema IBM Security QRadar.

Sobre Esta Tarefa

Na janela Gerenciamento de Sistema e Licença, é possível visualizar detalhes da licença, como o número de fontes de log permitidas e as datas de expiração.

Nota: Se você exceder o limite de fontes de logs configuradas, uma mensagem de erro será exibida. Se as fontes de log forem descobertas automaticamente e o limite for excedido, elas serão desativadas automaticamente. Para ampliar o número de fontes de log, entre em contato com seu representante de vendas.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Licenças**.
5. Para exibir a janela **Detalhes da Licença Atual** para uma licença, clique duas vezes na licença que você deseja visualizar.

O que Fazer Depois

Na janela **Licença Atual** é possível concluir as seguintes tarefas:

- Clique em **Fazer upload de licenças** para fazer o upload da licença. Consulte Fazendo Upload de uma Chave de Licença.
- Clique em **Alocar Licença para Sistema** na barra de ferramentas para designar uma licença. Consulte Alocando um Sistema para uma Licença.

Exportando uma Licença

Exporte informações da chave de licença para um sistema de desktop.

Sobre Esta Tarefa

É possível exportar informações da chave de licença para um arquivo externo em seu sistema de desktop.

Procedimento

1. Clique na guia **Administração**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Licenças**.
5. A partir do menu **Ações**, selecione **Exportar Licenças**.
6. Selecione uma das opções a seguir:
   - **Abrir com** – Abre os dados da chave de licença utilizando o aplicativo selecionado.
   - **Salvar Arquivo** – Salva o arquivo em seu desktop.
7. Clique em **OK**.

Gerenciamento de sistemas

Use a janela Gerenciamento de sistemas e licensas para gerenciar sistemas em sua implementação.

Use as opções disponíveis na janela Gerenciamento de sistemas e licensas para gerenciar sistemas em sua implementação. É possível visualizar detalhes do sistema, designar uma licensa a um sistema ou reiniciar e encerrar um sistema.

Visualizando Detalhes do Sistema

Visualize as informações sobre o sistema, incluindo licenças da janela Detalhes do Sistema.

Sobre Esta Tarefa

Abra a janela Detalhes do Sistema para visualizar informações sobre o sistema e a lista de licenças que estão alocadas para o sistema.

A lista de licenças fornece os seguintes detalhes para cada licença que está alocada para este sistema:

Tabela 15. Parâmetros de Licença

Parâmetro	Descrição
Identidade da Licença	Exibe o nome do produto do QRadar que essa licença fornece.

Tabela 15. Parâmetros de Licença (continuação)

Parâmetro	Descrição
Status da Licença	Exibe o status da licença que está alocada para esse sistema. Os status incluem: • Não alocada - Indica que esta licença não está alocada para um sistema. • Não implementada - Indica que essa licença está alocada para um sistema, mas você não implementou a mudança de alocação. Isso significa que a licença não está ativa em sua implementação ainda. • Implementada - Indica que essa licença está alocada e ativa em sua implementação. • Desbloqueada - Indica que essa licença foi desbloqueada. É possível desbloquear uma licença se ela tiver sido implementada nos últimos 10 dias. Esse é o período de carência padrão para realocar uma licença. Após o período de carência passar, a licença é bloqueada para o sistema. Se você precisar desbloquear uma licença após esse período, entre em contato com o Suporte ao Cliente. • Inválida - Indica que esta licença não é válida e deve ser substituída. Esse status pode indicar que sua licença foi alterada sem autorização.
Tipos de Dispositivo de Licença	Exibe o tipo de dispositivo para o qual esta licença é válida.
Data de Expiração da Licença	Exibe a data de expiração desta licença.
Limite de Taxa do Evento	Exibe o limite de taxa de eventos que essa licença permite.
Limite de Taxa de Fluxo	Exibe o limite de taxa de fluxo que esta licença permite.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Para exibir os detalhes do sistema, dê um clique duplo no sistema que você deseja visualizar.

O que Fazer Depois

Na janela Detalhes do Sistema, você pode concluir as seguintes tarefas:

- Selecione uma licença e clique em **Visualizar Licença**. Consulte "Visualizando Detalhes da Licença" na página 42.
- Clique em **Fazer upload de licenças** para fazer o upload da licença. Consulte "Fazendo Upload de uma Chave de Licença" na página 40.

- Clique em **Alocar Licença para Sistema** na barra de ferramentas para designar uma licença. Consulte "Alocando um sistema para uma licença".

Funcionamento do sistema

A visualização Funcionamento do sistema mostra notificações do sistema e informações de funcionamento para o host do IBM Security QRadar.

Selecione o ícone **Administrador** > **Configuração do Sistema** > **Funcionamento do Sistema** na área de Configuração do Sistema na guia Administrador para visualizar o uso da CPU, leituras e gravações da rede, leituras e gravações do disco, uso da memória, eventos por segundo (EPS) e fluxos por segundo (FPS).

Passe o mouse sobre um gráfico para visualizar mais informações e a métrica que está sendo graficamente representada.

Alocando um sistema para uma licença

Após obter uma licensa, utilize as opções na janela System and License Management para alocar uma licença.

Você pode alocar várias licenças para um sistema. Por exemplo, adicionando o IBM Security QRadar SIEM, você pode alocar IBM Security QRadar Risk Managere IBM Security QRadar Vulnerability Manager para seu sistema QRadar Console.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Selecione um sistema disponível.
6. Clique em **Alocar Licença para Sistema**.
7. Opcional: Para filtrar a lista de licenças, digite uma palavra-chave na caixa de procura Upload da Licença.
8. Na lista de licenças, selecione uma licença.
9. Selecione um sistema.
10. Clique em **Alocar Licença para Sistema**.

Reiniciando um Sistema

Utilize a opção **Reiniciar Sistema** na janela Gerenciamento de Sistema e Licença para reiniciar um sistema em sua implementação.

Sobre Esta Tarefa

A coleta de dados para enquanto o sistema está encerrando e reiniciando.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Selecione o sistema que você deseja reiniciar.

6. A partir do menu **Ações**, selecione **Reiniciar Sistema**.

Encerrando um Sistema

Utilize a opção **Encerrar** na janela Gerenciamento de Sistema e Licença para encerrar um sistema.

Sobre Esta Tarefa

A coleta de dados para enquanto o sistema está encerrando.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Selecione o sistema que deseja encerrar.
6. A partir do menu **Ações**, selecione **Encerrar**.

Exportando Detalhes do Sistema

Use a opção **Exportar Sistemas** na janela Gerenciamento de Licença e Sistema para exportar informações do sistema para um arquivo externo na área de trabalho do sistema

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. A partir do menu **Ações**, selecione **Exportar Sistemas**.
6. Selecione uma das opções a seguir:
   - **Abrir com** – Abre os dados da chave de licença utilizando o aplicativo selecionado.
   - **Salvar Arquivo** – Salva o arquivo em seu desktop.
7. Clique em **OK**.

Coletando arquivos de log

Os arquivos de log do QRadar contêm informações detalhadas sobre a implementação, como nomes de host, endereços IP e endereços de email. Caso precise de ajuda para a resolução de problemas, é possível coletar os arquivos de log e enviá-los para o Suporte ao Cliente IBM.

Sobre Esta Tarefa

É possível coletar arquivos de log diretamente do QRadar.

É possível coletar os arquivos de log de um ou mais sistemas host ao mesmo tempo. O tempo necessário para coletar os arquivos de log depende do tamanho da implementação e do número de hosts a serem incluídos na coleta de arquivos de log. Os arquivos de log do console do QRadar são incluídos automaticamente em todas as coletas de arquivos de log.

É possível continuar a usar o console do QRadar durante a execução da coleta de arquivos de log. Se o sistema estiver ativamente coletando arquivos de log, não é possível iniciar uma nova solicitação de coleta. Deve-se cancelar o processo de coleta ativo e iniciar outra coleta.

Após a conclusão do processo de coleta de arquivos de log, uma notificação do sistema aparece no painel **Monitoramento do Sistema**.

Procedimento

1. Clique na guia **Admin**.
2. Na janela de navegação, clique em **Configuração do Sistema** e clique no ícone **Gerenciamento de Sistema e Licença**.
3. Pressione Ctrl e clique em cada host a ser incluído na coleta de arquivos de log.
4. Clique em **Ações** > **Coletar Arquivos de Log**.
5. Clique em **Opções Avançadas** e escolha as opções para a coleta de arquivos de log. As coletas de arquivos de log criptografadas podem ser decriptografadas apenas pelo Suporte ao Cliente IBM. Caso deseje acessar a coleta de arquivos de log, não criptografe o arquivo.
6. Clique em **Coletar Arquivos de Log**.
7. Em **Mensagens de Atividades do Suporte ao Sistema**, uma mensagem indica o status do processo de coleta.

   Para cancelar um processo ativo de coleta de arquivos de log, clique no **X** na mensagem de notificação.
8. Para fazer download da coleta de arquivos de log, clique em **Clique aqui para fazer download dos arquivos** na notificação **Coleta de arquivos de log concluída com êxito**.

Implementando hosts e componentes gerenciados após a instalação

Depois da instalação, é possível incluir hosts gerenciados na imp lementação doIBM Security QRadar SIEM. Para ajudar a distribuir o processamento, você pode incluir o QRadar Event Collectors, o QRadar Processadores de Fluxo ou outros dispositivos em sua implementação.

É possível configurar os componentes, como scanners de vulnerabilidade, em um host gerenciado.

Nota: Use o **Editor de implementação** para incluir e configurar componentes de sua instalação de software. Você não pode ver visualizações de sua implementação em **Ações de implementação**.

Se você configurou o IBM Security QRadar Incident Forensics em sua implementação, pode incluir um host gerenciado do QRadar Incident Forensics. Para obter informações adicionais, consulte *Guia de instalação do IBM Security QRadar Incident Forensics*.

Se você configurou o IBM Security QRadar Vulnerability Manager em sua implementação, poderá incluir scanners de vulnerabilidade e um processador de vulnerabilidade. Para obter informações adicionais, consulte *IBM Security QRadar Vulnerability Manager User Guide*.

Se deseja gerenciamento de risco, você precisa instalar o IBM Security QRadar Risk Manager e, em seguida, incluir um host gerenciado. Para obter informações adicionais, consulte *IBM Security QRadar Risk Manager Installation Guide*.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela **Configuração do Sistema**, clique em **Gerenciamento do Sistema e de Licença**.
3. Na tabela de host, selecione uma das opções a seguir que você deseja gerenciar.
   - QRadar Console
   - Host gerenciado do QRadar
4. No menu **Ações de implementação**, escolha uma ação.
5. Insira as informações para a ação que você deseja realizar.
6. Feche a janela Gerenciamento do Sistema e de Licença.
7. Clique na guia **Admin**.
8. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Tarefas relacionadas:

"Incluindo Componentes" na página 144
Ao configurar sua implementação, você deve utilizar a página Visualização de Eventos no editor de implementação para incluir os componentes.

Gerenciamento da configuração de acesso

É possível usar a janela Configuração de sistema para configurar regras de firewall, funções de interface, senhas e tempos de sistemas.

Se a rede exigir mudanças de configuração da rede, tal como uma mudança de endereço IP, para seus sistemas de console e que não são de console após a instalação inicial de sua implementação, você deverá usar o utilitário **qchange_netsetup** para efetuar essas mudanças. Para obter informações adicionais sobre configurações de rede, consulte o *Guia de Instalação* de seu produto.

Configurando o Acesso ao Firewall

É possível configurar o acesso ao firewall local para ativar as comunicações entre dispositivos e o IBM Security QRadar. Além disso, você pode definir o acesso à janela Configuração do sistema.

Sobre Esta Tarefa

Apenas os hosts gerenciados listados que estão listados na caixa **Acesso de Dispositivo** têm acesso ao sistema selecionado. Por exemplo, se você inserir um endereço IP, apenas esse endereço IP terá acesso concedido ao Console. Todos os outros hosts gerenciados serão bloqueados.

Se você alterar o parâmetro **Porta de Monitoramento de Fonte de Fluxo Externa** na configuração doQFlow, também deverá atualizar a configuração de acesso ao firewall. Para obter informações adicionais sobre a configuração do QFlow, consulte Capítulo 11, "Editor de implementação", na página 139.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.

3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Selecione o host para o qual você deseja configurar as definições de acesso ao firewall.
6. No menu **Ações**, selecione **Gerenciar Sistema**.
7. Efetue login na janela Configuração do sistema. O padrão é:
   a. **Nome de Usuário:** `root`
   b. **Senha:** `<senha>` O nome de usuário e a senha fazem distinção entre maiúsculas e minúsculas.
8. No menu, selecione **Configuração do Host Gerenciado** > **Firewall Local**.
9. Configure os seguintes parâmetros de Acesso ao Dispositivo:

Opção	Descrição
Acesso ao Dispositivo	Na caixa **Acesso ao Dispositivo**, inclua todos os sistemas IBM que você deseja acessar para este host gerenciado. Apenas os hosts gerenciados listados possuem acesso. Por exemplo, se você inserir um endereço IP, apenas esse endereço IP terá acesso concedido ao host gerenciado. Todos os outros hosts gerenciados serão bloqueados.
Endereço IP	Digite o endereço IP do host gerenciado ao qual você deseja ter acesso.
Protocolo	Selecione o protocolo para o qual você deseja ativar o acesso para o endereço IP e a porta especificados. As opções incluem: • **UDP** – Permite tráfego de UDP. • **TCP** - Permite tráfego de TCP. • **Any** - Permite qualquer tráfego.
Porta	Digite a porta na qual você deseja ativar as comunicações.

10. Clique em **Permitir**.
11. Configure o parâmetro de Controle da Web de Administração do Sistema:

    Digite os endereços IP de hosts gerenciados aos quais você deseja permitir acesso à janela Configuração do sistema no campo **Endereço IP**. Apenas os endereços IP listados têm acesso à interface com o usuário. Se você deixar o campo em branco, todos os endereços IP terão acesso.

    Certifique-se de incluir o endereço IP de sua área de trabalho do cliente que deseja utilizar para acessar a interface com o usuário. A falha ao fazer isso pode afetar a conectividade.
12. Clique em **Permitir**.
13. Clique em **Aplicar Controle de Acesso**.
14. Aguarde a janela Configuração do sistema atualizar antes de continuar uma outra tarefa.

Atualizando a Configuração do Host

É possível utilizar a janela Configuração do sistema para configurar o servidor de correio que você deseja utilizar e a senha global para todos os sistemas em sua implementação doQRadar.

Sobre Esta Tarefa

A senha de configuração global não aceita caracteres especiais. A senha de configuração global deve ser a mesma em toda a sua implementação. Se você editar esta senha, também deverá editar a senha de configuração global em todos os sistemas em sua implementação.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Selecione o host para o qual você deseja atualizar as definições de configuração do host.
6. A partir do menu **Ações**, selecione **Gerenciar Sistema.**
7. Efetue login na janela Configuração do sistema. O padrão é:
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`

      O nome de usuário e a senha fazem distinção entre maiúsculas e minúsculas.
8. No menu, selecione **Configuração do Host Gerenciado** > **Configuração do QRadar**.
9. No campo **Servidor de Correio**, digite o endereço para o servidor de correio que você deseja utilizar. O QRadar SIEM utiliza este servidor de correio para distribuir alertas e mensagens do evento. Para utilizar o servidor de correio que o QRadar SIEM fornece, digite `localhost`.
10. Em **Insira a senha de configuração global**, digite a senha que você deseja utilizar para acessar o host. Digite a senha novamente para confirmação.
11. Clique em **Aplicar Configuração**.

Configurando Funções de Interface

É possível designar funções específicas para as interfaces de rede em cada host gerenciado.

Antes de Iniciar

Para obter assistência para determinar a função apropriada para cada interface, entre em contato com o Suporte ao Cliente.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Selecione o host para o qual você deseja configurar as definições de função da interface.
6. A partir do menu **Ações**, selecione **Gerenciar Sistema.**
7. Efetue login na janela Configuração do sistema. O padrão é:
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`

O nome de usuário e a senha fazem distinção entre maiúsculas e minúsculas.

8. No menu, selecione **Configuração do Host Gerenciado** > **Interfaces de Rede**.
9. Para cada interface de rede listada, selecione a função que deseja designar à interface na caixa de listagem **Função**.
10. Clique em **Salvar Configuração**.
11. Aguarde a janela Configuração do sistema atualizar antes de continuar.

Alterando a senha raiz do seu sistema QRadar

Você pode alterar a senha do root para seu sistema.

Antes de Iniciar

Quando a senha for modificada, assegure-se que os valores inseridos foram gravados. A senha raiz não aceita os seguintes caracteres especiais : apóstrofo ('), sinal de cifrão ($), exclamação (!).

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Selecione o host para o qual você deseja configurar as definições de função da interface.
6. No menu **Ações**, selecione **Gerenciar Sistema**.
7. Efetue login na janela Configuração do sistema. O padrão é:
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`

   O nome de usuário e a senha fazem distinção entre maiúsculas e minúsculas.
8. No menu, selecione **Configuração Host Gerenciado** > **Raiz Senha**.
9. Atualize a senha:
   a. –**Nova senha raiz** Digite a senha raiz necessária para acessar a janela Configuração do sistema.
   b. **Confirmar nova senha raiz** – Digite a senha novamente para confirmação.
10. Clique em **Atualizar senha**.

Configuração do tempo do sistema do QRadar

Ao executar um sistema que abrange diversos fusos horários, configure todos os dispositivos para usarem o mesmo fuso horário que o IBM Security QRadar Console. Como alternativa, é possível configurar todos os dispositivos, incluindo o QRadar Console, para usar a Hora de Greenwich (GMT).

Use um dos métodos a seguir para configurar o tempo do sistema do IBM Security QRadar:

- Configure um servidor Network Time Protocol (NTP) para manter o tempo do sistema.

  O horário é sincronizado automaticamente entre o QRadar Console e os hosts gerenciados.
- Configure o tempo do sistema manualmente.

Problemas causados pelos fusos horários incompatíveis

Para assegurar que as procuras e funções relacionadas a dados funcionem adequadamente, todos os dispositivos devem sincronizar configurações de tempo com o dispositivo QRadar Console. Quando as configurações do fuso horário forem incompatíveis, será possível ver resultados inconsistentes entre procuras do QRadar e dados do relatório.

O serviço Acumulador é executado em todos os dispositivos com armazenamento local para criar acumulações de minuto a minuto e rollups horários e diários. O QRadar usa os dados acumulados nos relatórios e gráficos de séries temporais. Quando os fusos horários são incompatíveis em uma implementação distribuída, o relatório e os gráficos de séries temporais podem mostrar resultados inconsistentes quando comparados com resultados de consulta AQL devido à forma como os dados acumulados são agregados.

As procuras do QRadar são executadas com relação aos dados que são armazenados nos bancos de dados Ariel, que usam uma estrutura de data (AAAA/MM/DD/HH/MM) para armazenar arquivos no disco. Mudar o fuso horário após os dados terem sido gravados no disco interromperá a sequência de nomenclatura de arquivo nos bancos de dados Ariel e poderá causar problemas de integridade de dados.

Configurando o servidor de tempo usando o RDATE

Utilize a guia sincrinizador do servidor de tempo para configurar seu servidor de tempo usando o RDATE.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Selecione o host para o qual você deseja configurar as definições de tempo do sistema.
6. No menu **Ações**, selecione **Gerenciar Sistema**.
7. Efetue login na janela Configuração do sistema.

   O nome de usuário e a senha fazem distinção entre maiúsculas e minúsculas.
8. No menu, selecione **Configuração do Host Gerenciado** > **Tempo do Sistema**.
9. Configure o fuso horário:
   a. Clique na guia **Alterar fuso horário**.
   b. Na caixa de listagem **Alterar o fuso horário para** , selecione o fuso horário no qual este host gerenciado está localizado.
   c. Clique em **Salvar**.
10. Configure o servidor de tempo :
    a. Clique na guia **Tempo de sincronização do servidor**.

       Configure os seguintes parâmetros:

Tabela 16. Parâmetros do servidor de Tempo

Parâmetro	Descrição
Nomes de servidores timeservers ou endereço	Digite o nome do host do servidor de tempo ou endereço IP.

Tabela 16. Parâmetros do servidor de Tempo (continuação)

Parâmetro	Descrição
Configure também, o tempo de hardware	Selecione esta caixa de opções se você deseja configurar o tempo de hardware.
Sincronizar no planejamento?	Selecione uma das opções a seguir: • Não – Selecione esta opção se você não deseja sincronizar a hora. Vá para a etapa c. • Sim – Selecione essa opção se você deseja sincronizar o tempo.
Planejamento Simples	Selecione esta opção se desejar que a atualização de tempo ocorra em um horário específico. Depois de selecionar essa opção, selecione um planejamento simples a partir da caixa de listagem.
Tempos e datas são selecionados abaixo	Selecione esta opção para especificar a hora que você deseja que a atualização de tempo para ocorrer. Depois de selecionar essa opção, selecione as horas e datas nas caixas de listagem.

11. Clique em **Sincronização e Aplicar**.

Configurando Manualmente as Configurações de Tempo para seu Sistema

Utilize as opções nas guias **Configurar Tempo** e **Alterar fuso horário** para configurar manualmente suas configurações de tempo.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Gerenciamento de Sistema e Licença**.
4. Na caixa de listagem **Exibir**, selecione **Sistemas**.
5. Selecione o host para o qual você deseja configurar as definições de tempo do sistema.
6. No menu **Ações**, selecione **Gerenciar Sistema**.
7. Efetue login na janela Configuração do sistema. O padrão é:
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`

   O nome de usuário e a senha fazem distinção entre maiúsculas e minúsculas.
8. No menu, selecione **Configuração do Host Gerenciado** > **Tempo do Sistema**.
9. Clique na guia **Configurar Tempo**.

   A página Configurar Tempo é dividida em guias. Você deve salvar cada configuração antes de continuar. Por exemplo, quando você configurar o tempo do sistema, deverá clicar em **Aplicar** na área de janela Tempo do Sistema antes de continuar.
10. Configure o tempo do sistema:
    a. Escolha uma das seguintes opções:

- Na área de janela Tempo do Sistema, utilizando as caixas de listagem, selecione a data e hora atuais que você deseja designar ao host gerenciado.
- Clique em **Configurar Tempo do Sistema para o Tempo de Hardware**.

b. Clique em **Aplicar**.

11. Configure o tempo de hardware:
    a. Escolha uma das seguintes opções:
       - Na área de janela Tempo de Hardware, utilizando as caixas de listagem, selecione a data e hora atuais que você deseja designar ao host gerenciado.
       - Clique em **Configurar Tempo de Hardware para o Tempo do Sistema**.

    b. Clique em **Salvar**.
12. Configure o fuso horário:
    a. Clique na guia **Alterar fuso horário**.
    b. Na caixa de listagem **Alterar fuso horário Para**, selecione o fuso horário no qual este host gerenciado está localizado.
    c. Clique em **Salvar**.

Capítulo 5. Configuração de fonte de informações sobre o usuário

Configure seu sistema IBM Security QRadar para coletar informações sobre o grupo e o usuário nos terminais Identidade e Gerenciamento de Acesso.

IBM Security QRadar SIEM utiliza as informações que são coletadas dos terminais para agregar valor às informações sobre o usuário que estão associadas ao tráfego e aos eventos que ocorrem em sua rede.

Visão geral de origem de informações do usuário

Você pode configurar uma fonte de informações sobre o usuário para ativar a coleta de informações do usuário a partir de um nó de extremidade de Gerenciamento de Identidade e Acesso.

Um terminal de Gerenciamento de Identidade e Acesso é um produto que coleta e gerencia as identidades do usuário eletrônico, associações de grupo e permissões de acesso. Esses terminais são chamados origens de informações do usuário.

Utilize os utilitários a seguir para configurar e gerenciar origens de informações do usuário :

- **Tivoli Directory Integrator**– É necessário instalar e configurar um Tivoli Directory Integrator em um não-QRadar do host.
- **UISConfigUtil.sh** – Utilize este utilitário para criar, recuperar, atualizar ou excluir origens de informações do usuário. Você pode utilizar origens de informações do usuário para integrar QRadar SIEM utilizando um Tivoli Directory Integrator remoto.
- **GetUserInfo.sh** – Use esse utilitário para coletar informações do usuário a partir de uma fonte de informações sobre o usuário e armazenar as informações em uma coleta de dados de referência. Você pode utilizar este utilitário para coletar informações do usuário on demand ou em um planejamento.

Fontes de informações do usuário

Uma fonte de informações sobre o usuário é um componente configurável que permite a comunicação com um nó de extremidade para recuperar as informações sobre o usuário e o grupo.

QRadarO sistema suporta as seguintes origens de informações do usuário :

Tabela 17. origens de informações suportadas.

Origem das Informações	Informações que são coletadas
Microsoft Windows Active Directory (AD) versão 2008 - Microsoft Windows AD é um serviço de diretório que autentica e autoriza todos os usuários e computadores que usam sua rede Windows.	• nome_completo • nome_usuário • nome_usuário_principal • nome_da_familia • nome_informado • Conta_desativada • Conta_bloqueada • Senha_expirada • Senha_não_pode_ser_aterada • Senha_não_expirada • Senha_não_expira
IBM Security Access Manager (ISAM), version 7.0 – ISAM é uma solução a autenticação e a autorização para Web corporativa, cliente / servidor, e aplicativos existentes. Para obter informações adicionais, consulte o IBM Security Access Manager (ISAM) a documentação do.	• Nome_no_rgy • Nome • Sobrenome • Conta_válida • Senha_válida
IBM Segurança Identity Manager (ISIM), version 6.0 – ISIM fornece o software e os serviços para a implementação de soluções de fornecimento baseado em. Este produto automatiza o processo de provisionamento de funcionários, contratados e parceiros de negócios com direitos de acesso IBM para os aplicativos que necessitam, seja em um ambiente corporativo fechado ou em toda uma empresa virtual ou estendida. Para obter informações adicionais, consulte a documentação do IBM Security Integration Manager (ISIM).	• Nome completo • DN

Coletas de dados de referência para obter informações do usuário

Este tópico fornece informações sobre como as coletas de dados de referência armazenam dados coletados a partir de origens de informações do usuário.

Quando QRadar SIEM a coleta de informações de um usuário de uma fonte de informações, ele automaticamente cria uma coleção de dados de referências para armazenar informações. O nome da coleção de dados de referência é derivado do nome do grupo de fonte de informações sobre o usuário. Por exemplo, uma coleção de dados de referência que é coletada a partir da Microsoft Windows AD pode ser chamada Admins do Domínio.

O tipo de coleta de dados de referência é um Mapa de Mapas. Em um Mapa de Referência de Mapas, os dados são armazenados em registros que mapear uma tecla para outra chave, que é, então, mapeado para um valor único.

Por exemplo:

- #

- Domain Admins
- # key1,key2,
- smith_j, Nome Completo,John Smith
- smith_j,account_is_disabled,0
- smith_j,account_is_locked
- smith_j,password_does_not_expire,1

Para obter informações adicionais sobre as coletas de dados de referência, consulte o *Nota Técnica Coletas de Dados de Referência*.

Exemplo de integração de fluxo de trabalho

Depois que as informações de usuário e grupo são coletadas e armazenadas em uma coleção de dados de referência, há muitas maneiras em que você pode utilizar os dados IBM Security QRadar SIEM.

É possível criar relatórios significativos e alertas que caracterizam usuário aderência a políticas de segurança de sua empresa.

Considere o exemplo a seguir:

garantir que as atividades que são executadas por usuários, ISIM privilegiado de acordo com suas políticas de segurança, você pode concluir as seguintes tarefas:

Criar uma origem de log para coletar e analisar dados de auditoria para cada servidor ISIM a partir do qual os logs são coletados. Para obter informações adicionais sobre como criar uma origem de log, consulte o *Guia de gerenciamento de origens de log*.

1. Criar uma origem de informações do usuário para o servidor de ISIM e coletar ISIM de informações do grupo de Administradores do usuário. Esta etapa cria uma coleta de dados de referência que é chamada Administradores ISIM. Consulte o "Criando uma Fonte de Informações Sobre o Usuário" na página 60.
2. Configure um bloco de construção para testar acontecimentos na qual a fonte de Endereço IP é o servidor ISIM e o nome do usuário é listado na ISIM coleta de dados de referência de administrador. Para obter informações adicionais sobre blocos de construção, consulte o *Guia do Usuário* para seu produto.
3. Criar uma procura de evento que utiliza o bloco de construção customizado como um filtro. Para obter informações adicionais sobre pesquisas de eventos, consulte o *Guia do Usuário* para seu produto.
4. Crie um relatório customizado que utiliza a procura de evento customizado para gerar relatórios diários sobre a atividade de auditoria dos usuários ISIM privilegiado. Esses relatórios indicam se qualquer atividade de administrador ISMI viola sua política de segurança. Para mais informações sobre relatórios, consulte o *Guia de Usuário* de seu produto.

Nota: Se quiser coletar logs de segurança do aplicativo, você deve criar um Módulo de Suporte de Dispositivo (DSM). Para obter informações adicionais, consulte *IBM Security QRadar DSM Configuration Guide*.

Visão geral das configurações de Fonte de informações de usuário e tarefas de gerenciamento

Para inicialmente integrar origens de informações do usuário, você deve executar as seguintes tarefas:

1. Configure um Tivoli Directory Integrator remoto. Consulte o "Configurando o Tivoli Directory Integrator Server".
2. Criar e gerenciar origens de informações do usuário. Consulte o "Criando e gerenciando fonte de informações sobre o usuário" na página 60.
3. Coletar informações do usuário. Consulte o "Coletando informações do usuário" na página 63.

Configurando o Tivoli Directory Integrator Server

Para o QRadar SIEM integrar-se com as fontes de informações sobre o usuário, você deve instalar e configurar um Tivoli Directory Integrator em um host não QRadar.

Sobre Esta Tarefa

Nenhuma configuração é necessária em seu sistema; no entanto, você deve acessar seu Console para obter o arquivo `QRadarIAM_TDI.zip`. Em seguida, instale e configure um servidor Tivoli Directory Integrator em um host separado. Se necessário, você também deve criar e importar um certificado autoassinado.

Quando você extrai o arquivo `QRadarIAM_TDI.zip` no servidor Tivoli Directory Integrator, o diretório TDI é criado automaticamente. O diretório TDI inclui os seguintes arquivos:

- QradarIAM.sh, que é o script de inicialização do TDI para Linux
- QradarIAM.bat, que é o script de inicializar do TDI para Microsoft Windows
- QradarIAM.xml, que é o script xml do TDI e deve ser armazenado no mesmo local que o arquivo QradarIAM.properties
- QradarIAM.properties, que é o arquivo de propriedades para o script xml do TDI

Quando você instala o Tivoli Directory Integrator, você deve configurar um nome para o diretório Solutions. Esta tarefa requer que você acesse o diretório Solutions. Portanto, nas etapas da tarefa, `<solution_directory>` refere-se ao nome que você forneceu ao diretório.

Os seguintes parâmetros são utilizados para criar e importar certificados:

Tabela 18. Parâmetros de Configuração de Certificação

Parâmetro	Descrição
<server_ip_address>	Define o endereço IP do servidor Tivoli Directory Integrator.
<days_valid>	Define o número de dias em que o certificado é válido.
<keystore_file>	Define o nome do arquivo keystore.
-storepass <senha>	Define a senha para o keystore.
- keypass <senha>	Define a senha para o par de chaves pública/privada.
<alias>	Define o alias para um certificado exportado.
<certificate_file>	Define o nome do arquivo do certificado.

Procedimento

1. Instale o Tivoli Directory Integrator em um host não QRadar. Para obter informações adicionais sobre como instalar e configurar o Tivoli Directory Integrator, consulte sua documentação do Tivoli Directory Integrator (TDI).
2. Utilizando o SSH, efetue login em seu Console como o usuário raiz.
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`
3. Copie o arquivo `QRadarIAM_TDI.zip` no servidor Tivoli Directory Integrator.
4. No servidor Tivoli Directory Integrator, extraia o arquivo `QRadarIAM_TDI.zip` no diretório Solutions.
5. Configure seu servidor Tivoli Directory Integrator para integração com o QRadar.
   a. Abra o arquivo `<solution_directory>/solution.properties` do Tivoli Directory Integrator.
   b. Remova o comentário da propriedade com.ibm.di.server.autoload. Se esta propriedade já estiver com o comentário removido, anote o valor da propriedade.
   c. Escolha uma das seguintes opções:
      - Altere os diretórios para o diretório autoload.tdi, que contém a propriedade com.ibm.di.server.autoload por padrão.
      - Crie um diretório autoload.tdi no <solution_directory> para armazenar a propriedade com.ibm.di.server.autoload.
   d. Mova os arquivos TDI/QRadarIAM.xml e TDI/QRadarIAM.property do diretório do Tivoli Directory Integrator para o diretório <solution_directory>/autoload.tdi ou o diretório que você criou na etapa anterior.
   e. Mova os scripts `QradarIAM.bat` e `QradarIAM.sh` do diretório do Tivoli Directory Integrator para o local a partir do qual você deseja iniciar o Tivoli Directory Integrator.
6. Se a autenticação baseada em certificado for necessária para seu sistema autenticar no Tivoli Directory Integrator, selecione uma das seguintes opções:
   - Para criar e importar um certificado autoassinado, consulte a Etapa 7.
   - Para importar um certificado de CA, consulte a Etapa 8.
7. Crie e importe o certificado autoassinado no armazenamento confiável do Tivoli Directory Integrator.
   a. Para gerar um keystore e um par de chaves pública/privada, digite o seguinte comando:
      - `keytool -genkey -dname cn=<server_ip_address> -validity <days_valid> -keystore <keystore_file> -storepass <password> -keypass <password>`
      - Por exemplo, `keytool -genkey -dname cn=192.168.1.1 -validity 365 -keystore server.jks -storepass secret -keypass secret`
   b. Para exportar o certificado a partir do keystore, digite o seguinte comando:
      - `keytool -export -alias <alias> -file <certificate_file> -keystore <keystore_file> - storepass <password>`
      - Por exemplo, `keytool -export -alias mykey -file server.cert -keystore server.jks -storepass secret`
   c. Para importar o certificado primário de volta para o keystore como o certificado de CA autoassinado, digite o seguinte comando:

- `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>.`
- Por exemplo, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`

d. Copie o arquivo do certificado para `/opt/qradar/conf/trusted_certificates` no QRadar SIEM Console.

8. Importe o certificado da CA no armazenamento confiável do Tivoli Directory Integrator.
   a. Para importar o certificado da CA no keystore como o certificado da CA autoassinado, digite o seguinte comando:
      - `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>.`
      - Por exemplo, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`
   b. Copie o arquivo de certificado da CA para `/opt/qradar/conf/trusted_certificates` no QRadar SIEM Console.
9. Edite o arquivo <solution_directory>/solution.properties para remover o comentário e configure as seguintes propriedades:
   - javax.net.ssl.trustStore=<keystore_file>
   - {protect}-javax.net.ssl.trustStorePassword=<password>
   - javax.net.ssl.keyStore=<keystore_file>
   - {protect}-javax.net.ssl.keyStorePassword=<password>

   Nota: A senha não modificada do padrão atual poderá ser exibida no seguinte formato: {encr}EyHbak. Insira a senha como texto simples. A senha é criptografada na primeira vez que você inicia o Tivoli Directory Integrator.
10. Use um dos scripts a seguir para iniciar o Tivoli Directory Integrator:
    - QradarIAM.sh para Linux
    - QradarIAM.bat para Microsoft Windows

Criando e gerenciando fonte de informações sobre o usuário

Use o utilitário UISConfigUtil para criar, recuperar, atualizar ou excluir fontes de informações sobre o usuário.

Criando uma Fonte de Informações Sobre o Usuário

Use o utilitário UISConfigUtil para criar uma fonte de informações sobre o usuário.

Antes de Iniciar

Antes de criar uma fonte de informações sobre o usuário, você deve instalar e configurar o servidor Tivoli Directory Integrator. Para obter informações adicionais, consulte "Configurando o Tivoli Directory Integrator Server" na página 58.

Sobre Esta Tarefa

Ao criar uma fonte de informações sobre o usuário, você deve identificar os valores de propriedade necessários para configurar a origem de informações sobre o usuário. A tabela a seguir descreve os valores da propriedade suportados:

Tabela 19. Valores de Propriedade da Interface com o Usuário Suportados

Propriedade	Descrição
tdiserver	Define o nome do host do servidor Tivoli Directory Integrator.
tdiport	Define a porta de atendimento para o conector HTTP no servidor Tivoli Directory Integrator.
hostname	Define o nome do host de fonte de informações sobre o usuário.
port	Define a porta de atendimento para o registro de Gerenciamento de Identidade e Acesso no host de informações sobre o usuário.
username	Define o nome de usuário que o QRadar SIEM usa para autenticar-se no registro de Gerenciamento de Identidade e Acesso.
password	Define a senha que é necessária para a autenticação no registro de Gerenciamento de Identidade e Acesso.
searchbase	Define o DN base.
search filter	Define o filtro de procura que é necessário para filtrar as informações do usuário que são recuperadas do registro de Gerenciamento de Identidade e Acesso.

Procedimento

1. Utilizando o SSH, efetue login em seu Console como o usuário raiz.
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`
2. Para incluir uma fonte de informações sobre o usuário, digite o comando a seguir: `UISConfigUtil.sh add <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2...,propn=valuen]`

   Em que:

   - `<name>` É o nome da fonte de informações sobre o usuário que você deseja incluir.
   - `<AD|ISAM|ISIM|ISFIM>` Indica o tipo de fonte de informações sobre o usuário.
   - `[-d description]` É uma descrição da fonte de informações sobre o usuário. Esse parâmetro é opcional.
   - `[-p prop1=value1,prop2=value2,...,propn=valuen]` Identifica os valores de propriedade necessários para a fonte de informações sobre o usuário. Para obter informações adicionais sobre os parâmetros suportados, consulte "Criando uma Fonte de Informações Sobre o Usuário" na página 60.

   Por exemplo:

   -
```
/UISConfigUtil.sh add "UIS_ISIM" -t ISIM -d "UIS for ISIM" -p
"tdiserver=nc9053113023.tivlab.austin.ibm.com,tdiport=8080,
hostname=vmibm7094.ottawa.ibm.com,port=389,
username=cn=root,password=password,\"searchbase=ou=org,DC=COM\",\
"searchfilter=(|(objectClass=erPersonItem)(objectClass=erBPPersonItem)
(objectClass=erSystemUser))\""
```

Recuperando Fontes de Informações do Usuário

Use o utilitário UISConfigUtil para recuperar fontes de informações sobre o usuário.

Procedimento

1. Utilizando o SSH, efetue login em seu Console como o usuário raiz.
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`
2. Escolha uma das seguintes opções:
   a. Digite o seguinte comando para recuperar todas as fontes de informações do usuário: `UISConfigUtil.sh get <name>`
   b. Digite o seguinte comando para recuperar uma fonte de informações sobre o usuário específica: `UISConfigUtil.sh get <name>`

      Em que `<name>` é o nome da fonte de informações sobre o usuário que você deseja recuperar.

      Por exemplo:

      ```
      [root@vmibm7089 bin]#.UISConfigUtil.sh get "UIS_AD"
      ```

Editando uma Origem de Informações sobre o Usuário

Use o utilitário UISConfigUtil para editar uma fonte de informações sobre o usuário.

Procedimento

1. Utilizando o SSH, efetue login em seu Console como o usuário raiz.
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`
2. Digite o comando a seguir para editar uma fonte de informações sobre o usuário: `UISConfigUtil.sh update <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2,...,propn=valuen]`

   Em que:

   - `<name>` É o nome da fonte de informações sobre o usuário que você deseja editar.
   - `<AD|ISAM|ISIM|ISFIM>` Indica o tipo de fonte de informações sobre o usuário. Para atualizar esse parâmetro, insira um novo valor.
   - `[-d description]` É uma descrição da fonte de informações sobre o usuário. Esse parâmetro é opcional. Para atualizar esse parâmetro, digite uma nova descrição.
   - `[-p prop1=value1,prop2=value2,...,propn=valuen]` Identifica os valores de propriedade necessários para a fonte de informações sobre o usuário. Para atualizar esse parâmetro, digite `novas propriedades`. Para obter informações adicionais sobre os parâmetros suportados, consulte “Criando uma Fonte de Informações Sobre o Usuário” na página 60.

   Por exemplo:

   ```
   ./UISConfigUtil.sh update "UIS_AD_update" -t AD -d "UIS for AD" -p
   "searchbase=DC=local"
   ```

Excluindo uma Fonte de Informações sobre o Usuário

Use o utilitário UISConfigUtil para excluir uma fonte de informações sobre o usuário.

Procedimento

1. Utilizando o SSH, efetue login em seu Console como o usuário raiz.
   a. Nome de usuário: `raiz`
   b. Senha: `<senha>`
2. Digite o seguinte comando para excluir uma fonte de informações sobre o usuário:

   ```
   UISConfigUtil.sh delete <name>
   ```

   Em que `<name>` é o nome da fonte de informações sobre o usuário que você deseja excluir.

O que Fazer Depois

As informações sobre o usuário coletadas são armazenadas em uma coleção de dados de referência no banco de dados do IBM Security QRadar SIEM. Se não existir nenhuma coleta de dados de referência, uma nova coleta de dados de referência será criada. Se uma coleção de dados de referência foi criada anteriormente para esta fonte de informações sobre o usuário, o mapa de referência será limpo de dados anteriores e as novas informações sobre o usuário serão armazenadas. Para obter informações adicionais sobre as coleções de dados de referência, consulte Coleções de Dados de Referência para obter informações sobre o usuário.

Coletando informações do usuário

Utilize as informações de usuários do utilitário GetUserInfo, de uma fonte de informações de usuário e armazenar os dados em uma coleção de dados de referência.

Sobre Esta Tarefa

Use essa tarefa para coletar informações de usuários on demand. se desejas criar informações de usuários automáticos em um planejamento, crie uma entrada de tarefa cron. create a cron job entry. Para obter informações adicionais sobre as tarefas cron, consulte a sua documentação Linux.

Procedimento

1. Utilizando o SSH, efetue login em seu Console como o usuário raiz.
   a. Nome de usuário: `raiz`
   b. `<senha>`
2. Digite o seguinte comando para coletar informações do usuário on demand:

   ```
   GetUserInfo.sh <UISName>
   ```

   Em que `<UISName>` é o nome da fonte de informações sobre o usuário que deseja coletar informações.

O que Fazer Depois

As informações do usuário coletados são armazenados em uma coleta de dados de referência no banco de dados. Se nenhuma coleção de dados de referência existir, uma nova coleção de dados de referência será criada. Se uma coleção de dados de referência foi criada anteriormente para esta fonte de informações sobre o usuário, o mapa de referência será limpo de dados anteriores e as novas informações sobre o usuário serão armazenadas. Para obter informações adicionais sobre as coletas de

dados de referência, consulte “Coletas de dados de referência para obter informações do usuário” na página 56.

Capítulo 6. Configurar QRadar

Use os recursos na guia **Admin** para configurar IBM Security QRadar SIEM

É possível configurar sua hierarquia de rede, as atualizações automáticas, configurações do sistema, depósitos de retenção de fluxos e eventos, notificações do sistema, configurações do console, motivos de fechamento de ofensa e gerenciamento de índices.

Hierarquia de Rede

QRadar utiliza a hierarquia de rede para entender o tráfego da rede e fornecer a você a capacidade de visualizar a atividade para toda a sua implementação.

Quando você desenvolve sua rede hierarquia, considere o método mais eficaz para visualizar atividade de rede. A hierarquia de rede não precisa ser parecida com a implementação física de sua rede. QRadar suporta qualquer hierarquia de rede que pode ser definidas por um intervalo de endereços IP. Você pode basear sua rede em muitas diferentes variáveis, inclusive geográficas ou unidades de negócios.

Ao definir sua rede hierarquia, você deve considerar os sistemas, usuários e servidores que podem ser agrupados.

Você pode agrupar sistemas e grupos de usuários que têm comportamento semelhante. No entanto, não do grupo de um servidor que possui comportamento exclusivo com outros servidores na sua rede. Colocando um servidor exclusivo único fornece a maior visibilidade no servidor QRadar, e você pode gerenciar políticas específicas.

Com um grupo, você pode locar servidores com alto volume de trafego, tais como emails, no topo do grupo. Esta hierarquia fornece a você uma representação visual quando uma discrepância ocorre.

Se seu processo de implementação processar mais de 600.000 fluxos de mensagens, é possível criar vários grupos de nível superior.

É possível organizar seus sistemas e redes por função ou os padrões de tráfego semelhantes. Por exemplo, servidores de correio, os usuários departamental, laboratórios, ou grupos de desenvolvimento. Utilizando esta organização, é possível diferenciar o comportamento da rede e reforçar as políticas de segurança de gerenciamento de rede.

Grandes grupos de rede podem causar dificuldades para você quando você visualizar informações detalhadas para cada objeto. Não configurar um grupo de rede com mais de 15 objetos.

Combinar vários Classless Inter-Domain Directas (CIDRs) ou sub-redes em um único grupo de rede para conservar o espaço em disco. Por exemplo:

Tabela 20. Exemplo de CIDRs múltiplos e sub-redes em um único grupo de rede

Grupo	Descrição	endereços IP
1	Marketing	10.10.5.0/24

Tabela 20. Exemplo de CIDRs múltiplos e sub-redes em um único grupo de rede (continuação)

Grupo	Descrição	endereços IP
2	Venda	10.10.8.0/21
3	Cluster do banco de dados	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32

Incluir servidores de chaves como objetos individuais e outros grandes, mas os servidores em objetos relacionados ao grupo multi-CIDR.

Defina um grupo global para que, quando novas redes forem definidas, as políticas apropriadas e monitores comportamentais sejam aplicados. Por exemplo:

Tabela 21. Exemplo de um grupo global

Grupo	Subgrupo	Endereço de IP
Cleveland	Diversos de Cleveland	10.10.0.0/16
Cleveland	Vendas de Cleveland	10.10.8.0/21
Cleveland	Marketing de Cleveland	10.10.1.0/24

Se você incluir uma rede para o exemplo, como 10.10.50.0/24 que é um departamento de RH, o tráfego é exibido como Cleveland-based e quaisquer regras que se aplicam ao grupo de Cleveland são aplicadas por padrão.

Valores CIDR aceitáveis

QRadaraceita valores CIDR específicos.

A tabela a seguir fornece uma lista dos valores CIDR que aceita: QRadar

Tabela 22. Valores CIDR aceitáveis

Comprimento CIDR	máscara	Número de Redes	Hosts
/1	128.0.0.0	128 A	2.147.483.392
/2	192.0.0.0	64 A	1.073.741.696
/3	224.0.0.0	32 A	536.870.848
/4	240.0.0.0	16 A	268.435.424
/5	248.0.0.0	8 A	134.217.712
/6	252.0.0.0	4 A	67.108.856
/7	254.0.0.0	2 A	33.554.428
/8	255.0.0.0	1 A	16.777.214
/9	255.128.0.0	128 B	8.388.352
/10	255.192.0.0	64 B	4.194.176
/11	255.224.0.0	32 B	2.097.088
/12	255.240.0.0	16 B	1.048.544
/13	255.248.0.0	8 B	524.272
/14	255.252.0.0	4 B	262.136

Tabela 22. Valores CIDR aceitáveis (continuação)

Comprimento CIDR	máscara	Número de Redes	Hosts
/15	255.254.0.0	2 B	131.068
/16	255.255.0.0	1 B	65.534
/17	255.255.128.0	128 C	32.512
/18	255.255.192.0	64 C	16.256
/19	255.255.224.0	32 C	8.128
/20	255.255.240.0	16 C	4.064
/21	255.255.248.0	8 C	2.032
/22	255.255.252.0	4 C	1.016
/23	255.255.254.0	2 C	508
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 sub-redes	124
/26	255.255.255.192	4 sub-redes	62
/27	255.255.255.224	sub-8	30
/28	255.255.255.240	sub-16	14
/29	255.255.255.248	sub-32	6
/30	255.255.255.252	sub-64	2
/31	255.255.255.254	nenhum	nenhum
/32	255.255.255.255	1/256 C	1

Por exemplo, uma rede é chamada de supernet quando o limite prefixo contém menos bits do que a máscara de rede natural (ou classful). Uma rede é chamada de uma sub-rede quando o prefixo limite contém mais bits que a máscara de rede natural:

- 209.60.128.0 é um endereço de rede classe C com uma máscara de /24.
- 209.60.128.0 /22 é uma supernet que lucra:
  - 209.60.128.0 /24
  - 209.60.129.0 /24
  - 209.60.130.0 /24
  - 209.60.131.0 /24
- 192.0.0.0 /25

  Intervalo do Host de sub-rede

  0 192.0.0.1-192.0.0.126

  1 192.0.0.129-192.0.0.254
- /26 192.0.0.0

  Intervalo do Host de sub-rede

  0 192.0.0.1 – 192.0.0.62

  1 192.0.0.65 – 192.0.0.126

  2 192.0.0.129 – 192.0.0.190

  3 192.0.0.193 – 192.0.0.254
- 192.0.0.0 /27

  Intervalo do Host de sub-rede

  0 192.0.0.1 – 192.0.0.30

1 192.0.0.33 - 192.0.0.62

2 192.0.0.65 – 192.0.0.94

3 192.0.0.97 – 192.0.0.126

4 192.0.0.129 – 192.0.0.158

5 192.0.0.161 – 192.0.0.190

6 192.0.0.193 – 192.0.0.222

7 192.0.0.225 – 192.0.0.254

Tarefas relacionadas:

"Definindo sua Hierarquia de Rede"
O QRadar considera todas as redes na hierarquia de rede como locais. Mantenha a hierarquia de rede atualizada para evitar falsas ofensas.

Definindo sua Hierarquia de Rede

O QRadar considera todas as redes na hierarquia de rede como locais. Mantenha a hierarquia de rede atualizada para evitar falsas ofensas.

Sobre Esta Tarefa

A relevância de uma ofensa, que é uma violação de segurança ou de conformidade, indica a importância de um destino. Áreas menos importantes da rede possuem menor relevância. O QRadar determina a relevância de uma ofensa conforme o peso das redes e ativos.

O peso de um objeto de rede é indicado por um valor numérico de 0 a 99, sendo 99 o maior e 0 o menor. Esse peso define a importância do objeto de rede em relação aos outros objetos de rede.

Os objetos de rede são contêineres de endereços CIDR. Qualquer endereço IP coberto por um intervalo CIDR na hierarquia de rede é considerado um endereço local. Qualquer endereço IP que não esteja definido em um intervalo de CIDR de objetos de rede é considerado um endereço IP remoto. Um CIDR pode pertencer a apenas um objeto de rede, no entanto, subconjuntos de um intervalo de CIDR podem pertencer a outro objeto de rede. O tráfego de rede corresponde ao CIDR mais exato. Um objeto de rede pode possuir intervalos de CIDR designados a ele.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Hierarquia de Rede**.
4. Na árvore de menus na janela Visualizações de rede, selecione a área da rede na qual você deseja trabalhar.
5. Para incluir objetos de rede, siga estas etapas:
   a. Clique em **Incluir** e digite um nome exclusivo e uma descrição do objeto.
   b. Na lista **Grupo**, selecione o grupo no qual você deseja incluir o novo objeto de rede.
   c. Para incluir um grupo, clique no ícone ao lado da lista **Grupo** e digite um nome para o grupo.
   d. Digite um intervalo de CIDR para o objeto e clique em **Incluir**.
   e. Clique em **Criar**.
   f. Repita as etapas para todos os objetos de rede.

6. Clique em **Editar** ou **Excluir** para trabalhar com objetos de rede existentes.

Conceitos relacionados:

"Valores CIDR aceitáveis" na página 66
QRadaraceita valores CIDR específicos.

Atualizações Automáticas

Você pode automaticamente ou manualmente atualizar os arquivos de configuração para assegurar que os arquivos de configuração contêm as mais recentes informações de segurança de rede.

QRadar utiliza arquivos de configuração do sistema para fornecer caracterizações útil de fluxos de dados de rede.

Requisitos de atualização automática

O Console deve estar conectado à Internet para receber as atualizações. Se o Console não está conectado à Internet, você deve configurar um servidor de atualização interno para o Console para fazer download dos arquivos a partir de.

arquivos de Atualização estão disponíveis para download manual a partir do seguinte Web site:

IBM Fix Central (http://www.ibm.com/support/fixcentral).

Para manter a integridade de sua configuração atual e informações, substituir seus arquivos de configuração existentes ou integrar os arquivos atualizados com seus arquivos existentes.

Depois de instalar atualizações em seu Console e implementar suas alterações, o Console atualiza seus hosts gerenciados se sua implementação for definida em seu editor de implementação. Para obter informações adicionais sobre o editor de implementação, consulte Capítulo 11, "Editor de implementação", na página 139.

Descrição das atualizações

Atualizar arquivos podem incluir as seguintes atualizações:

- Configuração de atualizações, as quais incluem as configurações de mudança de arquivo de vulnerabilidades, mapas QID, e atualizações sobre informações de segurança.
- Atualizações de DSM, que incluem correções para problemas de análise, alterações do scanner, e atualizações de protocolo.
- As atualizações, que incluem itens como arquivos JAR atualizados.
- atualizações menores, que incluem itens como obter scripts atualizados ou conteúdo da Ajuda On-line.

Frequência de atualizações automáticas para novas instalações e upgrades

A frequência padrão da atualização automática é determinado pelo tipo de instalação e versão do QRadar.

- Se você fizer upgrade do QRadar de versões anteriores à V7.2, o valor para o qual a frequência de atualização está configurada permanecerá o mesmo após o

upgrade. Por padrão, a atualização é configurada para semanalmente, mas é possível alterar manualmente a frequência.

- Se você fizer uma nova instalação do QRadar V7.2 ou posterior, a frequência padrão da atualização será diária. É possível alterar a frequência manualmente.

Conceitos relacionados:

"Configure uma atualização de servidor QRadar" na página 75

mIf your deployment includes a QRadar Console that is unable to access the Internet or you want to manually manage updates to your system, you can set up a QRadar update server to manage the update process.

Visualizando Atualizações Pendentes

Seu sistema é pré-configurado para atualizações automáticas semanais. É possível visualizar as atualizações pendentes na janela Atualizações.

Sobre Esta Tarefa

Seu sistema precisa estar operacional tempo suficiente para recuperar as atualizações semanais. Se não houver atualizações exibidas na janela Atualizações, o sistema não esteve em operação tempo suficiente para recuperar as atualizações semanais ou nenhuma atualização foi emitida. Se isso ocorrer, será possível verificar manualmente novas atualizações. Para obter informações adicionais sobre como verificar novas atualizações, consulte "Verificando novas atualizações" na página 73.

A barra de ferramentas**Verificar Atualizações** fornece as seguintes funções:

Tabela 23. Funções da Barra de Ferramentas Verificar Atualizações

Função	Descrição
Ocultar	Selecione uma ou mais atualizações e, em seguida, clique em **Ocultar** para remover as atualizações selecionadas a partir da página Verificar Atualizações. É possível visualizar e restaurar as atualizações ocultas na página Restaurar Atualizações Ocultas. Para obter informações adicionais, consulte "Restaurando Atualizações Ocultas" na página 74.
Instalar	É possível instalar manualmente as atualizações. Ao instalar atualizações manualmente, o processo de instalação é iniciado em um minuto. Para obter informações adicionais, consulte "Instalando Manualmente Atualizações Automáticas" na página 74.
Planejar	É possível configurar uma data e hora específicas para instalar manualmente as atualizações selecionadas em seu Console. O planejamento é útil quando você deseja planejar a instalação da atualização durante as horas de menor atividade. Para obter informações adicionais, consulte "Planejando uma Atualização" na página 72.

Tabela 23. Funções da Barra de Ferramentas Verificar Atualizações (continuação)

Função	Descrição
Remover do Planejamento	É possível remover planejamentos pré-configurados para instalar manualmente as atualizações em seu Console. Para obter informações adicionais, consulte "Planejando uma Atualização" na página 72.
Procurar por Nome	É possível localizar uma atualização específica pelo nome.
Próxima Atualização	Este contador exibe a quantidade de tempo até a próxima atualização automática. A lista de atualizações na página Verificar Atualizações é atualizada automaticamente a cada 60 segundos. O cronômetro é pausado automaticamente quando você seleciona uma ou mais atualizações.
Pausar	Pausa o processo de atualização automática. Para continuar a atualização automática, clique em **Reproduzir**.
Atualizar	Atualiza a lista de atualizações.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Atualização Automática**.
4. Para visualizar detalhes em uma atualização, selecione a atualização.

Configurando as configurações de atualização automática

É possível customizar as configurações de atualização automática para alterar a frequência, tipo de atualização, configuração do servidor e as configurações de backup.

Sobre Esta Tarefa

Você pode selecionar o **AutoDeploy** implementação automaticamente as atualizações. Se o **AutoDeploy** não for selecionado, então você deve implementar manualmente as alterações, na guia **Painel** , após as atualizações estiverem instaladas.

É possível selecionar **Reinicialização Automática do Serviço** para permitir atualizações automáticas que requerem a interface com o usuário para reiniciar. Uma interrupção na interface com o usuário ocorre quando o serviço é reiniciado. Como alternativa, você pode instalar manualmente o atualizado a partir de Verificar Atualizações janela.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Atualização Automática**.
4. No menu de navegação, clique em **Visualizar Settings**.
5. Na guia **Básica** , selecione o planejamento para atualizações.

6. Na seção **Atualizações de Configuração** , selecione o método que você deseja utilizar para atualizar os arquivos de configuração.
7. Na seção **Atualizações de DSM, Scanner, Protocolo**, selecione uma opção para instalar as atualizações.
8. Na seção **, Atualizações** , selecione uma opção para receber atualizações importantes para novos releases.
9. Na seção **atualizações menores** , selecione uma opção para receber as correções para problemas menores do sistema.
10. Selecione a caixa de opções **Implementar Automática** se quiser implementar alterações de atualização automaticamente após as atualizações estiverem instaladas.
11. Selecione a caixa de opções **Reinicialização Automática do Serviço** se você deseja reiniciar o serviço da interface com o usuário automaticamente após as atualizações estiverem instaladas.
12. Clique em **Avançadas**.
13. No campo **Servidor da Web**, digite o servidor da web a partir do qual você deseja obter as atualizações. O servidor da web padrão é https://qmmunity.q1labs.com/.
14. No **campo Diretório**, digite o local do diretório no qual o servidor da Web armazena as atualizações. O diretório padrão é `autoupdates/`.
15. Opcional: No campo **Servidor Proxy**, digite a URL para o servidor proxy. O servidor proxy é necessário se o servidor de aplicativos utiliza um servidor proxy para conexão com a Internet.
16. Opcional: No campo **Nome de Usuário do Proxy**, digite o nome de usuário para o servidor proxy. Um nome de usuário será necessário se você estiver utilizando um proxy autenticado.
17. No campo **Senha de Proxy**, digite a senha para o servidor proxy. Uma senha é necessária se estiver usando um proxy autenticado.
18. Selecione a caixa de seleção **enviar Feedback** se quiser enviar feedback para a IBM sobre a atualização. Se ocorrerem erros durante uma atualização, o feedback é automaticamente enviado por um formulário da Web.
19. Na lista **Período de Retenção de Backup**, digite ou selecione o número de dias que você deseja armazenar arquivos que são substituídas durante o processo de atualização. Os arquivos são armazenados no local que está especificado no **Local de Backup**. O mínimo é um dia, e o máximo é 65535 anos.
20. No campo **Local de Backup** , digite o local no qual você deseja armazenar os arquivos de backup.
21. No campo **Caminho de Download** , digite o local do caminho do diretório no qual você deseja armazenar DSM, secundários e atualizações importantes. O caminho do diretório padrão é `/store/configservices/staging/updates`.
22. Clique em **Salvar**.

Planejando uma Atualização

Atualizações automáticas ocorrem em um planejamento recorrente de acordo com as configurações na página Configuração de Atualização. Você também pode planejar uma atualização ou um conjunto de atualizações para execução em um horário específico.

Sobre Esta Tarefa

Para reduzir os impactos no desempenho em seu sistema, planeje uma atualização grande para executar durante as horas de menor atividade.

Para obter informações detalhadas sobre cada atualização, você pode selecionar a atualização. Uma descrição e quaisquer mensagens de erro são exibidas na área de janela à direita da janela.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Atualização Automática**.
4. Opcional: Se você deseja planejar atualizações específicas, selecione as atualizações que deseja planejar.
5. Na caixa de listagem **Planejar**, selecione o tipo de atualização que deseja planejar.
6. Usando o calendário, selecione a data e hora de início de quando você deseja iniciar seu atualizações planejadas.

Limpando as atualizações agendadas

É possível cancelar qualquer atualização agendada.

Sobre Esta Tarefa

Atualizações agendadas exibem o status **Planejado** no **campo Status**. Após o planejamento ser limpo, o status de atualizações é exibido como **Novo**.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Atualização Automática**.
4. No menu de navegação, clique em **Verificar Atualizações**.
5. Opcional: Se for necessário limpar atualizações específicas agendadas, selecione as atualizações que você deseja limpar.
6. Na caixa de listagem **Não agendada** selecione o tipo de agendamento de atualizaçãoque deseja limpar.

Verificando novas atualizações

IBMfornece atualizações em uma base regular. Por padrão, o recurso atualização automática é agendado para baixar e instalar atualizações automáticas. Se necessário uma atualização em um momento diferente do pré-configurado no planejamento, é possível fazer download de novas atualizações.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Atualização Automática**.
4. No menu de navegação, clique em **Verificar Atualizações**.
5. Clique em **Obter Novas Atualizações**.

Instalando Manualmente Atualizações Automáticas

O IBM fornece atualizações regularmente. Por padrão, atualizações são transferidas por download e instaladas automaticamente em seu sistema. No entanto, você pode instalar uma atualização em um momento diferente do planejamento pré-configurado.

Sobre Esta Tarefa

O sistema recupera as novas atualizações a partir do Fix Central. Isso pode demorar um longo período de tempo. Ao concluir, novas atualizações serão listadas na janela Atualizações.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Atualização Automática**.
4. No menu de navegação, clique em **Verificar Atualizações**.
5. Opcional: Se você deseja instalar atualizações específicas, selecione as atualizações que deseja planejar.
6. Na caixa de listagem **Instalar**, selecione o tipo de atualização que você deseja instalar.

Visualizando seu Histórico de Atualizações

Após uma atualização ser instalada com êxito ou ter falhado na instalação, a atualização é exibida na página Visualizar Histórico de Atualizações.

Sobre Esta Tarefa

Uma descrição da atualização e quaisquer mensagens de erro de instalação são exibidas na área de janela direita da página Visualizar Histórico de Atualizações. A página Visualizar Histórico de Atualizações fornece as seguintes informações:

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Atualização Automática**.
4. No menu de navegação, clique em **Visualizar Histórico de Atualizações**.
5. Opcional: Utilizando a caixa de texto **Procurar por Nome**, você pode digitar uma palavra-chave e, em seguida, pressionar Enter para localizar uma atualização específica pelo nome.
6. Para investigar uma atualização específica, selecione a atualização.

Restaurando Atualizações Ocultas

É possível remover atualizações da página Verificar Atualizações. É possível visualizar e restaurar as atualizações ocultas na página Restaurar Atualizações Ocultas.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Atualização Automática**.

4. No menu de navegação, clique em **Restaurar Atualizações Ocultas**.
5. Opcional: Para localizar uma atualização por nome, digite uma palavra-chave na caixa de texto **Procurar por Nome** e pressione Enter.
6. Selecione a atualização oculta que você deseja restaurar.
7. Clique em **Restaurar**.

Visualizando o Log de Atualização Automática

O log de atualização automática contém a atualização automática mais recente que foi executada em seu sistema.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Atualização Automática**.
4. No menu de navegação, clique em **Visualizar Log**.

Configure uma atualização de servidor QRadar

mIf your deployment includes a QRadar Console that is unable to access the Internet or you want to manually manage updates to your system, you can set up a QRadar update server to manage the update process.

O pacote de atualizações automáticas inclui todos os arquivos necesários para configurar manualmente um servidor de atualização e também os arquivos de configurações necessários para cada atualização. Após a connfiguração inicial, é necessário apenas fazer o download e descompactar os pacotes de atualizações mais atuais para atualizar manualmente a sua configuração.

É possível assinar as notificações em Fix Central para receber notificações de novas atualizações.

Conceitos relacionados:

"Atualizações Automáticas" na página 69
Você pode automaticamente ou manualmente atualizar os arquivos de configuração para assegurar que os arquivos de configuração contêm as mais recentes informações de segurança de rede.

Configurando seu Servidor de Atualização

Utilize esta tarefa para configurar um servidor Apache. Você deve criar um diretório de atualização e fazer download do pacote de atualização automática a partir do Fix Central.

Sobre Esta Tarefa

As atualizações automáticas estão disponíveis no Fix Central.

Procedimento

1. Acesse seu servidor Apache. Por padrão, o diretório de atualização está no diretório raiz da web do servidor Apache. É possível colocar o diretório em outro local se você configurar o QRadar apropriadamente.
2. Crie um diretório de atualização denominado `autoupdates/`.
3. Opcional: Crie uma conta de usuário e senha do Apache a serem utilizados pelo processo de atualização.

4. Faça download do pacote atualização automática a partir do Fix Central: http://www.ibm.com/support/fixcentral É possível encontrar produtos QRadar na lista Security Systems **Grupo de Produtos** no Fix Central.
5. Salve o arquivo do pacote de atualização automática em seu servidor Apache no diretório `autoupdates/` que você criou.
6. No servidor Apache, digite o seguinte comando para descompactar o pacote de atualização automática. **`tar -zxf updatepackage-[timestamp].tgz`**
7. Clique na guia **Admin**.
8. No menu de navegação, clique em **Configuração do sistema**.
9. Clique em **Atualização Automática**.
10. Clique em **Alterar Configurações**.
11. Selecione a **guia Avançado**.
12. Para direcionar o processo de atualização para o servidor Apache, configure os seguintes parâmetros no painel **Configuração do Servidor**:
    a. No campo **Servidor da Web**, digite o o endereço ou caminho do diretório de seu servidor Apache. Se o servidor Apache for executado em portas não padrão, inclua `:<portnumber>` no final do endereço. `https://qmmunity.q1labs.com/:8080`
    b. No **campo Diretório**, digite o local do diretório no qual o servidor da Web armazena as atualizações. O diretório padrão é `autoupdates/`.
    c. Opcional: No campo **Servidor Proxy**, digite a URL para o servidor proxy. O servidor proxy é necessário se o servidor de aplicativos utiliza um servidor proxy para conexão com a Internet.
    d. Opcional: No campo **Nome de Usuário do Proxy**, digite o nome de usuário para o servidor proxy. Um nome de usuário será necessário se você estiver utilizando um proxy autenticado.
    e. Opcional: No campo **Senha de Proxy**, digite a senha para o servidor proxy. Uma senha é necessária se estiver usando um proxy autenticado.
13. Selecione **Implementar Mudanças**.
14. Clique em **Salvar**.
15. Utilizando o SSH, efetue login no QRadar como o usuário raiz.
16. Digite o seguinte comando para configurar o nome de usuário que você configura para o servidor Apache: **`/opt/qradar/bin/UpdateConfs.pl -change_username <username>`**
17. Digite o seguinte comando para configurar a senha que você configura para o servidor Apache: **`/opt/qradar/bin/UpdateConfs.pl -change_password <password>`**
18. Teste seu servidor de atualização digitando o comando:**`lynx https://<your update server>/<directory path to updates>/manifest_list`**
19. Digite o nome do usuário e a senha.

Configurando o seu QRadarConsole como servidor de atualização.

Você pode configurar o Console para ser seu servidor de atualização QRadar.

Sobre Esta Tarefa

Para configurar seu console QRadar para ser seu servidor de atualização, conclua três tarefas:

- Crie um diretório de atualização automática.

- Faça download do pacote atualização automática a partir do Fix Central.
- Configure o QRadar para aceitar o autoupdates.

Procedimento

1. Efetue login no QRadar como o usuário raíz.
2. Digite o seguinte comando para criar o diretório autoupdate : **mkdir /opt/qradar/www/autoupdates/**
3. Faça download do pacote atualização automática a partir do Fix Central: http://www.ibm.com/support/fixcentral É possível encontrar produtos QRadar na lista Security Systems **Grupo de Produtos** no Fix Central.
4. Salve o arquivo do pacote de atualização automática em seu servidor Apache no diretório `autoupdates/` que você criou.
5. em seu console QRadar, digite o seguinte comando para descompactar o pacote autoupdate.**tar -zxf updatepackage-[timestamp].tgz**
6. Efetue log in na interface do usuário QRadar.
7. No menu de navegação, clique em **Configuração do sistema**.
8. Clique em **Atualização Automática**.
9. Clique em **Alterar Configurações**.
10. Selecione a **guia Avançado**.
11. No campo **Servidor da Web**, digite `https://localhost/`.
12. Limpe a caixa de opções **Enviar Alimentação**.

Adicionando novas atualizações

É possível fazer download das atualizações do Fix Central para seu servidor de atualização.

Antes de Iniciar

Você deve configurar seu servidor de atualização e configuração QRadar para receber atualizações do servidor de atualização.

Procedimento

1. Faça download do pacote atualização automática a partir do Fix Central: http://www.ibm.com/support/fixcentral É possível encontrar produtos QRadar na lista Security Systems **Grupo de Produtos** no Fix Central.
2. Salve o arquivo autoupdate no pacote de atualização do servidor no diretório `autoupdates/` que você criou.
3. Digite o comando a seguir para descompactar o pacote de atualização automática: **tar -zxf autoupdate-[timestamp].tgz**.
4. Efetue login no QRadar como o usuário raíz.
5. Digite o seguinte comando para testar sua atualização do servidor, **lynx https://<your update server>/<directory path to updates>/manifest_list**.
6. Digite o nome do usuário e a senha de sua atualização do servidor.

Configurando as definições de sistema

É possível configurar as definições do sistema.

Sobre Esta Tarefa

Na janela Configurações do Sistema, você pode configurar os seguintes parâmetros:

Tabela 24. janela parâmetros de Configurações do Sistema

Parâmetro	Descrição
Configurações do Sistema	
Endereço de e-mail administrativo	O endereço de e-mail do administrador de sistema designado. O endereço de e-mail padrão é root@localhost.
Alerta de emaail do endereço	O endereço de e-mail a partir do qual você deseja receber alertas de e-mail. Este endereço é exibido no campo **De** dos alertas de e-mail. Um endereço válido é requerido pela maioria dos servidores de e-mail. O endereço de e-mail padrão é root@<hostname.domain>.
Código do idioma do email	O código de idioma a ser usado para preferências de idioma e mensagens de email de alerta do sistema, incluindo os emails que são acionados em resposta a uma regra. A configuração padrão é inglês.
Resolução de duração do intervalo	A resolução de duração do intervalo determina o intervalo QRadar QFlow Collector e enviar aos coletores de eventos, pacotes de informações para o console. Se a opção de 30 segundos for selecionada, os resultados exibidos na QRadar interface de usuário como dados inseridos no sistema. No entanto, com intervalos mais curtos, o volume de dados série temporal é maior e o sistema pode experimentar atrasos no processamento das informações.
Excluir correio raíz	O email raíz é a loacalização padrão para mensagens de contexto de host.
Período de retenção de arquivos temporários	O período que você deseja que o sistema retenha arquivos temporários. O armazenamento padrão para arquivos temporários é o diretório `/store/tmp`.
Período de consulta de perfil ativo	O período para uma procura de ativo, para processar antes que ocorra um tempo limite.
Unindo eventos	As configurações de log para unir eventos. Selecione em **Sim** para ativar as fontes de log para unir, ou pacote configurável, ou eventos. Essa configuração se aplica a todas as novas fontes de log que você incluir. Para fontes de log que você incluiu anteriormente ou para alterar uma origem de log individual, você deve editar o parâmetro **Unindo Eventos** na configuração da origem de log.
Armazenamento de carga útil do evento	Fontes de log podem armazenar informações de carga útil do evento. Este valor se aplica a todas as fontes de log. No entanto, se você desejar alterar esse valor para uma origem de log específica, edite o parâmetro **Evento de carga útil** na configuração da origem de log. Para obter informações adicionais, consulte o *Guia de gerenciamento de origens de log*Guia de Usuários.
Acesso Global Iptables	Os endereços IP de sistemas não-Console que não possuem configuração iptables para a qual você deseja ativar o acesso direto. Para inserir múltiplos sistemas, digite uma vírgula para separar as listas de endereços IP.
Eventos de tempo limite Syslog (minutos)	A quantidade de tempo que o status de um dispositivo do syslog será registrado como um erro se nenhum evento for recebido dentro do período de tempo limite. O status é exibido na janela Fontes de Log.
Partição do testador limite (segundos)	A quantidade de tempo para um teste de partição para executar antes de ocorrer um tempo limite.
Número Máximo de Conexões TCP Syslog	O número máximo de conexões Transmission Control Protocol (TCP) syslog que você deseja permitir que seu sistema.
Diretório de Exportação	O local onde as exportações ofensas, evento e fluxo são armazenados. O local padrão é `/store/exports`.
Exibir País/Região Sinalizadores	Se informações geográficas estão disponíveis para um endereço IP, o país ou região está visualmente indicado por um sinalizador. É possível selecionar **Não** a partir desta caixa de listagem desativar esse recurso.
Configurações do Banco de Dados	
Arquivos de Dados do Usuário	O local onde as exportações do fluxo de eventos estão armazenados. O local padrão é `/store/users`.
Retenção de Acumulador minuto à minuto	O acumulações que você deseja reter os dados do período minuto a minuto. A cada 60 segundos, os dados são agregados em um único conjunto de dados.
Retenção de Acumulador de hora	O período que você deseja reter a acumulação de dados por hora. Ao final de cada hora, o minuto-conjuntos de dados por minuto são agregados em um único conjunto de dados por hora.
Retenção de Acumulador - Diário	O período que você deseja reter a acumulação de dados diários. Ao final de cada dia, os conjuntos de dados por hora são agregados em um único conjunto de dados diários.
Índice Retenção da carga útil.	A quantidade de tempo que você deseja armazenar índices de carga útil.

Tabela 24. janela parâmetros de Configurações do Sistema (continuação)

Parâmetro	Descrição
Violação do período de retenção	O período que você deseja reter as informações sobre a violação fechada. A configuração padrão é de 30 dias. O mínimo é 1 dia e o máximo é 2 anos. Depois que o período de retenção transcorra ofensas, ofensas fechadas são limpas do banco de dados. Ofensas podem ser mantidas indefinidamente se elas não são fechadas ou inativas, e eles ainda estão recebendo eventos. O juiz automaticamente marca uma ofensa como Inativa se a ofensa não recebeu um evento para 5 dias. Esse período de peregrinação é conhecido como o tempo sem utilização. Se um evento for recebido durante o tempo de inatividade, o tempo de inatividade é reconfigurado de volta para zero. Quando uma infração é fechada por você (Fechada) ou por fuincionário público (Inactive), a **o período de infração de retenção** configurado é aplicado.
Período de Retenção do Histórico de atacante	Na caixa de listagem, selecione a quantia de tempo que você deseja armazenar o histórico do atacante.
Destino Período de Retenção	Na caixa de listagem, selecione a quantia de tempo que você deseja armazenar o histórico de destino.
Configurações do Banco de Ariel	
Fluxo de Dados de Armazenamento Local	O local em que você deseja armazenar as informações do log do fluxo. O local padrão é `/store/ariel/flows`.
Efetue Localização do Armazenamento de Origem	O local onde você deseja armazenar as informações de fonte de log. O local padrão é `/store/ariel/events`.
Resultados da Procura Período de Retenção	A quantidade de tempo que você deseja armazenar os resultados da procura.
Relatórios Correspondidos Resultados Máx.	O número máximo de resultados você deseja um relatório para retornar.
Command Line Correspondidos Resultados Máx.	O número máximo de resultados que você deseja a partir da linha de comandos AQL para retornar.
da Web Limite de Tempo de Execução	A quantidade máxima de tempo, em segundos, que você deseja que uma consulta para processar antes de ocorrer um tempo limite.
Relatórios Relatórios Manual Limite de Tempo de Execução	A quantidade máxima de tempo, em segundos, que você deseja que uma consulta de relatórios para processar antes de ocorrer um tempo limite.
Limite de Tempo de Execução da Linha de Comandos	A quantidade máxima de tempo, em segundos, que você deseja que uma consulta na linha de comandos AQL para processar antes de ocorrer um tempo limite.
Último Minuto Web (Automático atualização) Limite de Tempo de Execução	A quantidade máxima de tempo, em segundos, que você deseja que uma atualização automática para processar antes que ocorra um tempo limite.
Efetue Fluxo Hashing	Armazena um arquivo hash para cada arquivo de log fluxo armazenadas. Selecione em **Sim** para ativar o registro.
Log de evento Hashing	Armazena um arquivo hash para cada arquivo de log de eventos armazenados. Selecione em **Sim** para ativar o registro.
Criptografia HMAC	Este parâmetro só é exibido quando o **Log de Eventos de Hashing** ou sistema de configuração **Fluxo de Log de Hashing** configuração está ativada. Selecione **Sim** para permitir QRadar para criptografar a integridade hashes armazenados no evento e fluxo de arquivos de log.
HMAC Chave	A chave que você deseja utilizar para criptografia HMAC. A chave deve ser exclusiva.
Conferir	Este parâmetro só é exibido quando o **HMAC Encryption** sistema de configuração está ativada. Redigite a chave que deseja utilizar para criptografia HMAC. A chave deve corresponder a chave que você digitou no campo **chave HMAC** .

Tabela 24. janela parâmetros de Configurações do Sistema (continuação)

Parâmetro	Descrição
Algoritimo Hashing	Você pode utilizar um algoritmo hash para integridade de banco de dados. QRadar utiliza os seguintes tipos de algoritmo hash : • **Message-Digest Algorithm Hash** – Transformações assinaturas digitais em valores menores chamados de Mensagens-Compilações (MD). • **Assegure que o Algoritimo (SHA) Hash Algorithm** - padrão que cria algorítimos maiores que (60 bit) MD. Se o **HMAC Criptografia** parâmetro é desativado, as seguintes opções estão disponíveis: • **MD2** – Algorithm que é definido pelo RFC 1319. • **MD5** – Algorithm que é definido pelo RFC 1321. • **SHA-1** – Algorithm que é definido pelo SHS (Secure Hash Standard), NIST FIPS 180-1. Esta é a definição padrão. • **SHA-256** - Algorítimo que é definido pelo esboço básico Federal Information Processing Standard 180-2, SHS. SHA-256 é um algoritmo hash 255-bit que é planejado para 128 bits de segurança contra ataques de segurança. • **SHA-384** – Algoritimo que é definido pelo rascunho Federal Information Processing Standard 180-2, SHS. SHA-384 é um algoritmo hash de bits, criado por truncando a saída SHA-512. • **SHA-512** – Algoritimo que é definido pelo projecto Federal Information Processing Standard 180-2, SHS. SHA-512 é um algoritmo hash de bits que é destinado a fornecer 256 bits de segurança. Se o parâmetro**HMAC Encryption** é ativado, as seguintes opções estão disponíveis: • **HMAC-MD5 –** Um método de criptografia que se baseia no algoritmo hash MD5. • **HMAC-SHA-1** – Um método de criptografia que é baseado no algoritmo hash SHA-1. • **HMAC-SHA-256 –** Um método de criptografia que se baseia no algoritmo hash SHA-256. • **HMAC-SHA-384 –** Um método de criptografia que se baseia no algoritmo hash SHA-384. • **HMAC-SHA-512** Um método de criptografia que se baseia no algoritmo hash SHA-512.
Vigilante de Transação Configurações	
Tempo Limite Máximo da Transação	Uma transação sentinela detecta aplicativos respondendo utilizando a análise de transação. Se um aplicativo não-responsivo for detectado, o sentinela transação tentará retornar o aplicativo para um estado funcional. O período de tempo que você desejar que o sistema verifique se há problemas transacional no banco de dados.
Host Resolva Transação em Non-Encrypted	O Vigilante de transação pode resolver todas as condições de erro que são detectados no Console ou hosts não-gerenciado criptografado. Se for selecionado **Não**, as condições são detectadas e loggadas, mas você deve intervir manualmente e corrigir o erro.
Resolva Transação em Encrypted do Host	O Vigilante de transação pode resolver todas as condições de erro que são detectados no host gerenciado criptografado. Se for selecionado **Não**, as condições são detectadas e loggadas, mas você deve intervir manualmente e corrigir o erro.
Configurações SNMP	
Versão do SNMP	A versão do SNMP que você deseja utilizar. Desative esta configuração se você não desejar que respostas SNMP no QRadar customizada no mecanismo de regras.
Configurações SNMPv2c	
Host de Destino	O endereço IP para o qual você deseja enviar notificações de SNMP.
Porta de Destino	O número da porta para os quais deseja enviar as notificações SNMP.
Comunidade	A comunidade SNMP, como público.
Configurações SNMPv3	
Host de Destino	O endereço IP para o qual você deseja enviar notificações de SNMP.
Porta de Destino	A porta à qual você deseja enviar notificações de SNMP.
Nome de Usuário	O nome do usuário que você deseja acessar propriedades de SNMP relacionados.
Nível de Segurança	O nível de segurança para SNMP.
Protocolo de Autenticação	O algoritmo que você deseja utilizar para autenticar os traps SNMP.
Senha de Autenticação	A senha que você deseja utilizar para autenticar os traps SNMP.
Protocolo de Privacidade	O protocolo que você deseja utilizar para decriptografar SNMP.
Senha de Privacidade	A senha que é utilizada para decriptografar SNMP.
Configurações de SNMP Daemon integrados	
Ativado	Habilita acesso aos dados do agente SNMP, usando solicitações SNMP. Após ativar o SNMP daemon, você deve acessar o host que é especificado no parâmetro **Destination Host**, e digite `qradar` no campo **Username**. Uma senha não é requerida local localização onde você configurou um host de destino para comunicar-se com o QRadar SIEM pode variar dependendo do host fornecedor. Para mais informações sobre como configurar seu host de destino para comunicar-se com QRadar, consulte a documentação do fornecedor.

Tabela 24. janela parâmetros de Configurações do Sistema (continuação)

Parâmetro	Descrição
Porta do Daemon	A porta que você deseja utilizar para o envio de pedidos SNMP.
Cadeia de Comunidade	A comunidade SNMP, tal como **público.** Este parâmetro aplica-se apenas se você estiver utilizando SNMPv2 e SNMPv3.
Lista de Acesso de IP	Os sistemas que acessam dados do agente SNMP usando uma solicitação SNMP. Se a opção **Ativada** estiver configurada para sim, esta opção é forçada.
IF-MAP Cliente/Configurações de Servidor	
Versão IF-MAP	A versão do IF-MAP que você requer. A interface para ponto de acesso de Metadados (IF-MAP) regula a ativação de resposta IBM Security QRadar SIEMe para alerta de dados de ofensa derivados de eventos, fluxos e dados em um servidor IF-MAP. Se essa configuração estiver desabilitada, outras configurações de cliente/ ou servidor IF-MAP não forem exibidas.
Endereço do Servidor	O endereço IP do servidor IF-MAP.
Porta Básica do Servidor	O número da porta para o servidor básico IF-MAP.
Porta de servidor de Credencial	The port number for the credential server. .
Autenticação	O tipo de autenticação que você requer. Antes de poder configurar a autenticação IF-MAP, você deve configurar seu certificado do servidor MAP IF-.
Senha Chave	A senha chave a ser compartilhada entre o IF-cliente e servidor MAP. Esta configuração é exibida somente quando você seleciona a opção **Mútuo** para o **Autenticação** configuração.
Nome de Usuário	O nome do usuário que é necessário para acessar o servidor IF-MAP. Esta configuração é exibida somente quando você seleciona a opção **Básica** para a configuração **Autenticação**.
Senha de usuário	A senha que é necessária para acessar o servidor IF-MAP. Esta configuração é exibida somente quando você seleciona a opção **Básica** para a configuração **Autenticação**.
Configurações de Perfil de Ativo Esta área de janela é exibida somente se IBM Security QRadar Vulnerability Manager for instalada em seu sistema.	
Período de Retenção de Perfil de Ativo	O período, em dias, que você deseja armazenar as informações do perfil de ativos. A configuração **Uso avançado** ativa QRadar para aplicar avançados, granular banco de dados lógicos para os dados de ativos. A lógica de retenção do banco de dados granular permite selecionar a partir de uma variedade de configurações diferentes. Se desejar aplicar um período de retenção para todos os dados e ativos, é possível configurar essa configuração de sistema.
Ativa identidade do Host DNS para consultas	Ativa QRadar para executar o Sistema de nomes de domínio (DNS) consultando a identidade de host.
Ativar Buscas WINS para Identidade do Host	Permite QRadar executar o Windows serviço do Nome da Internet (WINS) consultando a identidade de host.
Perfil ativo de intervalo de relatório	O intervalo, em segundos, que o banco de dados armazena em um novo ativo de perfil de informações.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Configurações do Sistema**.
4. Configure as configurações do sistema.
5. Clique em **Salvar**.
6. No menu da guia **Admin**, selecione **Avançado** > **Implementar Configuração Integral**.

   Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Visão geral de valores de retenção de ativos

Informações adicionais para o período, em dias, que você deseja armazenar as informações do perfil de ativos.

- Ativos são testados com relação aos limites de retenção em intervalos regulares. Por padrão, o intervalo de limpeza é de 12 horas

- Todos os períodos de retenção especificados estão relacionados à data da última visualização das informações, independentemente de as informações terem sido vistas pela última vez por um scanner ou observadas passivamente pelo sistema.
- Informações do ativo são excluídas conforme expiram, o que significa que após o intervalo de limpeza, todas as informações do ativo dentro de seu limite de retenção permanecem.
- Por padrão, ativos que estão associados a vulnerabilidades sem recursos (conforme detectado pelo QVM ou outro scanner) são retidos.
- Ativos podem sempre ser excluídos manualmente por meio da UI.

Tabela 25. Componentes do ativo

Componente do ativo	Retenção padrão (em dias)	Notas
Endereço IP	120 dias	Por padrão, Endereços IP fornecidos pelo usuário são retidos até serem excluídos manualmente.
Endereços MAC (Interfaces)	120 dias	Por padrão, interfaces fornecidas pelo usuário são retidas até que sejam excluídas manualmente.
Nomes de host de DNS e NetBIOS	120 dias	por padrão, os nomes de host fornecidos pelo usuário são retidos até que sejam excluídos manualmente.

Tabela 25. Componentes do ativo (continuação)

Componente do ativo	Retenção padrão (em dias)	Notas
Propriedades do Ativo	120 dias	Por padrão, Endereços IP fornecidos pelo usuário são retidos até serem excluídos manualmente. As propriedades do ativo que esse valor pode afetar são: • Nome Dado • Nome Unificado • Peso • Descrição • Proprietário de Negócios • Contato Comercial • Technical Owner • Contato Técnico • Local • Confiança de Detecção • Wireless AP • SSID Wireless • ID do Comutador • ID da Porta do Comutador • Requisito de Confidencialidade do CVSS • Requisito de Integridade do CVSS • Requisito de Disponibilidade do CVSS • Potencial de Danos Colaterais do CVSS • Usuário Técnico • S.O. Fornecido pelo Usuário • Tipo de Substituição de S.O. • ID de Substituição do S.O. • Estendido • Risco do Cvss Legado (Pré 7.2) • VLAN • Tipo de ativo

Tabela 25. Componentes do ativo (continuação)

Componente do ativo	Retenção padrão (em dias)	Notas
Produtos de Ativo	120 dias	Por padrão, produtos fornecidos pelo usuário são retidos até que sejam excluídos manualmente. Produtos de ativo incluem o seguinte: • S.O. do Ativo • Aplicativos Instalados do Ativo • Produtos associados às portas abertas do ativo
Portas "Abertas" do Ativo	120 dias	
Grupos netBIOS do ativo	120 dias	Grupos NetBIOS são raramente usados e muitos clientes podem não ter conhecimento de sua existência. Nos casos em que são usados, eles são excluídos após 120 dias.
Aplicativo Cliente do Ativo	120 dias	Aplicativos Clientes ainda não são alavancados na UI. Esse valor pode ser ignorado.
Usuários do Ativo	30 dias	

Configurando certificados do servidor IF-MAP

Antes de configurar a autenticação de IF-MAP na janela Configurações do sistema, é necessário configurar o certificado do servidor IF-MAP.

Configurando o certificado do servidor IF-MAP para autenticação básica

Esta tarefa fornece instrução sobre como configurar seu certificado IF-MAP para autenticação básica.

Antes de Iniciar

Entre em contato com o administrador de servidor IF-MAP para obter uma cópia do certificado público do servidor IF-MAP. O certificado deve possuir a extensão de arquivo `.cert`, por exemplo, ifmapserver.cert.

Procedimento

1. Utilizando o SSH, efetue login no QRadar como o usuário raiz.
2. Copie o certificado para o diretório `/opt/qradar/conf/trusted_certificates`.

Configurando o certificado do servidor IF-MAP para autenticação mútua.

Esta tarefa fornece instrução para como configurar seu certificado IF-MAP para autenticação mútua.

Antes de Iniciar

Entre em contato com o administrador de servidor IF-MAP para obter uma cópia do certificado público do servidor IF-MAP. O certificado deve possuir a extensão de arquivo `.cert`, por exemplo, ifmapserver.cert.

Autenticação mútua requer configuração de certificado em seu console e seu servidor IF-MAP. Para obter assistência para configurar o certificado em seu IF-MAP do servidor, entre em contato com seu administrador do servidor MAP IF-.

Procedimento

1. Utilizando o SSH, efetue login no QRadar como o usuário raiz.
2. Acesse o certificado no diretório `/opt/qradar/conf/trusted_certificates`
3. Copie o certificado intermediário SSL e SSL para o certificado raiz da Verisign IF-MAP servidor como certificados de CA. Para obter assistência, entre em contato com seu admistrador de servidor IF-MAP.
4. Digite o seguinte comando para criar o Public-Key Cryptography Standards arquivo com a extensão do arquivo filename .pkcs12 utilizando o seguinte comando:`openssl pkcs12 -export -inkey <private_key> -in <certificate> -out <pkcs12_filename.pkcs12> -name "IFMAP Client"`
5. Digite o seguinte comando para copiar o arquivo pkcs12 para o diretório /opt/qradar/conf/key_certificates :`/tmp:cp <pkcs12_filename.pkcs12> /opt/qradar/conf/key_certificates`
6. Create a client on the IF-MAP server with the Certificate authentication and upload the SSL certificate. Para obter assistência, entre em contato com seu admistrador de servidor IF-MAP.
7. Altere as permissões do diretório digitando os seguintes comandos:`chmod 755 /opt/qradar/conf/trusted_certificateschmod 644 /opt/qradar/conf/trusted_certificates/*.cert`
8. Digite o seguinte comando para reiniciar o serviço do Tomcat :`serviço tomcat reiniciar`

Substituindo certificados SSL nos produtos QRadar

Por padrão, o IBM Security QRadar é configurado com um certificado Security Sockets Layer autoassinado. Ao usar um certificado autoassinado para acessar a web, você recebe uma mensagem de aviso informando que o certificado não foi reconhecido. É possível substituir esse certificado SSL por um certificado autoassinado atualizado, por um assinado pela autoridade de certificação (CA) interna ou por um certificado assinado pela CA pública.

Visão geral de certificados SSL

SSL é um protocolo de segurança que fornece privacidade de comunicação para que os aplicativos cliente/servidor possam se comunicar de uma maneira projetada para evitar espionagem do tráfego de rede, violação e falsificação de mensagens.

SSL é um padrão de mercado usado pelos websites para proteger transações on-line. Para gerar um link SSL, um servidor da web requer um certificado SSL. Os certificados SSL são emitidos por autoridades de certificação internas ou de terceiros confiáveis.

Raiz confiável

Os navegadores e os sistemas operacionais incluem uma lista pré-instalada de certificados confiáveis, que são instalados no armazenamento de autoridades de Certificação Raiz Confiável.

Tabela 26. Certificados suportados pelo QRadar

Certificado	Descrição
Auto-assinado	Um certificado autoassinado fornece segurança básica, permitindo a criptografia de dados entre o usuário e o aplicativo. Como os certificados autoassinados não podem ser autenticados por nenhuma autoridade de certificação raiz existente conhecida, os usuários são avisados sobre esse certificado desconhecido e devem aceitá-lo para continuar.
Assinado pela CA interna	As organizações que têm sua própria autoridade de certificação raiz interna podem criar um certificado usando essa CA interna. Esse certificado é suportado pelo QRadar, e a autoridade de certificação raiz interna também é importada no ambiente do QRadar.
Assinado pela CA intermediária/CA pública	Os certificados assinados por CAs públicas conhecidas e os certificados intermediários são suportados pelo QRadar. Os certificados públicos assinados podem ser usados diretamente no QRadar, e os certificados que são assinados por CAs intermediárias são instalados usando o certificado assinado e o certificado intermediário para fornecer funções certificado válido. **Nota:** Um certificado intermediário geralmente é usado por organizações que criam múltiplas chaves SSL em seus ambientes e desejam que elas sejam assinadas por um fornecedor de certificação conhecido/comercial. Ao usar a chave intermediária, elas podem criar subchaves dela. Quando essa configuração for usada, o QRadar deverá ser configurado com o certificado intermediário e o certificado SSL do host para que as conexões com o host possam verificar o caminho do certificado completo.

Conexões SSL entre componentes do QRadar

Para estabelecer todas as conexões SSL internas entre componentes, o QRadar usa o certificado do servidor da web que é pré-instalado no QRadar Console. Quando o certificado pré-instalado é substituído, o processo de instalação do certificado copia o certificado para todos os hosts gerenciados na implementação, exceto para os dispositivos QRadar Incident Forensics.

Todos os certificados confiáveis do QRadar devem atender aos seguintes requisitos:

- O certificado deve ser um certificado X.509 e ter codificação Base64 PEM.
- O certificado deve ter uma extensão do arquivo `.cert`, `.crt`, `.pem` ou `.der`.
- Os arquivos keystore que contêm certificados devem ter a extensão de arquivo `.truststore`.
- O arquivo de certificado deve ser armazenado no diretório `/opt/qradar/conf/trusted_certificates`.

Importante: Se você é um cliente IBM Security QRadar Incident Forensics, entre em contato com o Suporte ao cliente (www.ibm.com/support/) para obter assistência com a instalação ou a atualização de seu certificado SSL customizado no keystore do QRadar Incident Forensics.

Se a chave SSL estiver configurada com uma senha, ela deverá ser inserida manualmente sempre que o serviço for reiniciado. Com essa configuração, o serviço da UI da web estará indisponível até que a senha seja inserida, como durante uma instalação de correção do QRadar, um failover de HA ou uma reinicialização do sistema. Neste exemplo, os usuários não poderão efetuar login e os hosts do QRadar gerenciados não poderão recuperar as atualizações de configuração ou a origem de log do relatório, mensagens de status de armazenamento de dados e regras até que o serviço da web fique disponível.

Criando uma solicitação de assinatura de certificado SSL com chaves RSA de 2048 bits

1. Use SSH para efetuar login no QRadar Console.
2. Gere um arquivo de chave privado usando o comando a seguir:

   ```
   openssl genrsa -out qradar.key 2048
   ```

   Nota: Não use as opções de criptografia privada, porque elas podem causar problemas de compatibilidade.
   O arquivo `qradar.key` é criado no diretório atual. Guarde esse arquivo para usá-lo ao instalar o certificado.
3. Gere o arquivo de solicitação de assinatura de certificado (CSR). O arquivo `qradar.csr` é usado para criar o certificado SSL, com uma CA interna ou com autoridades de certificação comerciais. Execute o comando a seguir e forneça as informações necessárias conforme é solicitado:

   ```
   openssl req -new -key qradar.key -out qradar.csr
   ```

   Exemplo de saída:

   ```
   Forneça as informações a seguir solicitadas na linha de comandos:
   [root@qradar ~]# openssl genrsa -out qradar.key 2048
   Generating RSA private key, 2048 bit long modulus
   .....................................+++
   ........................+++
   e is 65537 (0x10001)
   [root@bluecar ~]# openssl req -new -key qradar.key -out qradar.csr
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [XX]:US
   State or Province Name (full name) []:MyState
   Locality Name (eg, city) [Default City]:MyCity
   Organization Name (eg, company) [Default Company Ltd]:MyCompany
   Organizational Unit Name (eg, section) []:MyCompanyOrg
   Common Name (eg, your name or your server's hostname) []:qradar.mycompany.com
   ```

```
Email Address []:email@mycompany.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@bluecar ~]#
```

4. Se você deseja verificar as informações no CSR antes de enviá-las, digite o seguinte comando:

   ```
   openssl req -noout -text -in qradar.csr
   ```

   Se informações incorretas forem inseridas, execute o comando OpenSSL novamente para recriar o arquivo CSR.
5. Use o Secure File Transfer Protocol ou outro programa para copiar com segurança o arquivo CSR em seu computador.
6. Envie o CSR para a autoridade de certificação interna ou comercial para assinatura de acordo com as instruções da autoridade.

   Nota: O CSR é identificado como um certificado em formato Apache.

Certificados assinados por uma autoridade de certificação interna

Se o certificado for emitido por uma autoridade de certificação interna e não por um provedor de certificado comercial, o QRadar deverá ser atualizado para incluir o certificado raiz interno no armazenamento de certificados local para uma validação de certificado apropriada. Os certificados de verificação raiz são automaticamente incluídos com o sistema operacional.

Para atualizar o armazenamento de certificado raiz de âncoras de confiança no RedHat:

1. Copie o certificado raiz da CA para `/etc/pki/ca-trust/source/anchors/`.
2. Execute o comando a seguir na linha de comandos SSH:

   ```
   update-ca-trust
   ```

Instalando um novo certificado SSL no QRadar Console

Antes de Iniciar

Deve-se ter o seguinte:

- O certificado recém-assinado pela sua CA interna ou por um certificado público.
- A chave privada `qradar.key` para gerar o arquivo CSR.
- Um certificado intermediário, se usado pelo seu provedor de certificado.

Nota: Se um certificado intermediário for usado, execute o comando "install_ssl_cert.sh" com a sinalização `-b` para instalar o novo certificado e o certificado intermediário. Quando usado, ele solicita três caminhos de arquivos:

- `SSLCertifficateFile`
- `SSLIntermediateCertificateFile`
- `SSLCertificateKeyFile`

Procedimento

1. Use SSH para efetuar login no QRadar Console como o usuário raiz.
2. Instale o certificado inserindo o comando a seguir:

```
[root@csd2-primary ssl]# ls
cert.cert cert.key
[root@qradar ssl]# /opt/qradar/bin/install_ssl_cert.sh -b
Path to private key file (SSLCertificateKeyFile): /root/ssl/cert.key
Path to public key file (SSLCertificateFile): /root/ssl/cert.cert
```

Exemplo de saída:

```
You have specified the following:
SSLCertificateKeyFile of '/root/ssl/cert.key'
SSLCertificateFile of '/root/ssl/cert.cert'
Continue and reconfigure Apache now (includes restart of httpd daemon)
(Y/[N])? s
Restarting Apache
Stopping httpd: [ OK ]
Starting httpd: [ OK ]
Waiting for Apache to be running . done!
Stopping hostcontext
[Q] Shutting down hostcontext service: Sending SIGQUIT to h[ OK ]xt
[Q] Shutting down hostcontext service: [ OK ]
Restarting Tomcat
Sending SIGQUIT to tomcat [ OK ]
Stopping httpd: [ OK ]
Shutting down tomcat: [ OK ]
Starting tomcat: [ OK ]
Starting httpd: [ OK ]
Restarting hostcontext
[Q] Starting hostcontext service: [ OK ]
Restarting hostcontext on 172.16.77.105
OK: Successfully applied custom SSL certificate.
[root@qradar ssl]#
```

3. Na guia **Administração**, clique em **Avançado** > **Implementar configuração integral**

   Nota: Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleta de dados para eventos e fluxos para até que a implementação seja concluída.

Detecção de Problemas

Se houver problemas com o certificado, como um nome ou endereço IP incorreto, se a data de expiração for atingida ou se houver uma mudança de IP ou de nome do host no console, será possível escolher reverter para um certificado autoassinado.

Para gerar um certificado autoassinado, siga estas etapas no QRadar Console:

1. Faça backup dos certificados que foram instalados anteriormente e que não estão funcionando. Os certificados existentes são detectados e relatados quando você executa a geração de certificado, fazendo com que o processo de geração pare.

   ```
   mkdir /root/backup.certs/
   mv /etc/httpd/conf/certs/cert.* /root/backup.certs/
   ```

2. Execute o comando **/opt/qradar/bin/install_ssl_cert.sh -generate** para gerar novos certificados. Esse processo também é usado durante a instalação do QRadar para gerar o certificado SSL inicial.

   ```
   [root@qavm215 certs]# /opt/qradar/bin/install_ssl_cert.sh --generate
   Generating self-signed SSL certificate ... (OK)
   Installing generated SSL certificate ... (OK)
   Tue Sep 19 14:00:42 ADT 2017 [install_ssl_cert.sh] OK:
   Generated SSL certificate installed successfully
   [root@qavm215 certs]#
   ```

3. Mova o certificado recém-gerado para um novo diretório. Use o script `install_ssl_cert.sh` no modo de Instalação para instalar e distribuir os novos certificados SSL.

```
[root@qavm215 ~]# mkdir /root/updated.certs/
[root@qavm215 ~]# mv /etc/httpd/conf/certs/cert.* /root/updated.certs/
[root@qavm215 ~]# /opt/qradar/bin/install_ssl_cert.sh
Path to Public Key File (SSLCertificateFile): /root/updated.certs/cert.cert
Path to Private Key File (SSLCertificateKeyFile): /root/updated.certs/cert.key

You have specified the following:

       SSLCertificateFile of /root/updated.certs/cert.cert
    SSLCertificateKeyFile of /root/updated.certs/cert.key

Re-configure Apache now (includes restart of httpd) (Y/[N])? f
Backing up current SSL configuration ... (OK)
Installing user SSL certificate ... (OK)
Reloading httpd configuration:
 - Restarting httpd service ... (OK)
Restarting services:
 - Stopping hostcontext ... (OK)
 - Restarting Tomcat ... (OK)
 - Starting hostcontext ... (OK)
Tue Sep 19 14:45:57 ADT 2017 [install_ssl_cert.sh] OK:
Install SSL Cert Completed
[root@qavm215 ~]#
```

Endereçamento IPv6 em implementações de QRadar

O endereçamento IPv4 e IPv6 é suportado para conectividade de rede e gerenciamento de software e dispositivos IBM Security QRadar. Durante a instalação do QRadar, é solicitado que você especifique se seu protocolo da Internet é IPv4 ou IPv6.

Revise os detalhes a seguir sobre endereçamento IPv6.

"Componentes do QRadar que suportam endereçamento IPv6"

"Implementando QRadar em ambientes IPv6 ou mistos" na página 91

"Limitações de endereçamento IPv6 " na página 92

Componentes do QRadar que suportam endereçamento IPv6

Os componentes do QRadar a seguir suportam endereçamento IPv6:

Guia Atividade de Rede

Como **Endereço de Origem IPv6** e **Endereço de Destino IPv6** não são colunas padrão, eles não são exibidos automaticamente. Para exibir essas colunas, deve-se selecioná-las durante a configuração de seus parâmetros de procura (definição de coluna).

Para economizar espaço e indexar em um ambiente de origem IPv4 ou IPv6, campos de endereço IP extra não são armazenadas ou exibidos. Em uma combinação de ambientes IPv4 e IPv6, um registro de fluxo contém os dois endereços IPv4 e IPv6.

Os endereços IPv6 são suportadas para dados do pacote, incluindo dados sFlow e NetFlow V9. No entanto, versões mais antigas do NetFlow podem não suportar IPv6.

Guia Atividade de Log

Como **Endereço de Origem IPv6** e **Endereço de Destino IPv6** não são colunas padrão, eles não são exibidos automaticamente. Para exibir essas colunas, deve-se selecioná-las durante a configuração de seus parâmetros de procura (definição de coluna).

Quando um endereço não existe, os registros baseadas em modelo são usados para evitar desperdício de espaço. DSMs pode analisar endereços IPv6 a partir da carga útil do evento. Se algum DSM não puder analisar endereços IPv6, uma extensão de fonte de log poderá analisar os endereços. Para obter informações adicionais sobre extensões de origem de log, consulte *Guia de Usuários de Origens de Log*.

Procurando, agrupamento e relatando campos IPv6

É possível procurar eventos e fluxos usando parâmetros IPv6 nos critérios de procura.

Também é possível agrupar e classificar registros de eventos e fluxos que são baseados em parâmetros IPv6.

É possível criar relatórios que sejam baseados em dados de procuras baseadas em IPv6.

Regras Customizadas

A regra customizada a seguir para suportar endereçamento IPv6 foi incluída: **IP SRC/DST = Endereço IPv6**

Blocos de construção baseados em IPv6 estão disponíveis em outras regras.

Editor de implementação

O editor de implementação suporta endereços IPv6.

Módulos de suporte de dispositivos (DSMs)

DSMs podem analisar a origem IPv6 e o endereço de destino de cargas úteis de eventos.

Implementando QRadar em ambientes IPv6 ou mistos

Para efetuar login no QRadar em um ambiente misto ou IPv6, coloque o endereço IP entre colchetes:

```
https://[<Endereço IP>]
```

Ambientes IPv4 e IPv6 podem usar um arquivo de hosts para conversão de endereço. Em um ambiente IPv6 ou misto, o cliente resolve o endereço do Console pelo seu nome do host. Deve-se incluir o endereço IP do console IPv6 no arquivo `/etc/hosts` no cliente.

Fontes de fluxo, como NetFlow e sFlow, são aceitas a partir de endereços IPv4 e IPv6. Origens de eventos, como syslog e SNMP, são aceitas de endereços IPv4 e IPv6. É possível desativar pacotes configuráveis de superfluxos e fluxos em um ambiente IPv6.

Restrição:
Por padrão, não é possível incluir um host gerenciado somente por IPv4 em um console de modo misto IPv6 e IPv4. Deve-se executar um script para ativar um host gerenciado somente por IPv4.

Limitações de endereçamento IPv6

Quando o QRadar é implementado em um ambiente IPv6, as seguintes limitações são conhecidas:

- A hierarquia de rede não é atualizada para suportar IPv6.

  Algumas partes da implementação do QRadar, incluindo inspeção, procura e análise, não se beneficiam da hierarquia de rede. Por exemplo, na guia Atividade de Log, não é possível procurar ou agregar eventos Por Rede
- Nenhum perfil de ativo baseado em IPv6.
- Perfis de ativos são criados apenas se QRadar receber eventos, fluxos e dados de vulnerabilidades para hosts IPv4.
- Nenhum teste de perfil do host em regras customizadas para endereços IPv6.
- Nenhuma indexação ou otimização especializadas de endereços IPv6.
- Nenhuma origem e destino baseados em IPv6 para ofensas

Instalando um host gerenciado somente IPv4 em um ambiente misto

Por padrão, em produtos IBM Security QRadar, não é possível incluir um host gerenciado somente IPv4 em um console de modo misto IPv6 e IPv4. Deve-se executar um script para ativar um host gerenciado somente por IPv4.

Procedimento

1. Instale o QRadar Console selecionando endereçamento IPv6.
2. Após a instalação, no QRadar Console, digite o seguinte comando:
   `/opt/qradar/bin/setup_v6v4_console.sh`
3. Para incluir um host gerenciado IPv4, digite o seguinte comando:
   `/opt/qradar/bin/add_v6v4_host.sh`
4. Inclua o host gerenciado utilizando o editor de implementação.

Retenção de Dados

Configure o período de retenção customizada para datas específicas.

depósitos de Retenção de definir as políticas de retenção para eventos e fluxos de mensagens que correspondem aos requisitos de filtro customizado. Como QRadar recebe eventos e fluxos, cada evento e fluxo é comparado em relação a critérios de filtro depósito de retenção. Quando um evento ou fluxo corresponder a um filtro depósito de retenção, ele é armazenado no depósito de retenção até que o período de tempo da política de retenção for atingido. Esse recurso permite a configuração de múltiplos depósitos de retenção.

depósitos de retenção serão colocados em ordem de prioridade a partir da fileira de cima a linha inferior no Retenção de Evento e janelas de Retenção de Fluxo. Um registro é armazenado no depósito que corresponde aos critérios de filtro com prioridade mais alta. Se a gravação não corresponder a nenhum dos depósitos de retenção configurados, a gravação será armazenada no depósito de retenção padrão, que está localizado abaixo da lista de depósito de retenção configurável.

Configurando depósitos de retenção

Por padrão, as janelas Eventos de retenção e Fluxos de retenção fornece um depósito de retenção e 10 depósitos de retenção não configurados. Até que se

configure um depósito de retenção, todos os eventos events or flows são armazenados em um depósito de retenção padrão.

Sobre Esta Tarefa

As janelas Retenção de Evento e Retenção de Fluxo fornecem as seguintes informações para cada depósito de retenção :

Tabela 27. janela parâmetros de retenção

Parâmetro	**Descrição**
Ordem	A ordem de prioridade das partições de retenção.
Nome	O nome do depósito de retenção.
Retenção	O período de retenção do depósito de retenção.
Compactação	A política de compactação do depósito de retenção.
Exclusão de Política	A política de exclusão do depósito de retenção.
Filtrar	Os filtros aplicados ao depósito de retenção. Mova o ponteiro do mouse sobre o parâmetro **Filtros** para obter informações adicionais sobre os filtros aplicados.
Distribuições	O depósito de retenção usa como uma porcentagem de retenção de dados total em todos os seus depósitos de retenção.
Ativado	Especifica se o depósito de retenção está ativado (verdadeiro) ou desativado (false).
Data de criação	A data e hora em que o depósito de retenção foi criado.
Data da Modificação	A data e hora em que o depósito de retenção foi modificado pela última vez.

A barra de ferramentas fornece as seguintes funções:

Tabela 28. Barra de ferramentas da janela Retenção

Função	**Descrição**
Editar	Editar um depósito de retenção.
Ativar/Desativar	Ativar ou desativar um depósito de retenção. Quando a desativação de um depósito, quaisquer novos dados que corresponde aos requisitos do depósito desativado são armazenados no próximo depósito que corresponde as propriedades.
Excluir	Excluir um depósito de retenção. Quando você exclui um depósito de retenção, os dados contidos no depósito de retenção não são removidos do sistema, apenas os critérios que definem o depósito são excluídos. Todos os eventos ou fluxos de mensagens são mantidos em armazenamento.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. Clique em **de Eventos de Retenção** ou **Fluxo de Retenção** ícone.
4. Clique duas vezes no depósito de retenção primeiro disponível.
5. Configure os seguintes parâmetros:

Parâmetro	*Descrição*
Nome	Digite um nome exclusivo para o depósito de retenção.
Mantenha dados colocados nesse depósito para	Selecione um período de retenção. Quando o período de retenção for atingido, os dados são excluídos de acordo com o parâmetro *Excluir dados neste depósito*.
Permite que dados neste depósito sejam compactados.	Selecione a caixa de opção para ativar a compactação de dados e, em seguida, selecione um intervalo de tempo na caixa de listagem. Quando o quadro de tempo for atingido, todos os dados no depósito de retenção são elegíveis para serem compactadas. Isso aumenta a performance do sistema pela garantia que não há compressão de dados dentro do período específico. A compactação ocorre apenas quando o espaço em disco utilizado atingir 83% para cargas úteis e 85% para registros.
Excluir dados neste depósito	Selecione uma política de exclusão. Selecione **Quando o espaço de armazenamento é necessário** se você desejar dados que correspondam ao parâmetro *Mantenha dados colocados no depósito para esta* para permanecer no armazenamento até que o sistema de monitoramento detecte que o armazenamento em disco é necessário. Se o espaço em disco utilizado atingir 85% para registros e 83% para cargas úteis, os dados serão excluídos. A exclusão continua até que o espaço em disco utilizado atingir 82% para registros e 81% para cargas úteis. Selecione **Imediatamente após o período de retenção ter expirado** se você deseja que os dados sejam excluídos imediatamente na correspondência do **Mantenha dados colocados no depósito para este parâmetro**. Os dados são excluídos no processo de manutenção do disco próxima planejada, independentemente do espaço livre em disco e requisitos de compactação. Quando de armazenamento é necessário, apenas os dados que corresponde ao **Mantenha dados colocados no depósito** para este parâmetro ser excluído.

Parâmetro	*Descrição*
Descrição	Digite uma descrição para o depósito de retenção.
Filtros Atuais	Configure seus filtros. Na primeira lista, selecione um parâmetro que você deseja filtrar. Por exemplo, Dispositivo, Porta de Origem, ou Nome do Evento. Na segunda lista, selecione o modificador que deseja utilizar para o filtro. A lista de modificadores depende do atributo selecionado na primeira lista. No campo de texto, digite informações específicas relacionadas a seu filtro e, em seguida, clique em **Incluir Filtro**. Os filtros são exibidos na caixa de texto **Filtros atuais**. Você pode selecionar um filtro e clicar em **Remover Filtro** para remover um filtro da caixa de texto **Filtrar Atual**.

6. Clique em **Salvar**.
7. Clique em **Salvar**, novamente.

   O depósito de retenção iniciado armazenamento de dados que correspondem aos parâmetros de retenção imediatamente.

Gerenciando Sequência de Depósito de Retenção

É possível alterar a ordem dos depósitos de retenção para assegurar que os dados estejam sendo correspondidos com relação aos depósitos de retenção na ordem que corresponda aos seus requisitos.

Sobre Esta Tarefa

Os depósitos de retenção são sequenciados na ordem de prioridade da linha superior até a linha inferior nas janelas Retenção de Evento e Retenção de Fluxo. Um registro é armazenado no primeiro depósito de retenção que corresponde aos parâmetros de registro.

Não é possível mover o depósito de retenção padrão. Ele reside sempre no fim da lista.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. Clique no ícone **Retenção de Evento** ou **Retenção de Fluxo**.
4. Clique no ícone.
5. Selecione e mova o depósito de retenção necessário para o local correto.

Editando um Depósito de Retenção

Se necessário, você pode editar os parâmetros de um depósito de retenção.

Sobre Esta Tarefa

Na janela Parâmetros de Retenção, o painel Filtros Atuais não é exibido ao editar um depósito de retenção padrão.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. Escolha uma das seguintes opções:
4. Clique no ícone **Retenção de Evento**.
5. Clique no ícone **Retenção de Fluxo**.
6. Selecione o depósito de retenção que você deseja editar e, em seguida, clique em **Editar**.
7. Edite os parâmetros. Para obter informações adicionais, consulte "Configurando depósitos de retenção" na página 92.
8. Clique em **Salvar**.

Ativando e Desativando um Depósito de Retenção

Ao configurar e salvar um depósito de retenção, ele é ativado por padrão. É possível desativar um depósito para ajustar sua retenção de evento ou de fluxo.

Sobre Esta Tarefa

Ao desativar um depósito, quaisquer novos eventos ou fluxos que correspondam aos requisitos do depósito desativado são armazenados no próximo depósito que corresponde às propriedades de evento ou fluxo.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. Escolha uma das seguintes opções:
4. Clique no ícone **Retenção de Evento**.
5. Clique no ícone **Retenção de Fluxo**.
6. Selecione o depósito de retenção que você deseja desativar e, em seguida, clique em **Ativar/Desativar**.

Excluindo um Depósito de Retenção

Quando você exclui um depósito de retenção, os eventos ou fluxos contidos no depósito de retenção não são removidos do sistema, apenas os critérios que definem o depósito são excluídos. Todos os eventos ou fluxos são mantidos em armazenamento.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. Escolha uma das seguintes opções:
4. Clique no ícone **Retenção de Evento**.
5. Clique no ícone **Retenção de Fluxo**.
6. Selecione o depósito de retenção que você deseja excluir e, em seguida, clique em **Excluir**.

Configurando Notificações do Sistema

É possível configurar alertas de desempenho do sistema para limites. Esta seção fornece informações sobre a configuração dos limites de seu sistema.

Sobre Esta Tarefa

A tabela a seguir descreve os parâmetros da janela Notificações do Sistema Global

Tabela 29. Parâmetros da Janela Notificações do Sistema Global

Parâmetro	Descrição
Carregamento do sistema durante 1 minuto	Digite a média de limite de carregamento do sistema durante o último minuto.
Carregamento do sistema durante 5 minutos	Digite a média de limite de carregamento do sistema durante os últimos 5 minutos.
Carregamento do sistema durante 15 minutos	Digite a média de limite de carregamento do sistema durante os últimos 15 minutos.
Porcentagem de troca usada	Digite a porcentagem de limite de espaço de troca utilizado.
Pacotes recebidos por segundo	Digite o número de limite de pacotes recebidos por segundo.
Pacotes transmitidos por segundo	Digite o número limite de pacotes transmitidos por segundo.
Bytes recebidos por segundo	Digite o número limite de bytes recebidos por segundo.
Bytes transmitidos por segundo	Digite o número limite de bytes transmitidos por segundo.
Erros de recebimento	Digite o número limite de pacotes corrompidos recebidos por segundo.
Erros de transmissão	Digite o número limite de pacotes corrompidos transmitidos por segundo.
Colisões de pacotes	Digite o número limite de colisões que ocorrem por segundo durante a transmissão de pacotes.
Pacotes de recebimento descartados	Digite o número limite de pacotes recebidos que são descartados por segundo devido a uma falta de espaço nos buffers.
Pacotes de transmissão descartados	Digite o número limite de pacotes transmitidos que são descartados por segundo devido a uma falta de espaço nos buffers.
Erros da transportadora de transmissão	Digite o número limite de erros de transportadora que ocorrem por segundo durante a transmissão de pacotes.
Erros de quadro de recebimento	Digite o número limite de erros de alinhamento de quadro que ocorrem por segundo em pacotes recebidos.
Saturações de fifo de recebimento	Digite o número limite de erros de saturação Primeiro a Entrar, Primeiro a Sair (FIFO) que ocorrem por segundo em pacotes recebidos.

Tabela 29. Parâmetros da Janela Notificações do Sistema Global (continuação)

Parâmetro	Descrição
Saturações de fifo de transmissão	Digite o número limite de erros de saturação Primeiro a Entrar, Primeiro a Sair (FIFO) que ocorrem por segundo em pacotes transmitidos.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Notificações do Sistema Global**.
4. Insira valores para cada parâmetro que você deseja configurar.
5. Para cada parâmetro, selecione **Ativado** e **Responder se o valor for** e, em seguida, selecione uma das seguintes opções:

Opção	Descrição
Maior Que	Um alerta ocorrerá se o valor do parâmetro exceder o valor configurado.
Menor Que	Um alerta ocorrerá se o valor do parâmetro for menor que o valor configurado.

6. Digite uma descrição da resolução preferencial para o alerta.
7. Clique em **Salvar**.
8. No menu da guia, clique em **Implementar Mudanças**.

Configurando notificações por email customizadas

Ao configurar regras em QRadar, especifique que cada vez que a regra gerar uma resposta, uma notificação por email será enviada para os destinatários. A notificação por email fornece informações úteis, como propriedades de evento ou fluxo.

Sobre Esta Tarefa

É possível customizar o conteúdo que está incluído na notificação por email para resposta da regra editando o arquivo `alert-config.xml`.

Nota: As referências aos fluxos não se aplicam ao QRadar Log Manager.

Deve-se criar um diretório temporário no qual seja possível editar facilmente a cópia dos arquivos, sem o risco de sobrescrever os arquivos padrão. Depois de editar e salvar o arquivo `alert-config.xml`, deve-se executar um script que valide suas mudanças. O script de validação aplica automaticamente suas mudanças em uma área temporária, a partir da qual é possível implementar usando o editor de implementação QRadar.

Procedimento

1. Usando o SSH, efetue login no QRadar Console como o usuário raiz.
2. Crie um novo diretório temporário para usar para editar com segurança as cópias dos arquivos padrão.
3. Para copiar os arquivos que estão armazenados no diretório `custom_alerts` no diretório temporário, digite o seguinte comando:

```
cp /store/configservices/staging/globalconfig/templates/
custom_alerts/*.* <directory_name>
```

A opção <directory_name> é o nome do diretório temporário que você criou.

4. Confirme se os arquivos foram copiados com êxito:
   a. Para listar os arquivos no diretório, digite o seguinte comando:
      ```
      ls -lah
      ```
   b. Verifique se o arquivo a seguir está listado:
      ```
      alert-config.xml
      ```
5. Abra o arquivo `alert-config.xml` para edição.
6. Para criar vários elementos de modelo, copie o elemento `<template></template>`, incluindo tags e conteúdo e, em seguida, cole-o abaixo do elemento existente `<template></template>`.

   Restrição: Embora seja possível incluir vários elementos do modelo, é possível configurar o `Propriedade ativa` para `Verdadeiro` em apenas um evento e um tipo de modelo de fluxo.
7. Edite o conteúdo do elemento `<template></template>`:
   a. Especifique o tipo de modelo usando a propriedade XML a seguir:
      ```
      <templatetype></templatetype>
      ```
      Os valores possíveis são evento ou fluxo. Esse valor é obrigatório.
   b. Especifique o nome de modelo usando o elemento XML a seguir:
      ```
      <templatename></templatename>
      ```
   c. Configure o elemento ativo como true:
      ```
      <active>true</active>
      ```
   d. Edite o elemento subject, se necessário.
   e. Inclua ou remova parâmetros do elemento de corpo. Para obter parâmetros válidos, consulte a tabela Parâmetros Aceitos.
   f. Repita essas etapas para cada modelo que você incluir.
8. Salve e feche o arquivo.
9. Para validar suas mudanças, digite o seguinte comando:
   ```
   /opt/qradar/bin/runCustAlertValidator.sh
                                    <directory_name>
   ```
   A opção *<directory_name>* opção é o nome do diretório temporário que você criou.

   Se o script validar as mudanças com êxito, a seguinte mensagem será exibida:
   ```
   Arquivo alert-config.xml foi implementado com êxito para temporariedade!
   ```
10. Efetue login no QRadar.
11. Clique na guia **Admin**.
12. Selecione **Avançado** > **Implementar Configuração Integral**.

    Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Exemplo

Tabela 30. Parâmetros de notificação aceitos

Parâmetros Comuns	Parâmetros de Evento	Parâmetros de Fluxo
AppName	EventCollectorID	Tipo

Tabela 30. Parâmetros de notificação aceitos (continuação)

Parâmetros Comuns	Parâmetros de Evento	Parâmetros de Fluxo
RuleName	DeviceId	CompoundAppID
RuleDescription	DeviceName	FlowSourceIDs
EventName	DeviceTime	SourceASNList
EventDescription	DstPostNATPort	DestinationASNList
EventProcessorId	SrcPostNATPort	InputIFIndexList
Qid	DstMACAddress	OutputIFIndexList
Categoria	DstPostNATIPAddress	AppId
RemoteDestinationIP	DstPreNATIPAddress	Host
Payload	SrcMACAddress	Porta
Credibilidade	SrcPostNATIPAddress	SourceBytes
Relevância	SrcPreNATIPAddress	SourcePackets
Source	SrcPreNATPor	Direção
SourcePort	DstPreNATPort	SourceTOS
SourceIP		SourceDSCP
Destination		SourcePrecedence
DestinationPort		DestinationTOS
DestinationIP		DestinationDSCP
DestinationUserName		SourceASN
Protocolo		DestinationASN
StartTime		InputIFIndex
Duration		OutputIFIndex
StopTime		FirstPacketTime
EventCount		LastPacketTime
SourceV6		TotalSourceBytes
DestinationV6		TotalDestinationBytes
UserName		TotalSourcePackets
DestinationNetwork		TotalDestinationPackets
SourceNetwork		SourceQOS
Gravidade		DestinationQOS
CustomPropertiesList		SourcePayload

Configurando as Definições do Console

O Console fornece visualizações em tempo real, relatórios, alertas e investigação detalhada do tráfego de rede e ameaças à segurança. É possível configurar o Console para gerenciar implementações distribuídas do QRadar.

Sobre Esta Tarefa

A tabela a seguir descreve as configurações do Console:

Tabela 31. Configurações do Console

Configurações	Descrição
Configurações do Console	
ARP - Interfaces Seguras	Digite as interfaces que você deseja que sejam excluídas de atividades de resolução de ARP.
Resultados Por Página	Digite o número máximo de resultados que você deseja exibir na interface com o usuário. Este parâmetro aplica-se às guias **Ofensas**, **Atividade de Log**, **Ativos**,**Atividade de Rede** e **Relatórios**. Por exemplo, se o parâmetro **Tamanho da Página Padrão** for configurado como 50, a guia **Ofensas** exibirá um máximo de 50 ofensas.
Configurações de Autenticação	
Tempo Limite de Sessão Persistente (em dias)	Digite o período de tempo, em dias, em que um sistema do usuário é persistido.
Máximo de Falhas de Login	Digite o número de vezes que uma tentativa de login pode falhar.
Período de Tentativa de Falha de Login (em minutos)	Digite o período de tempo durante o qual o número máximo de falhas de login pode ocorrer antes que o sistema seja bloqueado.
Tempo de Bloqueio de Falha de Login (em minutos)	Digite o período de tempo que o sistema fica bloqueado se o valor de número máximo de falhas de login é excedido.
Lista de Desbloqueio de Host de Login	Digite uma lista de hosts que estão isentos de serem bloqueados no sistema. Insira múltiplas entradas utilizando uma lista separada por vírgula.
Tempo Limite de Inatividade (em minutos)	Digite a quantidade de tempo em que um usuário é automaticamente desconectado do sistema se não ocorre nenhuma atividade.
Arquivo de Mensagens de Login	Digite o local e o nome de um arquivo que inclui conteúdo que você deseja exibir na janela de login do QRadar. O conteúdo do arquivo é exibido abaixo da janela de login atual. O arquivo de mensagens de login deve estar localizado no diretório `/opt/qradar/conf` em seu sistema. Este arquivo estará no formato de texto. Para obter informações adicionais, consulte “Criando um arquivo de mensagens de login do QRadar” na página 106

Tabela 31. Configurações do Console (continuação)

Configurações	Descrição
Precedência da Permissão do Evento	Na caixa de listagem, selecione o nível de permissões da rede que você deseja designar aos usuários. Esse parâmetro afeta os eventos que são exibidos na guia **Atividade de Log**. As opções incluem: • **Apenas Rede** – Um usuário deve ter acesso à rede de origem ou à rede de destino do evento para ter essa exibição de eventos na guia **Atividade de Log**. • **Apenas Dispositivos** – Um usuário deve ter acesso a um dispositivo ou grupo de dispositivos que criou o evento para ter essa exibição de eventos na guia **Atividade de Log**. • **Redes e Dispositivos** – Um usuário deve ter acesso à rede de origem ou de destino e ao dispositivo ou grupo de dispositivos para ter uma exibição de eventos na guia **Atividade de Log**. • **Nenhum** – Todos os eventos são exibidos na guia **Atividade de Log**. Qualquer usuário com permissões de função de Atividade de Log é capaz de visualizar todos os eventos. Para obter informações adicionais sobre como gerenciar usuários, consulte Capítulo 3, "Gerenciamento do usuário", na página 11.
Configurações de DNS	
Ativar Consultas de DNS para Perfis de Ativos	Na caixa de listagem, selecione se deseja ativar ou desativar a capacidade para o QRadar procurar informações de DNS em perfis de ativos. Quando ativado, estas informações estão disponíveis no menu ativado pelo botão direito para o endereço IP ou o nome do host que está localizado no campo **Nome do Host (Nome do DNS)** no perfil do ativo.
Ativar Consultas de DNS para Identidade do Host	Na caixa de listagem, selecione se deseja ativar ou desativar a capacidade para o QRadar procurar informações de identidade do host. Quando ativado, estas informações estão disponíveis no menu ativado pelo botão direito para qualquer endereço IP ou nome do ativo.
Configurações de WINS	
Servidor WINS	Digite o local do servidor Windows Internet Naming Server (WINS).
Configfurações de Relatório	
Período de Retenção de Relatório	Digite o período, em dias, que você deseja que o sistema mantenha relatórios.

Tabela 31. Configurações do Console (continuação)

Configurações	Descrição
Configurações de Exportação de Dados	
Incluir Cabeçalho nas Exportações de CSV	Na caixa de listagem, selecione se deseja incluir um cabeçalho em um arquivo de exportação de CSV.
Máximo de Exportações Simultâneas	Digite o número máximo de exportações que deseja que ocorra de uma vez.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Console**.
4. Insira os valores para os parâmetros.
5. Clique em **Salvar**.
6. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Customizando o menu ativado pelo botão direito

Para fornecer acesso rápido às funções, customize as opções de menu usando uma interface de programação de aplicativo (API) de plug-in. Por exemplo, é possível incluir mais itens de menu, como uma opção para varrer o NetBIOS.

Sobre Esta Tarefa

O arquivo `ip_context_menu.xml` aceita nós XML `menuEntry` para customizar o menu ativado pelo botão direito.

```
<menuEntry name="{Name}" description="{Description}" exec="{ Command }"
url="{URL}" requiredCapabilities="{Required Capabilities}"/>
```

A lista a seguir descreve os atributos no elemento `menuEntry`:

Nome O texto que é exibido no menu ativado pelo botão direito.

Descrição
A descrição da entrada. O texto de descrição é exibido na dica de ferramenta de sua opção de menu. A descrição é opcional.

URL Especifica o endereço da web que é aberto em uma nova janela. É possível usar o marcador %IP% para representar o endereço IP. Para passar outros parâmetros de URL para esta URL, você deve utilizar a opção `&` , por exemplo, `url="/lookup?&ip=%IP%;force=true"`.

Comando
Um comando que você deseja executar no Console. A saída do comando é exibida em uma nova janela. Use o marcador %IP% para representar o endereço IP que está selecionado.

Recursos Necessários
Todos os recursos, por exemplo, "ADMIN", que o usuário deve ter antes de selecionar essa opção, delimitados por vírgulas. (Por exemplo, "ADMIN"). Se o usuário não tiver todos os recursos que estão listados, as entradas não serão exibidas. Os recursos necessários são um campo opcional.

O arquivo editado deve ser semelhante ao exemplo a seguir:

```
<?xml version="1.0" encoding="UTF-8"?>
<!- Este é um arquivo de configuração para incluir ações customizadas no
menu ativado pelo botão direito de endereço IP. As entradas devem estar em um dos
formatos seguintes: -->
<contextMenu>
<menuEntry name="Traceroute" exec="/usr/sbin/traceroute %IP%" />
<menuEntry name="External ARIN Lookup"
url="http://ws.arin.net/whois/?queryinput=%IP%" />
</contextMenu>
```

Procedimento

1. Utilizando o SSH, efetue login no IBM Security QRadar como o usuário raiz.
2. No QRadar do servidor, copie o arquivo `ip_context_menu.xml` a partir do diretório `/opt/qradar/conf/templates` para o diretório `/opt/qradar/conf` .
3. Abra o arquivo `/opt/qradar/conf/ip_context_menu.xml` para edição.
4. Edite os atributos no elemento `menuEntry`.
5. Salve e feche o arquivo.
6. Para reiniciar os serviços, digite o seguinte comando:

   ```
   service tomcat restart
   ```

O no menu de atalho para colunas de evento e de fluxo

Você pode incluir mais ações para as opções do mouse que estão disponíveis no colunas na tabela **Atividade de log** ou **Atividade de rede** tabela. Por exemplo, você pode incluir uma opção para visualizar mais informações sobre o IP de origem ou IP de destino.

É possível transmitir qualquer dados que estão no evento ou fluxo para o URL ou o script.

Restrição: Você pode incluir opções no menu de atalho apenas no dispositivo QRadar SIEM Console e para apenas alguns campos do banco de dados do Ariel .

Procedimento

1. Usando o SSH, efetue login no dispositivo QRadar Console como usuário raiz.
2. Vá para o diretório `/opt/qradar/conf` e criar um arquivo que é nomeado `arielRightClick.properties`.
3. Edite o arquivo `/opt/qradar/conf/arielRightClick.properties` . Utilize a tabela a seguir para especificar os parâmetros que determinam as opções para o menu **com o botão direito** .

Tabela 32. Descrição do arquivo de parâmetros `arielRightClick.properties`.

Parâmetro	Requisito	Descrição	Exemplo
`pluginActions`	Necessário	Indica ou uma URL ou ação de script.	
`arielProperty`	Necessário	Especifica a coluna ou nome do campo Ariel para o qual o menu ativado pelo botão direito está ativado.	**sourceIP** **sourcePort** **destinationIP** **qid**
`texto`	Necessário	Especifica o texto que é exibido no menu **ativado pelo botão direito**.	Procura no Google

Tabela 32. Descrição do arquivo de parâmetros `arielRightClick.properties` (continuação).

Parâmetro	Requisito	Descrição	Exemplo
`useFormattedValue`	Optional	Especifica se os valores formatados são transmitidos ao script. Definido como `true` para assegurar que o valor formatado para atributos, como `username` e de carga `útil`, são transmitidos. os valores Formatado são mais fáceis para os administradores para ler do que os valores não formatado.	Se o parâmetro for configurado para true para a propriedade nome do evento (QID), o nome do evento da QID são transmitidos ao script. Se o parâmetro estiver configurado como false, o bruto, não formatado QID valor é transmitido para o script.
`url`	Obrigatório para acessar um URL	Especifica a URL, que é aberto em uma nova janela, e os parâmetros a serem transmitidos para a URL. Utilize o formato: `$$Ariel_Field Nome`	`sourceIPwebUrlAction.url= http://www.mywebsite.com? q=$sourceIP$`
`command`	Necessário se a ação for um comando	Especifica o caminho absoluto do arquivo de comando ou script.	`destinationPortScript Action.command=/bin/echo`
`arguments`	Necessário se a ação for um comando	Especifica os dados a transmitir ao script. Utilize o seguinte formato: `$$Ariel_Field Nome`	`destinationPortScript Action.arguments=$qid$`

Para cada um dos nomes de chaves que estão especificados na lista *pluginActions* , defina a ação utilizando uma chave com o formato *nome de chave*, *de propriedade*.

4. Salve e feche o arquivo.
5. Efetue login no QRadar interface com o usuário.
6. Clique na guia **Admin**.
7. Selecione **Avançado** > **Reiniciar Servidor da Web**.

Exemplo

O exemplo a seguir mostra como incluir *de Teste de URL* como uma opção de atalho para endereços IP de origem.

```
pluginActions=sourceIPwebUrlAction

sourceIPwebUrlAction.arielProperty=sourceIP
sourceIPwebUrlAction.text=Test URL
sourceIPwebUrlAction.url=http://www.mywebsite.com?q=$sourceIP$
```

O exemplo a seguir mostra como ativar a ação de script para portas de destino.

```
pluginActions=destinationPortScriptAction

destinationPortScriptAction.arielProperty=destinationPort
destinationPortScriptAction.text=Test Unformatted Command
destinationPortScriptAction.useFormattedValue=falso
destinationPortScriptAction.command=/bin/echo
destinationPortScriptAction.arguments=$qid$
```

O exemplo a seguir mostra a inclusão vários parâmetros para uma URL ou uma ação de script.

```
pluginActions=qidwebUrlAction,sourcePortScriptAction

qidwebUrlAction.arielProperty qid =,dispositivo,eventCount
qidwebUrlAction.text=Search no Google
qidwebUrlAction.url=http://www.google.com?q=$qid$-$device$-$eventCount$

sourcePortScriptAction.arielProperty=sourcePort
sourcePortScriptAction.text=Port Unformatted Command
sourcePortScriptAction.useFormattedValue=true
sourcePortScriptAction.command=/bin/echo
sourcePortScriptAction.arguments=$qid$-$sourcePort$-$device$-$CONTEXT$
```

Criando um arquivo de mensagens de login do QRadar

É possível incluir e customizar uma mensagem de login em seu QRadar Console.

Antes de Iniciar

Deve-se ter acesso raiz para a interface da linha de comandos para criar um arquivo de mensagens de login.

Procedimento

1. Efetue login no QRadar como o usuário raíz.
2. No arquivo `/etc/`, digite o comando a seguir:

   ```
   vim loginMSG
   ```

   O editor Vim cria um arquivo `loginMsg`. Não especifique o nome do arquivo com caracteres especiais.
3. Pressione `i` para digitar sua mensagem.
4. Para salvar sua mensagem, pressione ESC.
5. Para retornar à linha de comandos, digite o comando a seguir:

   ```
   :wq
   ```
6. Pressione Enter.
7. Para ativar seu banner de login, acesse **Administrador** > **Configurações do sistema**.
8. Clique em **Configurações de autenticação**.
9. No campo **Arquivo de mensagem de login**, digite o caminho do arquivo a seguir:

   ```
   /etc/loginMsg
   ```
10. Clique em **Salvar**.
11. Efetue logout do QRadar para ver a nova mensagem de login.

Razões customizadas para encerramento de ofensas

É possível gerenciar oas opções listadas na caixa de listagem **Motivo para fechamento** na guia **Ofensas**.

Quando um usuário fecha uma ofensa na guia **Ofensas**, a janela Fechar ofensa é exibida. O usuário é solicitado a selecionar um motivo na caixa de listagem **Motivo para Fechamento**. Três opções são listadas:

- Ajuste falso-positivo
- Sem problema

- Violação de Política

Administradores podem adicionar, editar e deletar as razões customizadas para encerramento de ofensas na guia **Administração**.

Incluindo um motivo de ofensa customizada

Ao incluir uma razão de customizada para encerramento de ofensa, a nova razão é listada na janela Razões Customizadas para Encerramento e na caixa de lista **Razão para Fechamento** na janela Encerrar Ofensa da guia **Ofensas**.

Sobre Esta Tarefa

A janela Razões customizadas para encerramento de ofensas fornece os seguintes parâmetros.

Tabela 33. Parâmetros customizados de janelas motivos para encerramento.

Parâmetro	Descrição
Motivo	O motivo que é exibida na caixa de listagem **Razão para fechamento** na janela ofensa, na tabela **Ofensa.**
Criada por	O usuário que criou essa ofensa customizada.
Data de criação	A data e a hora de quando o usuário criou esta razão fechar ofensa customizado.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Razões customizadas para encerramento de ofensas**.
4. Clique em **Incluir**.
5. Digite a razão exclusivo para ofensas de fechamento. Os motivos devem ter entre 5 e 60 caracteres de comprimento.
6. Clique em **OK**. Sua nova ofensa customizada está agora listada na janela motivo para fechamento customizada. A caixa de lista **Motivo para Fechamento** na janela Fechar Ofensa do **Ofensas** guia também exibe o motivo customizado que você incluiu.

Editando Motivo Fechamento da Ofensa Customizado

A edição de um motivo de fechamento da ofensa customizado atualiza o motivo na janela Motivos do Fechamento Customizado e na caixa de listagem **Motivo para Fechamento** na janela Fechar Ofensa da guia **Ofensas**.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Razões customizadas para encerramento de ofensas**.
4. Selecione o motivo que você deseja editar.
5. Clique em **Editar**.
6. Digite um novo motivo exclusivo para fechamento de ofensas. Os motivos devem ter entre 5 e 60 caracteres de comprimento.

7. Clique em **OK**.

Excluindo um Motivo de Fechamento de Ofensa Customizado

A exclusão de um motivo de fechamento de ofensa customizado remove o motivo da janela Motivos de Fechamento Customizados e da caixa de listagem *Motivo para Fechamento* na janela Fechar Ofensa da guia **Ofensas**.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Razões customizadas para encerramento de ofensas**.
4. Selecione o motivo que você deseja excluir.
5. Clique em **Excluir**.
6. Clique em **OK**.

Configurando uma propriedade de recurso customizado

Defina propriedades do ativo para faciliar as consultas de ativos. As propriedades customizadas fornecem mais opções de consulta.

Procedimento

1. Clique na guia **Admin**.
2. Clique em **Propriedades Customizadas Ativo**.
3. No campo **Nome** , digite um descritor para a propriedade de recurso customizado.
4. No menu drop-down **Tipo** , selecione **Numeric** ou **Text** para definir o tipo de informações para a propriedade de recurso customizado.
5. Clique em **OK**.
6. Clique na guia **Ativos**.
7. Clique em **Editar ativo** > **Propriedades Customizadas Ativo**.
8. Insira as informações necessárias no campo de valor.
9. Clique em **OK**.

Gerenciamento de índice

O recurso Gerenciamento de índice permite controlar a indexação de banco de dados em propriedades de eventos e fluxos.

Indexar as propriedades de eventos e fluxos permitirá otimizar suas procuras. É possível ativar a indexação para qualquer propriedade que esteja listada na janela Gerenciamento de índice e ativá-la em mais de uma propriedade.

O recurso Gerenciamento de índice também fornece estatísticas, como:

- A porcentagem de procuras salvas em execução na sua implementação que incluem a propriedade indexada
- O volume de dados que são gravados no disco pelo índice durante o período de tempo selecionado

Para ativar a indexação de carga útil, deve-se ativar a indexação na propriedade de Filtro rápido.

Ativando Índices

A janela Gerenciamento de Índice lista todas as propriedades de evento e fluxo que podem ser indexadas e fornece estatísticas para as propriedades. As opções de barra de ferramentas permitem que você ative e desative a indexação em propriedades de evento e fluxo selecionadas.

Sobre Esta Tarefa

A modificação da indexação do banco de dados pode diminuir o desempenho do sistema. Certifique-se de monitorar as estatísticas após a ativação da indexação em várias propriedades.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em *Configuração do sistema*.
3. Clique no ícone **Gerenciamento de Index**.
4. Selecione uma ou mais propriedades em uma lista de Gerenciamento de Índice.
5. Escolha uma das seguintes opções:
   - Clique em **Ativar Índice**.
   - Clique em **Desativar Índice**.
6. Clique em **Salvar**.
7. Clique em **OK**.

Resultados

Nas listas que incluem propriedades de evento e fluxo, nomes de propriedades indexados são anexados com o seguinte texto: *[Indexado]*. Exemplos de tais listas incluem os parâmetros de procura nas páginas de critério de procura da guia *Atividade de Log* e *Atividade de Rede* e a janela Incluir Filtro.

Ativando indexação de carga útil para otimizar os tempos de procura

Para otimizar os tempos de procura de eventos e fluxos, ative a indexação de carga útil na propriedade **Filtro Rápido**.

Restrição:

Use o recurso **Filtro Rápido** nas guias **Atividade de Log** e **Atividade de Rede** para procurar cargas úteis de evento e fluxo usando uma sequência de textos. A indexação de carga útil aumenta os requisitos de armazenamento em disco e pode afetar o desempenho do sistema. Ative a indexação de carga útil se sua implementação atender às seguintes condições:

- Os processadores de evento e fluxo estão em menos de 70% de uso do disco.
- Os processadores de evento e fluxo são inferiores a 70% do máximo de eventos por segundo (EPS) ou da classificação fluxos por interface (FPI).

Procedimento

1. Na área de janela de navegação na guia **Admin** no produtoQRadar, clique em **Configuração do Sistema**.
2. Clique em **Gerenciamento de Índice**.
3. No campo **Procura Rápida**, digite `Filtro Rápido`.

A propriedade **Filtro Rápido** é exibida para eventos e fluxos.

4. Selecione a propriedade **Filtro Rápido** que deseja indexar.

   Na tabela de resultados, use o valor na coluna **Banco de Dados** para identificar a propriedade **Filtro Rápido** de fluxos ou eventos.

5. Na barra de ferramentas, clique em **Ativar Índice**.

   Um ponto verde indica que o índice de carga útil é ativado.

   Se uma lista incluir propriedades de fluxo ou evento indexadas, os nomes das propriedades serão anexados com o seguinte texto: `[Indexado]`.

6. Clique em **Salvar**.

O que Fazer Depois

Para gerenciar índices de carga útil, consulte "Configurando o período de retenção para índices de carga útil".

Configurando o período de retenção para índices de carga útil

É possível configurar o período de tempo que produtos IBM Security QRadar podem armazenar índices de carga útil.

Por padrão, índices de carga útil são mantidos por uma semana. O período de retenção mínimo é de um dia e o máximo é de dois anos.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Configurações do Sistema**.
4. Na seção **Configurações do Banco de Dados**, selecione um período de tempo de retenção da lista **Índice de Retenção da Carga Útil**.
5. Clique em **Salvar**.
6. Feche a janela Configurações do Sistema.
7. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Capítulo 7. Gerenciamento de conjuntos de referência

Utilizando a janela de Gerenciamento do Conjunto de Referência , é possível criar e gerenciar conjuntos de referência. Você também pode importar elementos em um conjunto de referência a partir de um arquivo externo.

Um conjunto de referência é um conjunto de elementos que são derivados de eventos e fluxos que ocorram em sua rede. Exemplos de elementos que são derivadas de eventos são endereços IP ou nomes de usuário.

Depois de criar um conjunto de referência, você pode criar regras para detectar atividade de log ou atividade de rede que está associado ao conjunto de referência. Por exemplo, você pode criar uma regra para detectar quando um usuário não autorizado tentar acessar os recursos de rede. Você também pode configurar uma regra para incluir um elemento em um conjunto de referência quando atividade de log ou atividade de rede correspondem às condições da regra. Por exemplo, você pode criar uma regra para detectar quando um funcionário acessa um Web site proibido e inclua esse funcionário do endereço IP para um conjunto de referência. Para obter informações adicionais sobre como configurar regras, consulte o *Guia do Usuário* para seu produto.

Incluindo um conjunto de referência

Na guia **Admin** , você pode incluir um conjunto de referência que você pode incluir em testes de regras.

Sobre Esta Tarefa

Depois de criar um conjunto de referência, o conjunto de referência será listada na janela Gerenciamento do Conjunto de Referência. No assistente de regra, esse conjunto de referência será listada como uma opção na página **Regra de Resposta**. Depois de configurar uma ou mais regras para enviar os elementos para este conjunto de referência, os parâmetros **Número de Elementos**, **Regras Associadas** e **Capacidade** são atualizados automaticamente.

Procedimento

1. No Gerenciamento do Conjunto de Referência janela, clique em **Novo**.
2. Configure os parâmetros:

Tabela 34. Parâmetros do Conjunto de Referência

Parâmetro	Descrição
Nome	Um nome exclusivo para esse conjunto de referência.
Tipo	Não é possível editar o parâmetro **Tipo** depois de criar um conjunto de referência.
Tempo de Vida de Elementos	A quantia de tempo que você deseja manter cada elemento no conjunto de referência. Se você especificar uma quantia de tempo, você também deverá indicar quando deseja iniciar o rastreamento de tempo para um elemento.

3. Clique em **Criar**.

Editando um Conjunto de Referência

Utilize a janela Gerenciamento do Conjunto de Referência para editar um conjunto de referência.

Procedimento

1. Na janela **Gerenciamento do Conjunto de Referência**, selecione um conjunto de referência
2. Clique em **Editar**.
3. Edite os parâmetros.

Tabela 35. Parâmetros do Conjunto de Referência

Parâmetro	Descrição
Nome	Um nome exclusivo para esse conjunto de referência. O comprimento máximo é de 255 caracteres
Tipo	Não é possível editar o parâmetro **Tipo** depois de criar um conjunto de referência.
Tempo de Vida de Elementos	A quantia de tempo que você deseja manter cada elemento no conjunto de referência. Se você especificar uma quantia de tempo, você também deverá indicar quando deseja iniciar o rastreamento de tempo para um elemento. **Permanente** é a configuração padrão.

4. Clique em **Enviar**.

Excluindo Conjuntos de Referência

É possível excluir um conjunto de referência a partir da janela Gerenciamento do Conjunto de Referência.

Sobre Esta Tarefa

Ao excluir conjuntos de referência, uma janela de confirmação indica se os conjuntos de referência que você deseja excluir possuem regras que estão associadas a eles. Após excluir um conjunto de referência, a configuração **Incluir no Conjunto de Referência** é limpa a partir das regras associadas.

Dica: Antes de excluir um conjunto de referência, você pode visualizar as regras associadas na guia **Referência**.

Procedimento

Escolha uma das seguintes opções:

- Na janela Gerenciamento do Conjunto de Referência, selecione um conjunto de referência e, em seguida, clique em **Excluir**.

- Na janela Gerenciamento do Conjunto de Referência, utilize a caixa de texto **Procura Rápida** para exibir apenas os conjuntos de referência que você deseja excluir e, em seguida, clique em **Excluir Listados**.

Visualizando o Conteúdo em um Conjunto de Referência

A guia **Conteúdo** fornece uma lista dos elementos que estão incluídos neste conjunto de referência.

Procedimento

1. Na janela Gerenciamento do Conjunto de Referência, selecione um conjunto de referência.
2. Clique em **Visualizar Conteúdo**.
3. Para visualizar o conteúdo, clique na guia **Conteúdo**.

   Dica: Use o campo **Procura Rápida** para filtrar por elementos específicos. Todos os elementos que correspondem à palavra-chave são listados na lista **Conteúdo**. Em seguida, é possível selecionar a ação na barra de ferramentas.

Tabela 36. Parâmetros da Guia Conteúdo

Parâmetro	Descrição
Valor	O valor do elemento. Por exemplo, se a referência contiver uma lista de endereços IP, o valor será o endereço IP.
Origem	O ***rulename*** é colocado no conjunto de referência como uma resposta a uma regra. O**Usuário** é importado de um arquivo externo ou incluído manualmente no conjunto de referência.
Tempo de Vida	O momento que resta até que este elemento seja removido do conjunto de referência.
Última Data Vista	A data e a hora em que esse elemento foi detectado pela última vez em sua rede.

4. Clique na guia **Referências** e visualize as referências.

   Dica: Use o campo **Procura Rápida** para filtrar por elementos específicos. Todos os elementos que correspondem à palavra-chave são listados na lista **Conteúdo**. Em seguida, é possível selecionar a ação na barra de ferramentas.

Tabela 37. Parâmetros da Guia Conteúdo

Parâmetro	Descrição
Nome da Regra	O nome desta regra.
Grupo	O nome do grupo ao qual esta regra pertence.
Categoria	A categoria da regra. As opções incluem **Regra Customizada** ou **Regra de Detecção de Anomalia**.
Tipo	O tipo desta regra.
Ativado	Indica se a regra está ativada ou desativada.

Tabela 37. Parâmetros da Guia Conteúdo (continuação)

Parâmetro	Descrição
Resposta	As respostas que estão configuradas para esta regra.
Origem	**Sistema** indica uma regra padrão. **Modificado** indica que uma regra padrão foi customizada. **Usuário** indica uma regra criada pelo usuário.

5. Para visualizar ou editar uma regra associada, dê um clique duplo na regra na lista **Referências**.

   No assistente de regra, é possível editar as definições de configuração da regra.

Incluindo um Elemento em um conjunto de referência

Você inclui um elemento para uma referência do conjunto utilizando a janela Gerenciamento do Conjunto de Referência.

Procedimento

1. Na janela Gerenciamento do Conjunto de Referência, selecione um conjunto de referência.
2. Clique em **Visualizar Conteúdo**.
3. Clique na guia **Conteúdo**.
4. Na barra de ferramentas, clique em **Novo**.
5. Configure os seguintes parâmetros:

Parâmetro	Descrição
Valor(es)	Se você deseja digitar vários valores, inclua um caractere separador entre cada valor, e em seguida, especifique o caractere separador no campo **Separador de caracteres**.
Caractere Separador	Digite o caractere separador que você utilizou no campo **Valor(s)**.

6. Clique em **Incluir**.

Excluindo Elementos de um Conjunto de Referência

É possível excluir elementos de um conjunto de referência.

Procedimento

1. Na janela Gerenciamento do Conjunto de Referência, selecione um conjunto de referência.
2. Clique em **Visualizar Conteúdo**.
3. Clique na guia **Conteúdo**.
4. Escolha uma das seguintes opções:
   - Selecione um elemento e, em seguida, clique em **Excluir**.

- Utilize a caixa de texto **Procura Rápida** para exibir apenas os elementos que você deseja excluir e, em seguida, clique em **Excluir Listados**.

5. Clique em **Excluir**.

Importando Elementos em um Conjunto de Referência

É possível importar elementos a partir de um arquivo CSV ou de texto externo.

Antes de Iniciar

Assegure que o arquivo CSV ou de texto que você deseja importar esteja armazenado em seu desktop local.

Procedimento

1. Na janela Gerenciamento do Conjunto de Referência, selecione um conjunto de referência.
2. Clique em **Visualizar Conteúdo**.
3. Clique na guia **Conteúdo**.
4. Na barra de ferramentas, clique em **Importar**.
5. Clique em **Procurar**.
6. Selecione o arquivo CSV ou de texto que você deseja importar.
7. Clique em **Importar**.

Exportando Elementos a Partir de um Conjunto de Referência

É possível exportar elementos do conjunto de referência para um arquivo CSV ou de texto externo.

Procedimento

1. Na janela Gerenciamento do Conjunto de Referência, selecione um conjunto de referência.
2. Clique em **Visualizar Conteúdo**.
3. Clique na guia **Conteúdo**.
4. Na barra de ferramentas, clique em **Exportar**.
5. Escolha uma das seguintes opções:
6. Se desejar abrir a lista para visualização imediata, selecione a opção **Abrir com** e selecione um aplicativo na caixa de listagem.
7. Se desejar salvar a lista, selecione a opção **Salvar Arquivo**.
8. Clique em **OK**.

Capítulo 8. Coleções dos dados de referência

Utilize os utilitários `ReferenceDataUtil.sh` para fazer as coletas de dados de referência complexa. Utilize as coletas de dados de referência para armazenar, recuperar e estruturas de dados complexos de teste.

É possivel criar os segiuntes tipos de dados de referências:

mapa de Referência
Os dados são armazenados em registros de que mapeiam uma tecla para vários valores. Por exemplo, para correlacionar a atividade do usuário em sua rede, você pode criar um mapa de referência que utiliza o parâmetro **Username** como uma chave e o usuário **ID Global** como um valor.

mapa de conjuntos de Referência
Os dados são armazenados em registros de que mapear uma tecla para vários valores. Por exemplo, para testar para acesso autorizado para uma patente, utilize uma propriedade de evento customizado para **ID Patentes** como a chave e o **Username** parâmetro como o valor. Utilize um mapa de conjuntos para preencher uma lista de usuários autorizados.

mapa de conjuntos de Referência
Os dados são armazenados em registros de que mapear uma tecla para outra chave, que é, então, mapeado para valor único. Por exemplo, para testar para violações de largura da banda da rede, você pode criar um mapa de mapas. Utilize o parâmetro **IP de Origem** como a primeira chave, o parâmetro **Aplicativo** como a segunda chave, e o parâmetro **Total de Bytes** como o valor.

Tabela de referência
Uma tabela de Referência é uma representação de valores utilizando uma combinação de duas teclas (key1 e key2). key1 pode mapear para key2s múltiplos. Cada key2 tem um mapeamento direto para um valor. Esse mapeamento permite que uma única key1 seja mapeada para vários pares de valor key2 na estrutura de dados da tabela de Referência.

Por exemplo, para testar violações de largura da banda da rede, é possível configurar a tabela de Referência para armazenar as informações relevantes, tais como 'Aplicativo', 'Usuário' e 'Horário da Violação' para cada IP de origem. Nesse caso, use a propriedade IP de Origem para key1, que pode ser mapeada para vários parâmetros key2.

- O 'Aplicativo' gerando esse tráfego é a primeira key2 e o valor armazena o parâmetro *Aplicativo*.
- O 'Usuário' é o segundo key2 e o valor armazena o parâmetro *Nome de Usuário*.
- O 'Horário da Violação' é a terceira key2 e o valor armazena o parâmetro *Horário de Início*.

Os requisitos do arquivo CSV para coletas de dados de referência

Se planejar importar um arquivo externo contendo elementos de dados em uma coleção de dados referenciais Assegure-se que aquele arquivo está separado por vírgula, no formato (CSV). Além disso, certifique-se de que você copiou o arquivo CSV para seu sistema.

O arquivo CSV deve seguir o formato nos exemplos de coletas de dados. O símbolo # na primeira coluna indica uma linha de comentário. A primeira sem comentários de linha é o cabeçalho da coluna e identifica o nome da coluna (por exemplo, `key1, key2, dados`). Em seguida, cada linha não comentada que se seguem, são do registro de dados que é incluída no mapa. Chaves são cadeias alfanuméricas.

Exemplo 1: mapa de Referência

```
#
#
# ReferenceMap
#
key1,data
key1,value1
key2,value2
```

Exemplo 2: mapa de conjuntos de Referência

```
#
#
# ReferenceMapOfSets
#
key1,data
key1,value1
key1,value2
```

Exemplo 3: Mapa de referencia de mapas

```
#
#
# ReferenceMapOfMaps
#
key1,key2,data
map1,key1,value1
map1,key2,value2
```

Example 3: Reference table

```
#
#
# ReferenceTable
#
key1,key2,type,data
map1,key1,type1,value1
map1,key2,type 1,value2
```

Criando uma Coleção de Dados de Referência

Utilize o utilitário `ReferenceDataUtil.sh` para criar uma coleção de dados de referência.

Procedimento

1. Utilizando o SSH, efetue login no QRadar como o usuário raiz.
2. Acesse o diretório /opt/qradar/bin.
3. Para criar a coleção de dados de referência, digite o seguinte comando:

   ```
   ./ReferenceDataUtil.sh create name [MAP | MAPOFSETS | MAPOFMAPS |
   REFTABLE] [ALN | NUM | IP | PORT | ALNIC | DATE]
   [-timeoutType=[FIRST_SEEN | LAST_SEEN]] [-TIMETOLIVE=]
   ```

4. Para preencher o mapa com dados de um arquivo externo, digite o seguinte comando:

   ```
   ./ReferenceDataUtil.sh load name filename [-encoding=...] [-sdf=" ... "]
   ```

Exemplo

```
Create an Alphanumeric Map
 ./ReferenceDataUtil.sh create testALN MAP ALN

Create a Map of Sets of PORT values that will age out 3 hours after they
were last seen
 ./ReferenceDataUtil.sh create testPORT MAPOFSETS PORT -timeoutType=LAST_SEEN
-timeToLive='3 hours'

Create a Map of Maps of Numeric values that will age out 3 hours 15 minutes
after they were first seen
 ./ReferenceDataUtil.sh create testNUM MAPOFMAPS NUM -timeoutType=FIRST_SEEN
-timeToLive='3 hours 15 minutes'

Create a ReferenceTable with a default of Alphanumeric values
 ./ReferenceDataUtil.sh create testTable REFTABLE ALN
-keyType=ipKey:IP,portKey:PORT,numKey:NUM,dateKey:DATE
```

O que Fazer Depois

Efetue login na interface com o usuário para criar regras que incluam dados para suas coleções de dados de referência. Também é possível criar testes de regras que detectam a atividade de elementos que estão em sua coleção de dados de referência. Para obter informações adicionais sobre como criar regras e testes de regras, consulte o *Guia de Usuários* para seu produto.

Referência de comando ReferenceDataUtil.sh

Você pode gerenciar coletas de seus dados de referência utilizando o utilitário `ReferenceDataUtil.sh`.

criar

Cria uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

[MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]
O tipo de coleta de dados de referência.

[ALN | ALNIC | NUM | IP | PORTA | DATE]
O tipo de dados no conjunto de referência :

- **ALN** especifica uma coleta de dados de referência de valores alfanuméricos. Esse tipo de dados suporta endereços IPv4 e IPv6.
- **ALNIC** specifies a reference data collection of alphanumeric values but tests ignore the case. Esse tipo de dados suporta endereços IPv4 e IPv6.
- **NUM** especifica uma coleta de dados de referência de valores numéricos.
- **Endereço IP** especifica uma coleta de dados de referência de endereços IP. Esse tipo de dados suporta apenas endereços IPv4.
- **PORT** especifica uma coleta de dados de referência de endereços PORT.
- **DATE** especifica uma coleta de dados de referência de valores de DATE.

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]
Especifica se o período de tempo que os elementos de dados permanecerão na coleta de dados de referência é a partir da hora em que o elemento foi visto pela primeira vez ou visto por último.

[-TimeToLive='']
A quantidade de tempo os elementos de dados permanecerão na coleta de dados de referência.

[-keyType=name:elementType,name:elementType,...]
Um obrigatório **REFTABLE** de parâmetro consistindo em pares nome de chave para **ELEMENTTYPE**.

[-key1Label='']
Um rótulo opcional para key1 ou a chave primária. Uma chave é um tipo de informação, como um Endereço IP.

[-valueLabel='']
Uma etiqueta opcional para os valores da coleta.

update

Cria uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]
Especifica se o período de tempo que os elementos de dados permanecerão na coleta de dados de referência é a partir da hora em que o elemento foi visto pela primeira vez ou visto por último.

[-timeToLive='']
A quantidade de tempo os elementos de dados permanecerão na coleta de dados de referência.

[-keyType=name:elementType,name:elementType,...]
Um obrigatório **REFTABLE** de parâmetro consistindo em pares nome de chave para **elementType**.

[-key1Label='']
Uma etiqueta opcional para key1.

[-valueLabel='']
Uma etiqueta opcional para os valores da coleta.

adicionar

Inclui um elemento de dados para uma coleta de dados de referência

name
O nome da coleta de dados de referência.

<value> <key1> [key2]
O par de valores de chaves que você deseja incluir. MAP e MAPOFSETS requerem Chave 1. MAPOFMAPS e REFTABLE requerem Chave 1 e Chave 2. Chaves são sequências alfanuméricas. Chave 2 é a chave de segundo nível e é necessária quando você inclui ou exclui de uma coleção MAPOFMAPS ou REFTABLE.

[-sdf=" ... "]
A sequência Formato de Data Simples que é utilizada para analisar os dados de data.

excluir

Exclui um elemento a partir de uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

<value> <key1> [key2]
O par de valor de chave que você deseja excluir. MAP e MAPOFSETS requerem Chave 1. MAPOFMAPS e REFTABLE requerem Chave 1 e Chave 2. Chaves são cadeias alfanuméricas.

[-sdf=" ... "]
A sequência Formato de Data Simples que é utilizada para analisar os dados de data.

remover

Remove uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

limpar

Apaga todos os elementos de uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

list

Lista elementos em uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

[displayContents]
Lista todos os elementos na coleta de dados de referência especificado.

listall

Lista todos os elementos em todas as coletas de dados de referência.

[displayContents]
Lista todos os elementos em todas as coletas de dados de referência.

carregamento

Preenche uma coleta de dados de referência com dados a partir de um arquivo CSV externo.

name
O nome da coleta de dados de referência.

filename
O nome do arquivo completo para ser carregado. Cada linha no arquivo representa um registro a ser incluído na coleta de dados de referência.

[-encoding=...]
Codificando o que é usado para ler os arquivos.

[-sdf=" ... "]
A sequência Formato de Data Simples que é utilizada para analisar os dados de data.

Capítulo 9. Gerenciando serviços autorizados

É possível configurar serviços autorizados na guia **Administrador** para autenticar um serviço de suporte ao cliente ou uma chamada API para sua implementação do QRadar.

Autenticando um serviço de suporte ao cliente permite que o serviço se a sua interface com o usuário QRadar e ou fechar ou atualizar as notas para uma ofensa utilizando um serviço da Web. Você pode incluir ou revogar um serviço autorizado a qualquer momento.

A API RESTful do QRadar usa serviços autorizados para autenticar chamadas API para o QRadar Console. Para obter mais informações sobre a API RESTful, consulte o *Guia da API do IBM Security QRadar*.

O Gerenciar Serviços Autorizados janela fornece as seguintes informações:

Tabela 38. Parâmetros para serviços autorizados

Parâmetro	Descrição
Nome do Serviço	O nome do serviço autorizado.
Autorizado Por	O nome do usuário ou administrador que autorizou o além do serviço.
Autenticação do Token de	O token que está associada a este serviço autorizado.
Função de usuário	O user que está associada a este serviço autorizado.
Perfil de Segurança	O perfil de segurança que está associado a este serviço autorizado.
Criado	A data em que este serviço autorizado foi criado.
Expira em	A data e hora em que o serviço autorizado expirar. Por padrão, o serviço autorizado é válido por 30 dias.

Visualizando Serviços Autorizados

A janela Serviços Autorizados exibe uma lista de serviços autorizados, a partir da qual é possível copiar o token para o serviço.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Serviços Autorizados**.
4. Na janela Gerenciar Serviços Autorizados, selecione o serviço autorizado apropriado.

   O token é exibido no campo **Token Selecionado** na barra superior. É possível copiar o token para o software do fornecedor para autenticar com o QRadar.

Adicionando um serviço autorizado

Use a janela adicionando um serviço aoutorizado, adicione um novo serviço autorizado.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Serviços Autorizados**.
4. Clique em **Incluir Serviço Autorizado**.
5. No campo **Nome do Serviço** , digite um nome para este serviço autorizado. O nome pode ter até 255 caracteres de comprimento.
6. Na lista **Função do Usuário**, selecione a função do usuário que você deseja designar a esse serviço autorizado. As funções de usuário que são designadas a um serviço autorizado para determinar as funções que este serviço pode acessar na interface com o usuário QRadar.
7. Na lista **Perfil de segurança**, selecione o perfil de segurança que você deseja designar a esse serviço autorizado. O perfil de segurança determina as redes e fontes de log às quais esse serviço pode acessar na interface com o usuário do QRadar.
8. Na lista **Data de Expiração**, digite ou selecione uma data que você deseja que esse serviço para expirar. Se uma data de expiração não é necessária, selecione **Sem Expiração**
9. Clique em **Criar Serviço**.

   A mensagem de confirmação contém um campo de token que você deve copiar para seu fornecedor de software para autenticar com QRadar SIEM.

Revogando Serviços Autorizados

Utilize a janela Incluir Serviço Autorizado para revogar um serviço autorizado.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Serviços Autorizados**.
4. Na janela Gerenciar Serviços Autorizados, selecione o serviço que você deseja revogar.
5. Clique em **Revogar Autorização**.

Suporte ao cliente de serviços autenticados

Após configurar um serviço autorizado, você deve configurar seu serviço de suporte ao cliente para acessar QRadar informações de ofensa.

Por exemplo, é possível configurar QRadar para enviar um trap SNMP que incluem as ofensas de informação de ID.

Seu serviço usa um token autorizado para autenticar QRadar pela passagem de informação atravéz de uma sequência de conmsulta HTTP. Quando autenticada, o serviço interpreta o token de autorização como o nome de ususário durante a sessão.

Seu soporte ao cliente deve usar uma sequencia de consulta para atualizar notas, ideferir ou fechar uma ofensa.

Descartar uma ofensa

O suporte ao cliente de serviço deve utilizar uma cadeia de consulta para fechar uma ofensa.

Para fechar uma ofensa, serviço de suporte ao cliente deve utilizar a cadeia de consultas a seguir :

```
https://<IP address >/console/do/sem/properties?appName=Sem&
dispatch=updateProperties&ID=<Offense ID>&nextPageId= OffenseList
&nextForward=offensesearch&attribute=dismiss&daoName =ofensa&Saída=1
&authenticationToken=<Token>
```

Tabela 39. Parâmetros de sequência de consultas para o serviço de suporte ao cliente

Parâmetro	Descrição
<Endereço IP>	O endereço IP de seu sistema QRadar.
<ID da Ofensa>	O identificador que é designado para a ofensa QRadar. Para obter o ID da ofensa, consulte a guia **Ofensas**. Para obter informações adicionais, consulte *IBM Security QRadar SIEM Users Guide*.
<Token>	O identificador de token que é fornecido para o serviço autorizado na interface com o usuário do QRadar.

Fechando uma ofensa

O suporte ao cliente de serviço deve utilizar uma cadeia de consulta para fechar uma ofensa.

Para fechar uma ofensa, serviço de suporte ao cliente deve utilizar a cadeia de consultas a seguir :

```
https://<IP Address>/console/do/sem/properties?appName=Sem&
dispatch=updateProperties&ID=<Offense ID>&nextPageId= OffenseList
&nextForward=offensesearch&attribute=dismiss&daoName =ofensa&value=2
&authenticationToken=<Token>
```

Tabela 40. Parâmetros de sequência de consultas para o serviço de suporte ao cliente

Parâmetro	Descrição
<Endereço IP>	O endereço IP de seu sistema QRadar.
<ID da Ofensa>	O identificador que é designado para a ofensa QRadar. Para obter o ID da ofensa, consulte a guia **Ofensas**. Para obter informações adicionais, consulte *IBM Security QRadar SIEM Users Guide*.
<Token>	O identificador de token que é fornecido para o serviço autorizado na interface com o usuário do QRadar.

Incluir notas a uma ofensa

Deve-se usar uma sequência de consulta para incluir notas a uma ofensa.

Para incluir notas a uma ofensa, seu serviço de suporte ao cliente deve usar as seguintes sequências de consulta:

```
https://<Endereço IP>/console/do/sem/properties?appName=Sem&amp;
dispatch=updateProperties&amp;ID=<ID da Ofensa>& OffenseList nextPageId=
amp; & nextForward=offensesearch amp; & attribute=notes amp; & valor=
amp;daoName =ofensa&amp;<NOTES>& authenticationToken= amp;<Token>
```

Tabela 41. Parâmetros de sequência de consultas para o serviço de suporte ao cliente

Parâmetro	Descrição
<Endereço IP>	O endereço IP de seu sistema QRadar.
<ID da Ofensa>	O identificador que é designado para a ofensa QRadar. Para obter o ID da ofensa, consulte a guia **Ofensas**. Para obter informações adicionais, consulte *IBM Security QRadar SIEM Users Guide*.
<Token>	O identificador de token que é fornecido para o serviço autorizado na interface com o usuário do QRadar.

Capítulo 10. Gerenciar de backup e recuperação

É possível recuperar e fazer backup de configuração de informações e dados do QRadar.

Você pode utilizar o recurso de backup e recuperação para fazer backup dos seus dados de eventos e fluxo no entanto, você deve restaurar de eventos e fluxo de dados manualmente. Para obter assistência na restauração de dados de eventos e fluxo, consulte o *Restaurando Dados Sua Nota Técnica*.

Por padrão, o QRadar cria um backup archive de suas informações de configuração diariamente à meia-noite. O arquivamento de backup inclui informações de configuração, dados ou ambos a partir do dia anterior.

Você pode utilizar dois tipos de backups: backups de configuração e backups de dados.

Backups de configuração incluem os seguintes componentes:

- Recursos
- Certificados
- Logotipos customizados
- Regras Customizadas
- Dispositivo de Suporte Módulos (DSMs)
- Categorias de Evento
- Fontes de Fluxo
- Fluxo e procuras de eventos
- Grupos
- Informações de gerenciamento de índice
- Informações de chave de licença
- Fontes de log
- Ofensas
- Elementos do conjunto de referência
- Planejamentos de armazenamento e encaminhamento
- Usuários e informações de funções de usuário
- Vulnerabilidade de dados (se QRadar Vulnerability Manager for instalado)

Backups de dados incluem as seguintes informações:

- Informações de log de auditoria
- Dados do evento
- Dados de Fluxo
- Dados do relatório
- Índices

Gerenciamento de arquivo de backup

Visualizar e gerenciar arquivos de backup

Na janela Gerenciador de arquivos de backup, é possível visualizar e gerenciar todos os arquivos de backup com êxito.

Visualizando Archives de Backup

Utilize a janela Archives de Backup para visualizar uma lista de seus archives de backup.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Backup e Recuperação**.

Importando um Archive de Backup

A importação de um backup archive é útil se você deseja restaurar um backup archive que foi criado em outro host do QRadar.

Sobre Esta Tarefa

Se você colocar um backup archive do QRadar no diretório `/store/backupHost/inbound` no servidor do Console, o backup archive será importado automaticamente.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Backup e Recuperação**.
4. No campo **Fazer Upload do Archive**, clique em **Procurar**.
5. Localize e selecione o archive do qual você deseja fazer upload. O archive deve incluir uma extensão .tgz.
6. Clique em **Abrir**.
7. Clique em **Fazer Upload**.

Excluindo um Archive de Backup

Para excluir um backup archive, o backup archive e o componente de Contexto de Host devem estar localizados no mesmo sistema. O sistema também deve estar em comunicação com o Console e nenhum outro backup pode estar em andamento.

Sobre Esta Tarefa

Se um arquivo de backup for excluído, ele será removido do disco e do banco de dados. Além disso, a entrada será removida dessa lista e um evento de auditoria será gerado para indicar a remoção.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Backup e Recuperação**.
4. Na seção **Backups Existentes**, selecione o archive que você deseja excluir.
5. Clique em **Excluir**.

Criação de backup archive

Por padrão, o QRadar cria um backup archive de suas informações de configuração diariamente à meia-noite. O backup archive inclui informações de configuração, dados, ou ambos, a partir do dia anterior. É possível customizar esse backup noturno e criar uma configuração de backup on demand, conforme necessário.

Agendando backup noturno

Use a janela Configuração de recuperação de backup para configurar um processo de agendamento noturno.

Sobre Esta Tarefa

Por padrão, o processo de backup noturno inclui apenas os arquivos de configuração. É possível customizar seu processo de backup noturno para incluir dados do seu console e de seu host gerenciado. Também é possível customizar seu período de retenção de backup, local do backup archive, o limite de tempo para um backup para processar antes de expirar o tempo limite e a prioridade de backup em relação a outros processos. QRadar

A janela Backup Recovery de Configuração fornece os seguintes parâmetros:

Tabela 42. Parâmetros de configuração de recuperação

Parâmetro	Descrição
Configuração de Backup Geral	
Caminho do Repositório de Backup	Digite o local onde deseja armazenar o arquivo de backup. O local padrão é `/store/backup`. Esse caminho deve existir antes que o processo de backup for iniciado. Se esse caminho não existir, o processo de backup será interrompida. Se você modificar esse caminho, certifique-se de que o novo caminho é válido em todos os sistemas em sua implementação. • dados ativos são armazenados no diretório `/armazenar`. Se possuir ambos, os dados ativos e arquivos de backup armazenado no mesmo diretório, a capacidadde de armazenamento de dados deve facilmente ser alcançada e seus backups agendados irão falhar. Recomendamos que você especificar um local de armazenamento em outro sistema ou copie seus arquivos de backup para outro sistema depois que o processo de backup for concluído. Você pode utilizar um NFS (Network File System) solução de armazenamento em seu QRadar de implementação. Para obter informações adicionais sobre como utilizar o NFS, consulte o *Guia de armazenamento não integrado*.

Tabela 42. Parâmetros de configuração de recuperação (continuação)

Parâmetro	Descrição
Período de Retenção de Backup (dias)	Digite ou selecione o período de tempo, em dias, que você deseja armazenar arquivos de backup. O padrão é 2 dias. Este período de tempo só afeta arquivos de backup gerado como um resultado de um processo planejado. backups on demand ou arquivos de backup importados não são afetadas por este valor.
Planejamento de Backup Noturno	Selecione uma opção de backup.
Selecione os hosts gerenciados nos quais você gostaria de executar backups de dados:	Essa opção é exibida somente se você selecionar a opção **Configuração e Backups de Dados**. Todos os hosts em sua implementação são listados. O primeiro host na lista é seu; ele está ativado para backup de dados por padrão, portanto, nenhuma caixa de opções é exibida. Se você tiver hosts gerenciados em sua implementação, os hosts gerenciados são listados abaixo do Console e cada host gerenciado inclui uma caixa de opções. Selecione a caixa de opção para os hosts gerenciados nos você deseja executar backups de dados. Para cada host (console ou host gerenciado), é possivel opcionalmente limpar os ítens de dados que deseja excluir do arquivo de backup.
Backup Apenas de Configuração	
Limite de Tempo de Backup (min)	Digite ou selecione o período de tempo, em minutos, que você deseja permitir que o backup seja executado. O padrão é 180 minutes. Se o processo de backup excede o limite de tempo configurado, o processo de backup é automaticamente cancelado.
Prioridade de Backup	Nessa caixa de listagem, selecione o nível de importância que desejado, para que o sistema insira no processo de backup de configuração em comparação com outros processos. Uma prioridade média ou alta têm um impacto maior no desempenho do sistema.
Backup de Dados	
Limite de Tempo de Backup (min)	Digite ou selecione o período de tempo, em minutos, que você deseja permitir que o backup seja executado. O padrão é 1020 minutes. Se o processo de backup excede o limite de tempo configurado, o backup é automaticamente cancelado.

Tabela 42. Parâmetros de configuração de recuperação (continuação)

Parâmetro	Descrição
Prioridade de Backup	Na lista, selecione o nível de importância que você deseja que o sistema para colocar no processo de backup de dados em comparação com outros processos. Uma prioridade média ou alta têm um impacto maior no desempenho do sistema.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Backup e Recuperação**.
4. Na barra de ferramentas, clique em **Configurar**.
5. Na janela Configuração de Recuperação de Backup , customize backup noturno.
6. Clique em **Salvar**.
7. Feche a janela de Arquivos de Backup.
8. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Criando um Archive de Backup de Configuração On Demand

Se você precisar fazer backup de seus arquivos de configuração em um momento diferente do seu backup planejado noturno, poderá criar um backup archive on demand. Archives de backup on demand incluem apenas informações de configuração.

Sobre Esta Tarefa

Você inicia um backup archive on demand durante um período em que o QRadar possui a carga de processamento baixa, tal como depois de horários normais de trabalho. Durante o processo de backup, o desempenho do sistema é afetado.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Backup e Recuperação**.
4. Na barra de ferramentas, clique em **Backup On Demand**.
5. Insira os valores para os parâmetros a seguir:

Opção	Descrição
Nome	Digite um nome exclusivo que você deseja designar para este backup archive. O nome pode ter até 100 caracteres alfanuméricos de comprimento. O nome pode conter caracteres a seguir: sublinhado (_), traço (-) ou ponto (.).
Descrição	Digite uma descrição para este backup archive de configuração. A descrição pode ter até 255 caracteres de comprimento.

6. Clique em **Executar Backup**.

   É possível iniciar um novo backup ou restaurar processos apenas depois que o backup on demand for concluído. É possível monitorar o processo de backup archive na janela Archives de Backup. Consulte "Visualizando Archives de Backup" na página 128.

Restauração de arquivo de backup

Restaurar um arquivo de backup pode ser útil se for preciso restaurar previamente configurações de arquivos arquivadas, dados de ativos, e odados de ofensas em seu QRadar sistema.

Antes de restaurar um arquivo de backup, observe as seguintes considerações:

- Você só pode restaurar um backup archive criado dentro do mesmo release de software, incluindo o nível de correção. Por exemplo, se você estiver executando IBM Security QRadar 7.1.0 (MR2), o arquivo de backup deve ter sido criado em IBM Security QRadar.
- O processo de restauração restaura apenas suas informações de configuração, dados de ativo, e ofensa de dados. Para obter assistência na restauração de seus dados do evento ou fluxo, consulte o *Restaurando Dados Sua Nota Técnica*.
- Se o arquivo de backup se originou em um sistema do Console endereço com NAT, você pode apenas restaurar esse backup archive em um sistema com NAT.

Durante o processo de restauração, as seguintes etapas são executadas no Console:

1. os arquivos existentes e as tabelas de banco de dados são submetidos a backup.
2. Tomcat é encerrado.
3. Todos os processos do sistema serão encerrados.
4. Os arquivos são extraídos do arquivo de backup e restaurados em disco.
5. tabelas de banco de dados são restaurados.
6. Todos os processos do sistema serão reiniciados.
7. Tomcat for reiniciado.

Restaurando um Archive de Backup

É possível restaurar um backup archive. A restauração de um backup archive é útil se você tiver uma falha de hardware do sistema ou desejar armazenar um backup archive em um dispositivo de substituição.

Sobre Esta Tarefa

É possível reiniciar o Console somente após o processo de restauração ser concluído.

O processo de restauração pode demorar várias horas; o tempo de processo depende do tamanho do backup archive que deve ser restaurado. Ao concluir, uma mensagem de confirmação é exibida.

Uma janela fornece o status do processo de restauração. Esta janela fornece quaisquer erros para cada host e instruções para solucionar os erros.

Os seguintes parâmetros estão disponíveis na janela Restaurar um Backup:

Tabela 43. Parâmetros de Restaurar um Backup

Parâmetro	Descrição
Nome	O nome do backup archive.
Descrição	A descrição, se houver, do backup archive.
Tipo	O tipo de backup. Apenas backups de configuração podem ser restaurados, portanto, este parâmetro exibe **config**.
Selecionar Todos os Itens de Configuração	Quando selecionada, esta opção indica que todos os itens de configuração são incluídos na restauração do backup archive.
Restaurar Configuração	Lista os itens de configuração a serem incluídos na restauração do backup archive. Para remover itens, é possível limpar as caixas de seleção para cada item que você deseja remover ou limpar a caixa de seleção **Selecionar Todos os Itens de Configuração**.
Selecionar Todos os Itens de Dados	Quando selecionada, esta opção indica que todos os itens de dados são incluídos na restauração do backup archive.
Restaurar Dados	Lista os itens de configuração a serem incluídos na restauração do backup archive. Todos os itens são limpos por padrão. Para restaurar itens de dados, é possível selecionar as caixas de seleção para cada item que você deseja restaurar.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Backup e Recuperação**.
4. Selecione o archive que você deseja restaurar.
5. Clique em **Restaurar**.
6. Na janela Restaurar um Backup, configure os parâmetros.
7. Clique em **Restaurar**.
8. Clique em **OK**.
9. Clique em **OK**.
10. Escolha uma das seguintes opções:
    - Se a interface com o usuário foi fechada durante o processo de restauração, abra um navegador da web e efetue login no QRadar.
    - Se a interface com o usuário não foi fechada, a janela de login será exibida. Efetue login no QRadar.
11. Siga as instruções na janela de status.

O que Fazer Depois

Após verificar que seus dados foram restaurados para seu sistema, assegure que sua DSMs, scanners de avaliação de vulnerabilidades (VA) e protocolos de origem de log também são restauradas.

Se o backup archive se originou em um cluster HA, você deverá clicar em **Implementar Mudanças** para restaurar a configuração de cluster HA após a conclusão da restauração. Se a replicação de disco estiver ativada, o host secundário sincronizará imediatamente os dados depois que o sistema for restaurado. Se o host secundário foi removido da implementação após um backup, o host secundário exibirá um status de falha na janela Gerenciamento de Sistema e Licença.

Restaurando um Archive de Backup Criado em um Sistema QRadar Diferente

Cada backup archive inclui as informações de endereço IP do sistema a partir do qual o backup archive foi criado. Ao restaurar um backup archive a partir de um sistema QRadar diferente, o endereço IP do backup archive e o sistema que você está restaurando são incompatíveis. É possível corrigir os endereços IP incompatíveis.

Sobre Esta Tarefa

É possível reiniciar o Console somente após o processo de restauração ser concluído.

O processo de restauração pode demorar várias horas; o tempo de processo depende do tamanho do backup archive que deve ser restaurado. Ao concluir, uma mensagem de confirmação é exibida.

Uma janela fornece o status do processo de restauração. Esta janela fornece quaisquer erros para cada host e instruções para solucionar os erros.

Você deve parar o serviço iptables em cada host gerenciado em sua implementação. O serviço Iptables é um firewall baseado em Linux.

A janela Restaurar um Backup (Acessibilidade de Hosts Gerenciados) fornece as informações a seguir.

Tabela 44. Parâmetros de Restaurar um Backup (Acessibilidade de Host Gerenciado)

Parâmetro	Descrição
Nome do host	O nome do host gerenciado.
Endereço IP	O endereço IP do host gerenciado.
Status de Acesso	O status de acesso para o host gerenciado.

A janela Restaurar um Backup fornece os seguintes parâmetros:

Tabela 45. Parâmetros de Restaurar um Backup

Parâmetro	Descrição
Nome	O nome do backup archive.
Descrição	A descrição, se houver, do backup archive.
Tipo	O tipo de backup. Apenas backups de configuração podem ser restaurados, portanto, este parâmetro exibe **config**.

Tabela 45. Parâmetros de Restaurar um Backup (continuação)

Parâmetro	Descrição
Selecionar Todos os Itens de Configuração	Quando selecionada, esta opção indica que todos os itens de configuração são incluídos na restauração do backup archive. Esta caixa de seleção é selecionada por padrão. Para limpar todos os itens de configuração, desmarque a caixa de seleção.
Restaurar Configuração	Lista os itens de configuração a serem incluídos na restauração do backup archive. Todos os itens são selecionados por padrão. Para remover itens, é possível limpar as caixas de seleção para cada item que você deseja remover ou limpar a caixa de seleção **Selecionar Todos os Itens de Configuração**.
Selecionar Todos os Itens de Dados	Quando selecionada, esta opção indica que todos os itens de dados são incluídos na restauração do backup archive. Esta caixa de seleção é selecionada por padrão. Para limpar todos os itens de dados, limpe esta caixa de seleção.
Restaurar Dados	Lista os itens de configuração a serem incluídos na restauração do backup archive. Todos os itens são limpos por padrão. Para restaurar itens de dados, é possível selecionar as caixas de seleção para cada item que você deseja restaurar.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Backup e Recuperação**.
4. Selecione o archive que você deseja restaurar.
5. Clique em **Restaurar**.
6. Na janela Restaurar um Backup, configure os parâmetros.
7. Clique em **Restaurar**.
8. Pare as tabelas IP:
   a. Utilizando o SSH, efetue login no host gerenciado como o usuário raiz.
   b. Digite o comando **`service iptables stop`**.
   c. Repita para todos os hosts gerenciados em sua implementação.
9. Na janela Restaurar um Backup, clique em **Testar Acesso aos Hosts**.
10. Após completar o teste para todos os hosts gerenciados, verifique se o status na coluna **Status de Acesso** indica o status **OK**.
11. Se a coluna **Status de Acesso** indicar um status **Nenhum Acesso** para um host, pare iptables novamente e, em seguida, clique em **Testar Acesso ao Host** novamente para tentar uma conexão.
12. Na janela Restaurar um Backup, configure os parâmetros.
13. Clique em **Restaurar**.
14. Clique em **OK**.
15. Clique em **OK** para efetuar login.

16. Escolha uma das seguintes opções:
    - Se a interface com o usuário foi fechada durante o processo de restauração, abra um navegador da web e efetue login no QRadar.
    - Se a interface com o usuário não foi fechada, a janela de login será exibida. Efetue login no QRadar.
17. Visualize os resultados do processo de restauração e siga as instruções para resolver quaisquer erros.
18. Atualize a janela do navegador da web.
19. No guia **Administrador**, selecione **Avançado** > **Configuração de Implementação Integral**.

    Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

O que Fazer Depois

Após verificar que seus dados foram restaurados para seu sistema, você deve reaplicar RPMs para quaisquer DSMs, scanners de avaliação de vulnerabilidades (VA) ou protocolos de origem de log.

Se o backup archive se originou em um cluster HA, você deverá clicar em **Implementar Mudanças** para restaurar a configuração de cluster HA após a conclusão da restauração. Se a replicação de disco estiver ativada, o host secundário sincronizará imediatamente os dados depois que o sistema for restaurado. Se o host secundário foi removido da implementação após um backup, o host secundário exibirá um status de falha na janela Gerenciamento de Sistema e Licença.

Restaurando Dados

É possível restaurar os dados em seu QRadar Console e hosts gerenciados a partir de arquivos de backup. A parte de dados dos arquivos de backup inclui informações sobre todas as ofensas, incluindo informações de endereço IP de origem e de destino, dados de ativo, informações da categoria de evento, dados de vulnerabilidade, dados do evento e fluxo de dados.

Cada host gerenciado em sua implementação, incluindo o QRadar Console, cria todos os arquivos de backup no diretório `/store/backup/`. Seu sistema pode incluir uma montagem de `/store/backup` a partir de um serviço SAN ou NAS externo. Serviços externos fornecem retenção de dados offline, de longo prazo, que é comumente requerida para os regulamentos de conformidade, como PCI.

Restrição: Você deve restaurar o backup da configuração antes de restaurar o backup de dados.

Antes de Iniciar

Assegure-se de que as condições a seguir sejam atendidas:

- Se você estiver restaurando dados em um novo QRadar Console, o backup da configuração será restaurado.
- Você conhece o local do host gerenciado no qual os dados são submetidos a backup.

- Se sua implementação incluir um ponto de montagem separado para esse volume, o diretório `/store` ou `/store/ariel` possuirá espaço suficiente para os dados que você deseja recuperar.
- Você conhece a data e hora para os dados que deseja recuperar.

Procedimento

1. Utilizando o SSH, efetue login no QRadar SIEM como o usuário raiz.
2. Acesse o diretório `/store/backup`.
3. Para listar os arquivos de backup, digite `ls -l`
4. Se os arquivos de backup forem listados, vá para o diretório raiz digitando `cd /`

   Importante: Os arquivos restaurados devem estar no diretório `/store`. Se você digitar `cd` em vez de `cd /`, os arquivos serão restaurados no diretório `/root/store`.
5. Para extrair os arquivos de backup para seu diretório original, digite o seguinte comando:

   `tar -zxpvPf /store/backup/backup.<name>.<hostname_hostID>`
   `.<target date>.<backup type>.<timestamp>.tgz`

Tabela 46. Descrição de Variáveis de Nome do Arquivo

Variável de Nome do Arquivo	Descrição
hostname_hostID	O nome do sistema QRadar que hospeda o arquivo de backup seguido pelo identificador para o sistema QRadar
target date	A data em que o arquivo de backup foi criado. O formato da data prevista é *<day>_<month>_<year>*
backup type	As opções são `dados` ou `configurações`
timestamp	O horário em que o arquivo de backup foi criado.

Resultados

Backup diário de dados captura todos os dados em cada host. Se desejar restaurar dados em um host gerenciado que contém apenas dados de evento ou de fluxo, apenas esses dados serão restaurados para esse host.

Verificando Dados Restaurados

Verifique se seus dados foram restaurados corretamente no IBM Security QRadar.

Procedimento

1. Para verificar se os arquivos foram restaurados, revise o conteúdo de um dos diretórios restaurados digitando o seguinte comando:

   `cd /store/ariel/flows/payloads/<yyyy/mm/dd>`

   É possível visualizar os diretórios restaurados que são criados para cada hora do dia. Se os diretórios estiverem ausentes, os dados não poderão ser capturados para esse período de tempo.
2. Verifique se os dados restaurados estão disponíveis.
   a. Efetue login na interface do QRadar.
   b. Clique na guia **Atividade do Log** ou **Atividade de Rede**.
   c. Selecione **Editar Procura** na lista **Procurar** na barra de ferramentas.

d. Na área de janela Intervalo de Tempo da janela Procurar, selecione **Intervalo Específico**.
e. Selecione o intervalo de tempo dos dados restaurados e, em seguida, clique em **Filtrar**.
f. Visualize os resultados para verificar os dados restaurados.
g. Se os dados restaurados não estiverem disponíveis na interface do QRadar, verifique se os dados estão restaurados no local correto e se as permissões de arquivo estão configuradas corretamente.

   Arquivos restaurados devem estar no `diretório /store`. Se você digitou `cd` em vez de `cd /` quando extraiu os arquivos restaurados, verifique o diretório `/root/store` para obter os arquivos restaurados. Se você não alterou diretórios antes de extrair os arquivos restaurados, verifique o diretório `/store/backup/store` para obter os arquivos restaurados.

   Geralmente, os arquivos são restaurados com as permissões originais. No entanto, se os arquivos são de propriedade da conta do usuário raiz, problemas poderão ocorrer. Se os arquivos são de propriedade da conta do usuário raiz, altere as permissões utilizando os comandos **`chown`** e **`chmod`**.

O que Fazer Depois

Depois de verificar se seus dados foram restaurados, você deve reaplicar RPMs para quaisquer DSMs, scanners de avaliação de vulnerabilidades (VA) e protocolos de origem de log.

Capítulo 11. Editor de implementação

Use o editor de implementação para gerenciar os componentes individuais do seu QRadar. Após a configuração de sua implementação, é possível acessar e configurar os componentes individuais de cada host gerenciado em sua implementação.

Requisitos do editor de Implementação

Antes de poder utilizar o editor de implementação, assegure-se de que ele atenda aos requisitos mínimos do sistema.

O editor de implementação requer Java Runtime Environment (JRE). Você pode fazer download Java 1,6 ou 1,7 do Java site (www.java.com). Se estiver utilizando o navegador da Web Mozilla Firefox, você deve configurar seu navegador para aceitar Java Network Language Protocol (JNLP) os arquivos.

Muitos navegadores da Web que utilizam o mecanismo do Internet Explorer Microsoft , tais como Maxthon, instala componentes que podem ser incompatíveis com a guia **Admin**. Deverá ser solicitado a desabilitação de qualquer navegador da web que está instalado no seu sistema.

Para acessar o editor de implementação a partir de um servidor proxy ou firewall, você deve configurar as definições de proxy apropriado em seu desktop. O software de varredura e, em seguida, detectar automaticamente as configurações de proxy a partir de seu navegador.

Para configurar as definições de proxy, abra o Java de configuração em seu Painel de Controle e configurar o endereço IP de seu servidor proxy. Para obter informações adicionais, consulte a documentação daMicrosoft.

Visualizações do editor de implementação

O editor de implementação fornece diferentes visualizações de sua implementação.

É possível acessar o editor de implementação usando a guia **Admin**. Você pode utilizar o editor de implementação para criar sua implementação, designar conexões e configurar cada componente.

Depois de atualizar suas definições de configuração utilizando o editor de implementação, você deve salvar essas mudanças para a área de preparação. Você deve implementar manualmente todas as mudanças utilizando a opção de menu da guia **Admin**. Todas as mudanças implementadas são então aplicadas em toda a sua implementação.

O editor de implementação fornece as visualizações a seguir:

Visualização do Sistema

Use a página Visualização do Sistema para designar o componente de software para hosts gerenciados em sua implementação. A página Visualização do Sistema

inclue todos os hosts gerenciados em sua implementação. Um host gerenciado é um sistema em sua implementação que tem o software do QRadar que está instalado.

Por padrão, a página Visualização do Sistema também inclui os seguintes componentes:

- **Host Context**, que monitora todos os componentes do QRadar para assegurar que cada componente esteja funcionando conforme o esperado.
- **Accumulator**, que analisa fluxos, eventos, relatando e gravando dados do banco de dados e alertando sobre um módulo do sistema de dispositivo (DSM).

  Um acumulador está em qualquer host que contenha um Processador de eventos.

Na página Visualização do Sistema , a área de janela esquerda fornece uma lista de hosts gerenciados, que podem ser visualizados e configurados. O editor de implementação pesquisa sua implementação quanto às atualizações de hosts gerenciados. Se o editor de implementação detectar mudanças em um host gerenciado em sua implementação, uma mensagem será exibida notificando-lhe sobre a mudança. Por exemplo, se um host gerenciado for removido, uma mensagem será exibida indicando que os componentes designados àquele host devem ser novamente designados a outro host.

Além disso, se um host gerenciado for incluído em sua implementação, o editor de implementação exibirá uma mensagem indicando que o host gerenciado foi incluído.

Visualização do evento

Use a página Visualização do evento para criar uma visualização de seus componentes.

- Componentes do QRadar QFlow Collector
- Processadores de Eventos
- QRadar Event Collectors
- Fontes externas
- Destinos externos
- Componentes do Funcionário Público
- Nós de Dados

Na página Visualização do evento, a área de janela esquerda fornece uma lista de componentes que você pode incluir na visualização. A área de janela direita fornece uma visualização de sua implementação.

Visualização de vulnerabilidade

Utilize a página Visualização de vulnerabilidade para criar uma visualização dos componentes do IBM Security QRadar Vulnerability Manager. É necessário instalar o IBM Security QRadar Vulnerability Manager para exibir essa visualização. Para obter informações adicionais, consulte *IBM Security QRadar Vulnerability Manager User Guide*

Configurando as preferencias do editor de implementação.

É possível configurar as preferências do editor de implementação para modificar os incrementos de zoom e a enquete de frequência de presença.

Procedimento

1. Selecione**Arquivo** > **Editar Preferencias**.
2. Para configurar o parâmetro **Enquete de frequência de presença**, digite com que frequência, em milisegundos, você deseja que o host gerenciado monitores suas implantações para as atualizações.
3. Para configurar o parâmetro **Incremento de Zoom** , digite o valor do incremento quando a opção zoom for selecionada.

   Por exemplo, 0,1 indica 10%.

Construindo a implementação usando o Editor de implementação

Use o Editor de implementação na guia **Administrador** para incluir e configurar componentes na implementação do IBM Security QRadar. Também é possível usar o Editor de implementação para consultar as visualizações da sua implementação.

Antes de Iniciar

Para incluir hosts gerenciados em uma implementação existente ou para incluir o QRadar Event Collectors, Processadores de Fluxo, ou outros dispositivos para sua implementação, use as **Ações de implementação** na ferramenta **Gerenciamento da Licença e do Sistema** na guia **Administrador**.

Antes de poder usar o editor de implementação, assegure-se de que as condições a seguir sejam atendidas:

- Instale o Java Runtime Environment (JRE). Você pode fazer download Java 1,6 ou 1,7 do Java site (www.java.com).
- Se você estiver utilizando um navegador Firefox, você deve configurar seu navegador para aceitar Java Network Language Protocol (JNLP) os arquivos.
- Planeje sua QRadar de implementação, incluindo os endereços IP e as informações de login para todos os dispositivos em sua implementação.

Procedimento

1. Clique na guia **Administrador** e clique em **Editor de Implementação**.
2. Clique na guia **Visualização do Evento** e inclua componentes de evento na implementação.
3. Clique na guia **Visualização do Sistema** e construa o sistema.
4. Configure os componentes.
5. Para organizar a implementação, no Editor de Implementação, clique em **Arquivo** > **Salvar em Preparação**.
6. Implemente a configuração ao escolher uma das seguintes opções na guia de **Administrador** no QRadar Console.
   - Clique em **Implementar Mudanças**.
   - Clique em **Avançado** > **Implementar Configuração Integral**.

   Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Tarefas relacionadas:

"Implementando hosts e componentes gerenciados após a instalação" na página 47
Depois da instalação, é possível incluir hosts gerenciados na imp lementação doIBM Security QRadar SIEM. Para ajudar a distribuir o processamento, você pode incluir o QRadar Event Collectors, o QRadar Processadores de Fluxo ou outros dispositivos em sua implementação.

Gerando chaves públicas para produtos QRadar

Para encaminhar eventos normalizados no editor de implementação do IBM Security QRadar, deve-se copiar o arquivo de chave pública, `/root/.ssh/id_rsa.pub,` da origem externa para o destino externo.

Se a origem externa e o destino externo estiverem em sistemas separados, a chave pública será gerada automaticamente. Se a origem e o destino externos estiverem em um sistema multifuncional, a chave pública não será gerada automaticamente. Você deve gerar manualmente a chave pública.

Procedimento

Para gerar manualmente a chave pública, siga estas etapas:

1. Use SSH para efetuar login em seu sistema como usuário raiz.
2. Para gerar a chave pública, digite o seguinte comando:
   `opt/qradar/bin/ssh-key-generating`
3. Pressione Enter.
   O par de chaves pública e privada é gerado e salvo na pasta `/root/.ssh/id_rsa` .

Gerenciador de visualização do evento

Use a página Visualização do evento para criar e gerenciar os componentes da sua implementação.

Construindo sua visualização do evento

Para construir seu Visualização de Eventos, execute as seguintes etapas:

1. Incluir componentes em sua visualização.
2. Conecte os componentes.
3. Conecte as implementações.
4. Renomeie os componentes para cada componente possui um nome exclusivo.

Visualizações de eventos dos componentes QRadar em sua implementação

Use a página Visualização de Eventos para criar uma visualização de seus componentes IBM Security QRadar, incluindo QRadar QFlow Collectors, Processadores de Eventos, QRadar Event Collectors, origens externas, destinos externos e componentes Funcionário Público.

QRadar QFlow Collector

QRadar VFlow Collector coleta fluxos de rede de dispositivos em sua rede. Os feeds registrados e em tempo real são incluídos, como toques de rede, portas de span, NetFlow e logs de fluxo do QRadar.

QRadar QFlow Collector agrupa pacotes individuais relacionados em um fluxo. Um fluxo é iniciado quando QRadar QFlow Collector detecta o primeiro pacote que tem um endereço IP de origem exclusivo, endereço IP de destino, porta de origem, porta de destino e outras opções de protocolo específicas.

Cada novo pacote é avaliado. Conta os bytes e pacotes adicionados a estatística de contagem no fluxo de gravação. No final de um intervalo, um registro de status do fluxo é enviado para um Coletor de eventos e os contadores de estatística para o fluxo são redefinidas. Um fluxo termina quando nenhuma atividade para o fluxo for detectado dentro do tempo configurado.

Se o protocolo não suporta conexões de porta-baseado em QRadar combina todos os pacotes entre os dois hosts em um único fluxo de registro. No entanto, QRadar QFlow Collector não registra fluxos até que uma conexão seja estabelecida com outro componente QRadar e dados sejam recuperados.

Coletor de eventos

Coleta eventos de segurança de dispositivos de segurança, que são conhecidos como fontes de log, em sua rede.

O Coletor de eventos normaliza os eventos coletados e envia as informações para o Processador de eventos.

Você pode conectar um console do Processador de eventos para um Processador de eventos no QRadar Console ou para outro Processador de eventos em sua implementação. O acumulador reune informações de evento e fluxo do Processador de eventos.

O Processador de eventos em QRadar Console é sempre conectado ao Funcionário Público. Esta conexão não pode ser excluída.

Nó de dados

O Nó de dados recebe eventos de segurança e fluxos de processadores de Evento e Fluxo associados.

O Nó de dados armazena estes dados de segurança para o disco.

O Nó de dados é sempre conectado ao Processador de eventos ou Processador de Fluxo componentes

Fonte externa

Uma origem de dados externa que encaminha dados normalizados para um Coletor de eventos. É possível configurar uma origem externa para receber dados e criptografar os dados antes do encaminhamento.

Versões mais recentes dos sistemas QRadar podem receber dados de versões anteriores dos sistemas QRadar. No entanto, as versões anteriores não podem receber dados das versões mais recentes. Para evitar, faça upgrade de todos os destinatários antes de você fazer upgrade dos remetentes.

Destino externo

Indica um dispositivo externo que recebe um eventos ou dados de fluxo. Um destino externo só pode receber dados de um Coletor de eventos.

Versões mais recentes dos sistemas QRadar podem receber dados de versões anteriores dos sistemas QRadar. No entanto, as versões anteriores não podem receber dados das versões mais recentes. Para evitar, faça upgrade de todos os

destinatários antes de você fazer upgrade dos remetentes.

Funcionário Público

Você pode incluir um componente Funcionário Público para cada implementação. O Funcionário Público fornece visualizações, relatórios, alertas e análise de tráfego de rede e os eventos de segurança. O Funcionário Público processa os eventos ou fluxos usando as regras customizadas que são configuradas para criar uma resposta. Se regras customizadas não existir, o Funcionário Público utiliza a regra padrão configurado para processar os violadores evento ou fluxo.

O Funcionário Público prioriza a resposta e designa um valor de magnitude que é baseado em diversos fatores, incluindo o número de respostas, gravidade, relevância e credibilidade.

Após o Funcionário Público estabelecer a magnitude, ele fornece várias opções para resolução.

Incluindo Componentes

Ao configurar sua implementação, você deve utilizar a página Visualização de Eventos no editor de implementação para incluir os componentes.

Você pode incluir os seguintes componentes para sua página QRadar Visualização de Eventos:

- Coletor de eventos
- Processador de eventos
- Origem externa
- Destino externo
- QRadar QFlow Collector
- Nó de dados

Procedimento

1. Na guia **Admin**, clique em **Editor de Implementação**.
2. Na janela Componentes de Eventos, selecione um componente que você deseja incluir em sua implementação.
3. Digite um nome exclusivo para o componente que você deseja incluir e clique em **Avançar**.

   Restrição: O nome pode ter até 20 caracteres de comprimento e pode incluir sublinhados ou hifens.
4. Na caixa de listagem **Selecione um host para designar**, selecione um host gerenciado, e, em seguida, clique em **Avançar**.
5. Clique em **Concluir**.
6. Repita as etapas 3 – 5 para cada componente que você deseja incluir em sua visualização.
7. No menu do editor de implementação, selecione **Arquivo > Salvar para migração**.

   O editor de implementação salva suas alterações na área de migração de dados e fecha automaticamente.
8. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Conectando Componentes

Depois de incluir todos os componentes necessários em sua página Visualização de Eventos, você deve conectá-los.

Sobre Esta Tarefa

Utilize a página Visualização de Eventos para conectar os componentes juntos. Algumas restrições são impostas. Por exemplo, é possível conectar um Coletor de eventos a um Processador de eventos, mas não a um componente do Funcionário Público.

A tabela a seguir descreve os componentes que você pode conectar.

Tabela 47. Descrição de Conexões de Componentes Suportadas

Conexão de Origem	Conexão de Destino	Descrição
QRadar QFlow Collector	Coletor de eventos	Um QRadar QFlow Collector pode se conectar somente a um Coletor de eventos. Um QRadar QFlow Collector não pode ser conectado a um Coletor de eventos de um dispositivo 15xx. O número de conexões não é restrito.
Coletor de eventos	Processador de eventos	Um Coletor de eventos pode ser conectado apenas a um Processador de eventos. Um Coletor de eventos do Console pode ser conectado apenas a um Processador de eventos do Console. Esta conexão não pode ser removida. Um Coletor de Eventos que não é do Console pode ser conectado a um Processador de eventos no mesmo sistema. Um Coletor de eventos não do Console pode ser conectado a um Processador de eventos remoto, mas apenas se o Processador de eventos não existir no Console.
Coletor de eventos	Destino externo	O número de conexões não é restrito.

Tabela 47. Descrição de Conexões de Componentes Suportadas (continuação)

Conexão de Origem	Conexão de Destino	Descrição
Origem externa	Coletor de eventos	O número de conexões não é restrito. Um Coletor de eventos conectado a um dispositivo somente de Evento não pode receber uma conexão externa do hardware do sistema que possui o recurso **Receber Fluxos** ativado. Um Coletor de eventos conectado a um dispositivo somente QFlow não pode receber uma conexão externa a partir de um sistema remoto se o sistema possui o recurso **Receber Eventos** ativado.
Processador de eventos	Funcionário Público (MPC)	Apenas um Processador de eventos pode se conectar a um Funcionário Público.
Processador de eventos	Processador de eventos	Um Processador de eventos do Console não pode se conectar a um Processador de eventos não do Console. Um Processador de eventos não do Console pode ser conectado a um outro Processador de eventos do Console ou não do Console, mas não a ambos ao mesmo tempo. Um Processador de eventos não do Console é conectado a um Processador de eventos do Console quando um host gerenciado não do Console é incluído.
Nó de dados	Processador de eventos	Só é possível conectar um Data Node a um Processador de Evento ou Fluxo. Você pode conectar vários Nós de dados para o Processador de Eventos mesmo para criar um cluster de armazenamento.

Procedimento

1. Na página Visualização de Eventos, selecione o componente para o qual você deseja estabelecer uma conexão.
2. Clique em **Ações** > **Incluir Conexão**.

   Uma seta é exibida em seu mapa. A seta representa uma conexão entre dois componentes.
3. Arraste a extremidade da seta para o componente com o qual você deseja estabelecer uma conexão.
4. Opcional: Configure a filtragem de fluxo em uma conexão entre um QRadar QFlow Collector e um Coletor de eventos.
   a. Clique com o botão direito do mouse na seta entre o QRadar QFlow Collector e o Coletor de eventos e clique em **Configurar**

b. No campo para o parâmetro **Filtro de Fluxo**, digite os endereços IP ou endereços CIDR para os QRadar Event Collectors para os quais você deseja que o QRadar QFlow Collector envie fluxos.

5. Clique em **Salvar**.
6. Repita estas etapas para todos os componentes restantes que requerem conexões.

Encaminhando Eventos e Fluxos Normalizados

Para encaminhar eventos e fluxos normalizados, configure um Coletor de eventos externo em sua implementação atual para receber eventos e fluxos a partir de um Coletor de eventos externo associado na implementação de recebimento.

Sobre Esta Tarefa

É possível incluir os seguintes componentes em sua página Visualização de Eventos:

- Uma **Origem Externa** é um Coletor de eventos externo a partir do qual você deseja receber dados de eventos e fluxos.

  Restrição: A origem externa deve ser configurada com as permissões apropriadas para enviar dados de eventos e fluxos para seu destino externo.
- Um **Destino Externo** é um Coletor de eventos externo para o qual você deseja enviar dados de eventos e fluxos.

Exemplo:

Para encaminhar eventos e fluxos normalizados entre duas implementações (A e B), em que a implementação B deseja receber eventos e fluxos da implementação A:

1. Configure a implementação A com um destino externo para fornecer o endereço IP do host gerenciado que inclui o Coletor de Eventos B.
2. Conecte o Coletor de Eventos A ao destino externo.
3. Na implementação B, configure uma origem externa com o endereço IP do host gerenciado que inclui Coletor de eventos A e a porta que Coletor de eventos A está monitorando.

Se desejar desconectar a origem externa, você deverá remover as conexões de ambas as implementações. A partir da implementação A, remova o destino externo e, na implementação B, remova a origem externa.

Para ativar a criptografia entre as implementações, você deve ativar a criptografia na origem e no destino externos. Além disso, você deve assegurar que a chave pública SSH para a origem externa (cliente) esteja disponível para o destino (servidor) para assegurar o acesso apropriado. Por exemplo, para ativar a criptografia entre a origem externa e Coletor de eventos B:,

1. Crie chaves ssh usando o comando **ssh-keygen -1 -t rsa** e pressione Enter quando for solicitado o diretório e o passphrase. Isso coloca o arquivo no diretório `//root/.ssh` por padrão.
2. Copie o arquivo `id_rsa.pub` para o diretório `/root/.ssh` no Coletor de eventos e no console de origem. Renomeie o arquivo para `authorized_keys`.

   Se você não tiver designado privilégios de proprietário rw (chmod 600 authorized_keys) ao arquivo e ao diretório-pai, é possível usar o comando **ssh-copy-id**. Por exemplo, **ssh-copy-id -i hostUsername@hostIP**. O **-i**

especifica que o arquivo de identidade `/root/.ssh/id_rsa.pub` seja usado. Por exemplo, `ssh-copy-id -i root@10.100.133.80`. Esse comando irá anexar todas as entradas ou criar um arquivo `authorized_keys` no console de destino com os privilégios corretos. Ele não verifica entradas duplicadas. O `authorized_keys` também precisa estar presente no console onde outros recursos são utilizados. Se um host gerenciado for incluído em um console que está encaminhando eventos, um arquivo `authorized_keys` também precisará estar presente no seu diretório `/root/.ssh`. Se não, a inclusão de um host gerenciado falhará. Isso é necessário independentemente de a criptografia ser usada entre o host gerenciado e o console.

3. No console de origem, crie um arquivo `ssh_keys_created` sob `/opt/qradar/conf`. Esse arquivo precisa ser criado para que o encaminhamento de eventos e fluxos não seja interrompido quando outros recursos (como incluir um host gerenciado em um dos consoles) forem combinados. Altere o proprietário e o grupo para **nobody** e a permissão para **775** se necessário. `chown nobody:nobody /opt/qradar/conf/ssh_keys_created` e `chmod 775 /opt/qradar/conf/ssh_keys_created` para assegurar que o arquivo possa ser submetido a backup e restauração corretamente.
4. Siga a etapa de origem e destino externos para 2 consoles. Programe o console de destino primeiro e, em seguida, implemente as mudanças. Programe o console de origem seguinte e, em seguida, implemente as mudanças.

O diagrama a seguir mostra o encaminhamento de eventos e fluxos entre as implementações.

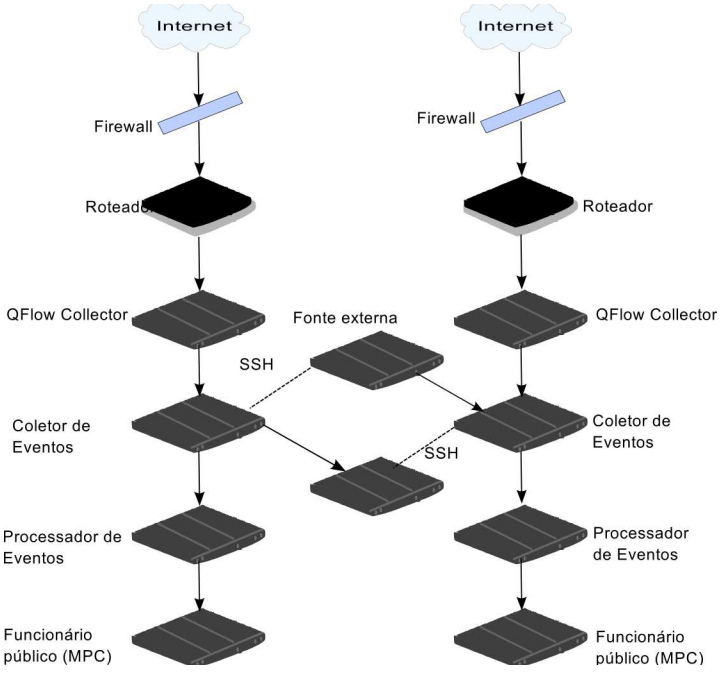

Figura 1. Encaminhando eventos entre implementações usando SSH

Se a origem ou o destino externo for um sistema multifuncional, a chave pública não será gerado automaticamente, portanto, você deve gerar manualmente a chave pública. Para obter informações adicionais sobre como gerar chaves públicas, consulte sua documentação do Linux.

Se você atualizar sua configuração do Coletor de eventos ou as portas de monitoramento, deverá atualizar manualmente as configurações de origem e de destino para manter a conexão entre as implementações.

Procedimento

1. Na guia **Admin**, clique em **Editor de Implementação**.
2. Na área de janela Componentes de Eventos, selecione **Origem Externa** ou **Destino Externo**.
3. Digite um nome exclusivo para a origem externa ou o destino externo. O nome pode ter até 20 caracteres de comprimento e pode incluir sublinhados ou hifens. Clique em **Avançar**.
4. Insira os valores para os parâmetros e clique em **Concluir**.

   O nome do host para o campo **Insira um nome para o host externo** pode conter no máximo 20 caracteres e pode incluir caracteres de sublinhados ou hifens.

   Se você selecionar a caixa de seleção **Criptografar o tráfego a partir da origem externa**, também deverá selecionar a caixa de seleção de criptografia na origem e no destino externos associados.
5. Repita para todas as origens e os destinos externos restantes.
6. No menu do editor de implementação, clique em **Arquivo** > **Salvar para Migração**.
7. No menu da guia **Admin**, selecione **Avançado** > **Implementar Configuração Integral**.

   Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Encaminhando fluxos filtrados

É possível configurar o encaminhamento de fluxos filtrados. É possível usar fluxos filtrados para dividir o encaminhamento de fluxo entre múltiplas caixas e encaminhar fluxos específicos para investigações específicas.

Procedimento

1. No sistema de destino, configure o sistema de origem como uma origem externa.
   a. Na guia **Administração**, clique em **Gerenciamento de sistema e licença** > **Ações de implementação** > **Gerenciar origens externas**.
   b. Inclua o endereço IP do sistema de origem e selecione **Receber eventos** e/ou **Receber fluxos**.
   c. Selecione **Gerenciar conexões** e selecione qual host está esperando receber a conexão externa.
   d. Clique em **Salvar**.
   e. Selecione **Implementar configuração completa** no menu **Avançado** para que as mudanças entrem em vigor.
2. No sistema de origem, configure o destino de encaminhamento, o endereço IP e o número da porta.
   a. Clique em **Menu principal** > **Administrador**.
   b. Clique em **Destinos de encaminhamento** > **Incluir**.
   c. Configure o endereço IP do sistema de destino e a porta de destino.
   d. Insira 32000 para o número da porta no sistema de origem. A porta 32000 é usada para encaminhamento de fluxo.

e. Selecione **Normalizado** na lista **Formato do evento**.

3. Configure as regras de roteamento.
   a. Clique em **Menu principal** > **Administrador**.
   b. Clique em **Regras de roteamento** > **Incluir**.
   c. Selecione as regras que você deseja incluir.

      Nota: As regras só encaminharão fluxos corretamente com base em ofensas ou informações de CRE se **Encaminhamento off-line** estiver selecionado na tela Regras de roteamento.

   Os fluxos filtrados na tela **Regras de roteamento** são encaminhados.

Renomeando Componentes

Você deve renomear um componente em sua visualização para identificar componentes exclusivamente por meio de sua implementação.

Procedimento

1. Na área de janela Componentes do Evento, selecione o componente que você deseja renomear.
2. Clique em **Ações** > **Renomear Componente**.
3. Digite um novo nome para o componente.

   O nome deve ser alfanumérico sem caracteres especiais.
4. Clique em **OK**.

Visualizando o progresso de reequilíbrio dos dados

Depois de instalar um Nó de dados em sua implementação, visualize o progresso dos dados que estão se movendo entre o processador de eventos e o Nó de dados. Se o reequilíbrio de dados estiver concluído, será possível visualizar informações adicionais sobre os Data Nodes implementados.

Procedimento

1. No QRadar SIEM, clique na guia **Admin** para visualizar o status de dados de nós em sua implementação na parte superior da janela.
2. Clique em **Visualizar** na coluna **Detalhe** para abrir a janela **Detalhes do sistema e da licença**.
3. Visualize o progresso de um reequilíbrio dos dados, e a capacidade do dispositivo Nó de dados no **de Distribuição de Dados de Segurança** .

Arquivando conteúdo do Data Node

Quando você configura um dispositivo de Data Node no modo **Archive**, nenhum dado será gravado no aplicativo. Os dados existentes são salvos.

Procedimento

1. No Editor de Implementação, clique com o botão direito no Data Node que deseja configurar para o modo archive e clique em **Configurar**.
2. Clique em **Archive**.
3. A partir do menu da guia **Admin**, clique em **Implementar Mudanças**.
4. Se desejar continuar realizando balanceamento dos dados para um Data Node que está em modo archive, clique com o botão direito em **Configurar** > **Ativo**.

Salvando dados do processador de evento em um dispositivo de Data Node

Melhore o desempenho do processador de evento salvando todos os dados em um dispositivo de Data Node e não no processador de evento. Se nenhum dispositivo de Data Node estiver disponível no mesmo cluster do processador de evento, esse processador de evento salvará os dados localmente. Quando um dispositivo de Data Node torna-se disponível, ele transfere tantos dados quanto possíveis a partir do processador de evento. Os Data Nodes balanceiam os dados para que todos os Data Nodes em um cluster tenham a mesma porcentagem de espaço livre.

Procedimento

1. No Editor de Implementação, clique com o botão direito no processador de evento que tem os dados que deseja transferir para um dispositivo de Data Node e clique em **Configurar**.
2. Clique em **Ativo** e selecione **Somente Processamento** na lista.
3. A partir do menu da guia **Admin**, clique em **Implementar Mudanças**.

Gerenciamento de visualização do sistema

Use a página Visualização do sistema para selecionar quais componentes são necessários para executar cada host gerenciado em sua implementação.

Visão geral da página Visualização do Sistema

Utilize a página Visualização do Sistema para gerenciar todos os hosts gerenciados em sua rede.

Um host gerenciado é um componente em sua rede que inclui o software do QRadar. Se um dispositivo do QRadar estiver sendo usado, os componentes desse modelo de dispositivo serão exibidos na página Visualização do Sistema. Se o software do QRadar estiver instalado em seu hardware, a página Visualização do Sistema incluirá um componente Host Context.

Use a página Visualização do Sistema para as tarefas a seguir:

- Incluir hosts gerenciados em sua implementação.
- Utilizar redes NAT em sua implementação.
- Atualizar a configuração de porta do host gerenciado.
- Designar um componente para um host gerenciado.
- Configurar o Host Context.
- Configurar um acumulador.

Requisitos de compatibilidade de software para hosts do console e hosts que não são do console

Não é possível incluir, designar ou configurar componenentes em um host gerenciado que não seja do console, quando a versão do QRadar é incompatível com a versão no console. Se componentes tiverem sido designados previsamente a um host gerenciado e ele estiver executando uma versão incompatível, será possível visualizar ainda os componentes. Entretanto, não será possível atualizar ou excluir esses componentes.

Criptografia

A criptografia fornece maior segurança para todo o tráfego entre hosts gerenciados. Para fornecer segurança melhorada, QRadar também fornece suporte integrado para OpenSSH. Quando integrado com QRadar, o OpenSSH fornece comunicação segura entre os componentes.

A criptografia ocorre entre os hosts gerenciados em sua implementação, portanto, é possível que sua implementação deva consistir em mais de um host gerenciado antes da criptografia. A criptografia é ativada utilizando túneis SSH (redirecionamento de porta) iniciado a partir do cliente. Um do cliente é o sistema que inicia uma conexão em uma relação cliente/servidor. Quando a criptografia estiver ativada para um host gerenciado, túneis de criptografia são criadas para todos os aplicativos clientes em um host gerenciado. túneis protegido de criptografia fornecem acesso aos respectivos servidores. Se você ativar a criptografia em um host gerenciado não do Console, túneis de criptografia são automaticamente criadas para os bancos de dados e conexões de serviço de suporte diferente para o Console.

Ao ativar a criptografia em um host gerenciado, o túnel SSH criptografia é criado no host cliente. Por exemplo, a conexão entre o Processador de eventos e Coletor de eventos a conexão entre Processador de eventos e Funcionário Público são criptografadas. Ao ativar a criptografia no QRadar Console, um túnel de criptografia é utilizado quando a sua procura eventos utilizando a guia **Ofensas**.

Dica: É possível com o botão direito do mouse em um componente para ativar a criptografia entre componentes.

Importante: Ativando a criptografia reduz o desempenho de um host gerenciado pelo menos 50%.

Incluindo um host gerenciado

Utilize a página System View do editor de implementação para incluir um host gerenciado.

Antes de Iniciar

Certifique-se de que você instalou o QRadar no host gerenciado.

Se você deseja ativar o NAT (Network Address Translation) para um host gerenciado, a rede deve utilizar tradução de NAT estático. Para obter informações adicionais, consulte “Redes NAT - ativado” na página 158.

Se você deseja incluir um host ativado e gerenciado NAT para um Console que não está configurado para suportar o NAT, você deve desativar NAT no Console. Para obter informações adicionais, consulte “Alterando o Status NAT para um host gerenciado” na página 160.

Procedimento

1. Clique em **Ações** > **Incluir um Host Gerenciado**.
2. Clique em **Avançar**.
3. Insira os valores para os parâmetros.

   Utilize a tabela a seguir para ajudá-lo a configurar os parâmetros.

Tabela 48. Parâmetros para o host gerenciado

Cabeçalho	Cabeçalho
Host é NATed	Selecione a caixa de opções para utilizar uma conversão de endereço de rede existente (NAT) nesse host gerenciado.
Ativar Criptografia	Selecione a caixa de opções para criar um túnel SSH de criptografia para o host.
	Selecione a caixa de opção para ativar a compactação de dados entre dois hosts gerenciados.

4. Se você selecionou a caixa de seleção **Host é NAT**, configure os parâmetros.

Tabela 49. Parâmetros para um NAT - ativado de rede

Parâmetro	Descrição
Digite um IP público do servidor ou dispositivo a adicionar.	O host gerenciado utiliza este endereço IP para se comunicar com outros hosts gerenciados em redes diferentes utilizando o NAT.
Selecione a rede com NAT	Se o host gerenciado está na mesma sub-rede que o Console, selecione o Console da rede ativado para NAT. Se o host gerenciado não está na mesma sub-rede que o Console, selecione o host gerenciado da rede ativada pelo NAT.

5. Clique em **Avançar**.
6. Clique em **Concluir**.
7. Implemente suas mudanças.

Conceitos relacionados:

"Redes NAT - ativado" na página 158

A conversão de endereço de rede (NAT) converte um endereço IP em uma rede em um endereço IP diferente em outra rede. A NAT fornece maior segurança para sua implementação do IBM Security QRadar porque as solicitações são gerenciadas por meio do processo de conversão e os endereços IP internos são ocultados. Com a NAT, os computadores que estão localizados em uma rede privada interna são convertidos por meio de um dispositivo de rede, geralmente um firewall, e podem comunicar-se com a Internet pública por meio dessa rede. Use a NAT para mapear endereços IP internos individuais para endereços IP externos individuais.

Editando um Host Gerenciado

Utilize a página Visualização do Sistema do editor de implementação para editar um host gerenciado.

Antes de Iniciar

Se você deseja ativar o NAT (Network Address Translation) para um host gerenciado, a rede deve utilizar tradução de NAT estático. Para obter informações adicionais, consulte "Redes NAT - ativado" na página 158.

Se você deseja incluir um host ativado e gerenciado NAT para um Console que não está configurado para suportar o NAT, você deve desativar NAT no Console.

Para obter informações adicionais, consulte “Alterando o Status NAT para um host gerenciado” na página 160.

Procedimento

1. Clique na guia **Visualização do Sistema**.
2. Clique com o botão direito no host gerenciado que você deseja editar e selecione **Editar host gerenciado**.

   Esta opção está disponível apenas quando o componente selecionado possui um host gerenciado que está executando uma versão compatível do QRadar.
3. Clique em **Avançar**.
4. Edite os valores de parâmetro, conforme necessário.

   Utilize a tabela a seguir para ajudá-lo a configurar os parâmetros.

Tabela 50. Parâmetros para o host gerenciado

Cabeçalho	Cabeçalho
Host é NATed	Selecione a caixa de opções para utilizar uma conversão de endereço de rede existente (NAT) nesse host gerenciado.
Ativar Criptografia	Selecione a caixa de opções para criar um túnel SSH de criptografia para o host.
	Selecione a caixa de opção para ativar a compactação de dados entre dois hosts gerenciados.

5. Se você selecionou a caixa de seleção **Host é NAT**, configure os parâmetros.

Tabela 51. Parâmetros para um NAT - ativado de rede

Parâmetro	Descrição
Digite um IP público do servidor ou dispositivo a adicionar.	O host gerenciado utiliza este endereço IP para se comunicar com outros hosts gerenciados em redes diferentes utilizando o NAT.
Selecione a rede com NAT	Se o host gerenciado está na mesma sub-rede que o Console, selecione o Console da rede ativado para NAT. Se o host gerenciado não está na mesma sub-rede que o Console, selecione o host gerenciado da rede ativada pelo NAT.

6. Clique em **Avançar**.
7. Clique em **Concluir**.

Removendo um Host Gerenciado

É possível remover hosts não gerenciados pelo Console a partir de sua implementação. Não é possível remover um host gerenciado que hospeda o Console do QRadar.

Dica: A opção **Remover Host** está disponível apenas quando o componente selecionado possui um host gerenciado que está executando uma versão compatível do QRadar.

Procedimento

1. Clique na guia **Visualização do Sistema**.
2. Clique com o botão direito no host gerenciado que você deseja excluir e selecione **Remover host**.
3. Clique em **OK**.
4. Na guia/menu **Admin**, clique em **Avançado** > **Implementar Configuração Integral**.

   Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Configurando um host gerenciado

Use a página Visualização de sistema no editor de implementação para configurar um host gerenciado.

Procedimento

1. Na página Visualização de sistema, clique com o botão direito no host gerenciado que deseja configurar e clique em **Configurar**.
2. Insira os valores para os parâmetros:

   Nos campos **Portas a excluir**, use uma vírgula para separar diversas portas.
3. Clique em **Salvar**.

Designando um componente em um host

Utilize a página System View para designar os QRadar componentes que você incluiu na página Visualização de Eventos para os hosts gerenciados em sua implementação.

Dica: A caixa de listagem exibe apenas os hosts gerenciados que estão executando uma versão compatível do QRadar.

Procedimento

1. Clique na guia **Visualização do Sistema**.
2. Na caixa de listagem **Host gerenciado** selecione o host que você deseja designar a esse componente. QRadar to.
3. Selecione o componente que você deseja designar a um host gerenciado.
4. No menu, selecione **Ações > Designar**.
5. Na caixa de listagem **Selecione um host** , selecione o host que você deseja designar a esse componente. Clique em **Avançar**.
6. Clique em **Concluir**.

Configurando Contexto de host

Utilize o Visualização do Sistema página do editor de implementação para configurar o componente Contexto de hostem um host gerenciado.

O monitora todos os componente Contexto de host QRadar componentes para assegurar que cada componente está operando conforme o esperado.

Procedimento

1. No editor de implementação, clique na guia **Visualização do Sistema**.
2. Selecione o host gerenciado que inclui o contexto do host que você deseja configurar.

3. Selecione o componente Contexto de host.
4. Clique em **Ações** > **Configurar**.
5. Insira os valores para os parâmetros.

Tabela 52. Parâmetros do Contexto de host

Parâmetro	Descrição
Limite de Aviso	Quando o limite configurado de uso do disco for excedido, um e-mail será enviado para o administrador do que indica o estado atual de uso do disco. O limite de aviso padrão é 0.75 Portanto, quando o uso do disco exceder 75%, um e-mail que indica que é o uso do disco exceder 75% é enviado. Se o uso do disco continua a aumentar acima do limite configurado, um novo e-mail é enviado após cada aumento de 5% em uso. Por padrão, Contexto de hostmonitora os seguintes partições para uso de disco : • `/` • `/store` • `/store/tmp` **Nota:** Emails de notificação são enviados de um endereço de email que é especificado em um parâmetro **Email de alerta do endereço**, ao endereço de email especificado no parâmetro **Endereço de email administrativo**. Estes parâmetros são configurados na janela Configurações do Sistema. Para obter informações adicionais, consulte Capítulo 6, “Configurar QRadar”, na página 65.
Recuperção Limite	Quando o sistema excede o limite de encerramento, uso do disco deve cair abaixo do limite de recuperação antes que os processos sejam reiniciados. O padrão é 0,90. Portanto, os processos não são reiniciados até que o uso do disco está abaixo de 90%. **Nota:** Emails de notificação são enviados de um endereço de email que é especificado em um parâmetro **Email de alerta do endereço**, ao endereço de email especificado no parâmetro **Endereço de email administrativo**. Estes parâmetros são configurados na janela Configurações do Sistema. Para obter informações adicionais, consulte Capítulo 6, “Configurar QRadar”, na página 65.

Tabela 52. Parâmetros do Contexto de host (continuação)

Parâmetro	Descrição
Encerramento Limite	Quando o sistema excede o limite de encerramento, uso do disco deve cair abaixo do limite de recuperação antes que os processos sejam reiniciados. Um e-mail é enviado ao administrador que indica o estado atual do sistema. O padrão é 0,95, portanto, quando o uso do disco excede 95%, pare todos os processos. **Nota:** Emails de notificação são enviados de um endereço de email que é especificado em um parâmetro **Email de alerta do endereço**, ao endereço de email especificado no parâmetro **Endereço de email administrativo**. Estes parâmetros são configurados na janela Configurações do Sistema. **Nota:** Para obter informações adicionais, consulte Capítulo 6, "Configurar QRadar", na página 65.
Inspeção Intervalo	A frequência, em milissegundos, que você deseja determinar o uso do disco.
Inspeção Intervalo	A frequência, em milissegundos, que você deseja inspecionar SAR de saída.
Intervalo de Alerta	A frequência, em milissegundos, que você deseja ser notificado de que o limite foi excedido.
Tempo de Resolução	O tempo, em segundos, que você deseja que a inspeção SAR para ser contratado.
Inspeção Intervalo	A frequência, em milissegundos, que você deseja monitorar os arquivos de log.
Monitorados SYSLOG FileName	Um nome do arquivo para o arquivo SYSLOG.
Alertar Tamanho	O número máximo de linhas que você deseja monitorar a partir do arquivo de log.

6. Clique em **Salvar**.

Configurando um acumulador

Utilize a página Visualização do Sistema do editor de implementação para configurar o componente do acumulador em um host gerenciado.

O componente do acumulador ajuda com a coleta de dados e a detecção de anomalias para o Processador de eventos em um host gerenciado. O componente do acumulador é responsável por receber fluxos de eventos e fluxos do Processador de eventos local, gravando dados do banco de dados, e contém o mecanismo de detecção de anomalias (ADE).

Procedimento

1. No editor de implementação, clique na guia **Visualização do Sistema**.
2. Selecione o host gerenciado que você deseja configurar.
3. Selecione o componente do acumulador.

4. Clique em **Ações** > **Configurar**.
5. Configure os parâmetros.

Tabela 53. Parâmetros do Acumulador

Parâmetro	Descrição
Acumulador Central	Especifica se o componente atual é um acumulador central. Um central acumulador existe apenas em um sistema do Console.
Mecanismo de Detecção de Anomalias	O ADE é responsável por analisar os dados de rede e encaminhar os dados para o sistema de regras para resolução. Para o acumulador central, digite o endereço e a porta utilizando a seguinte sintaxe: *<>Console:<>port* Para um acumulador não central, digite o endereço e a porta utilizando a seguinte sintaxe: *<non-Console IP Address>:<>port*
Porta de Atendimento do Acumulador de Fluxo	A porta de atendimento responsável por receber fluxos de fluxos a partir do Processador de eventos. O valor padrão é 7802.
Endereço DSM de Alertas	O endereço do módulo do sistema de dispositivo (DSM) que é utilizado para encaminhar alertas a partir do acumulador. Utilize a seguinte sintaxe: *<>DSM_IP address:<>DSM port number*.

6. Clique em **Salvar**.

Redes NAT - ativado

A conversão de endereço de rede (NAT) converte um endereço IP em uma rede em um endereço IP diferente em outra rede. A NAT fornece maior segurança para sua implementação do IBM Security QRadar porque as solicitações são gerenciadas por meio do processo de conversão e os endereços IP internos são ocultados. Com a NAT, os computadores que estão localizados em uma rede privada interna são convertidos por meio de um dispositivo de rede, geralmente um firewall, e podem comunicar-se com a Internet pública por meio dessa rede. Use a NAT para mapear endereços IP internos individuais para endereços IP externos individuais.

A configuração de NAT do QRadar requer NAT estática e permite apenas um endereço IP público por host gerenciado.

Qualquer host do QRadar que não esteja no mesmo grupo de NAT com seu peer ou esteja em um grupo de NAT diferente é configurado para usar o endereço IP público desse host para alcançá-lo. Por exemplo, ao configurar um endereço IP público no QRadar Console, qualquer host que esteja localizado no mesmo grupo de NAT usa o endereço IP privado do QRadar Console para comunicação. Qualquer host gerenciado que esteja localizado em um grupo de NAT diferente utiliza o endereço IP público do QRadar Console para comunicação.

Se você tiver um host em um desses locais do grupo de NAT, mas não requerer conversão externa, insira o endereço IP privado nos campos **IP privado** e **IP público**. Os sistemas em locais remotos com um grupo de NAT diferente do console ainda requerem um endereço IP externo e uma NAT, já que eles precisam ser capazes de estabelecer conexões com o console. Somente hosts que estejam localizados no mesmo grupo de NAT que o console podem usar os mesmos endereços IP públicos e privados.

Incluindo uma rede NAT - ativado para QRadar

Utilize o editor de implementação para incluir uma rede para sua implementação NAT - ativado QRadar.

Antes de Iniciar

Certifique-se de que você configurar suas redes NAT - ativado utilizando a conversão de NAT estático. Essa configuração assegura que as comunicações entre hosts gerenciados que existem em diferentes redes. NAT - ativado

Procedimento

1. No editor de implementação, clique no ícone **Redes NAT**.
2. Clique em **Incluir**.
3. Digite um nome para uma rede que deseja utilizar para NAT.
4. Clique em **OK**.

   A janela Gerenciar NAT Redes é exibida, incluindo o incluído NAT - ativado de rede.
5. Clique em **OK**.
6. Clique em **Sim**.

Editando uma Rede NAT - ativado

Utilizando o editor de implementação, você pode editar uma rede NAT - ativado.

Procedimento

1. No editor de implementação, clique no ícone **Redes NAT**.
2. Selecione a rede NAT - ativado que deseja editar e clique em **Editar**.
3. Digite um novo nome para a rede NAT - ativado e clique em **OK**.

   A janela Gerenciar Redes NAT mostra as redes NAT - ativado atualizadas.
4. Clique em **OK**.
5. Clique em **Sim**.

Excluindo uma Rede do NAT - ativado a Partir do QRadar

Utilize o editor de implementação para excluir uma rede do NAT - ativado a partir de sua implementação:

Procedimento

1. No editor de implementação, clique no ícone **Redes NAT**.
2. Selecione a rede do NAT - ativado que você deseja excluir.
3. Clique em **Excluir**.
4. Clique em **OK**.
5. Clique em **Sim**.

Alterando o Status NAT para um host gerenciado

Utilize o editor de implementação para alterar o status de NAT um host gerenciado em sua implementação.

Antes de Iniciar

Se você deseja ativar NAT para um host gerenciado, o NAT - ativado de rede deve estar utilizando a conversão de NAT estático.

Para alterar seu status NAT em um host gerenciado, certifique-se de atualizar a configuração do host gerenciado dentro de QRadar antes de atualizar o dispositivo. Atualizar a primeira configuração previne o host de tornar-se inalcançável e você pode implementar mudanças a esse host.

Procedimento

1. No editor de implementação, clique na guia **Visualização do Sistema**.
2. Clique com o botão direito no host gerenciado que você deseja editar e selecione **Editar host gerenciado**.
3. Clique em **Avançar**.
4. Escolha uma das seguintes opções:
   - Se necessário habilitar o NAT para o host gerenciado, selecione a caixa de seleção **Host NATed** clique em **Avançar**.
   - Se você desejar desativar NAT para o host gerenciado, limpe a caixa de opções **do host NAT**.

   Importante: Quando modificar o status NAT para um host gerenciado existente, mensagens de erro serão exibidas. Ignore essas mensagens de erro.
5. Se você habilitar o NAT, selecione uma redeNAT - ativado, e insira valores para os parâmetros:

Tabela 54. Parâmetros para um NAT - ativado de rede

Parâmetro	Descrição
Mude o IP público do servidor ou dispositivo a incluir	O gerenciador de host usa esse endereço de IP para comunicar-se com outro host gerenciado que pertence a diferentes redes usando o NAT.
Selecione a rede com NAT	Atualize a configuração de rede. NAT - ativado
Gerenciar Listas NATs –	A conversão de endereço de rede (NAT) converte um endereço IP em uma rede para um endereço IP diferente em uma outra rede. NAT fornece maior segurança para sua implementação desde que solicitações sejam gerenciadas por meio do processo de conversão e a ocultação de endereços IP internos. Para obter informações adicionais, consulte “Redes NAT - ativado” na página 158.

6. Clique em **Avançar**.
7. Clique em **Concluir**.
8. Atualizar a configuração para o dispositivo (de firewall) ao qual o host gerenciado está se comunicando.
9. Na guia/menu **Admin**, clique em **Avançado** > **Implementar Configuração Integral**.

Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Configuração do componente

Utilize o editor de implementação para configurar cada componente em sua implementação.

Configurando um QRadar QFlow Collector

Utilize o editor de implementação para configurar um QRadar QFlow Collector.

Sobre Esta Tarefa

É possível configurar um filtro de fluxo na conexão a partir de um QRadar QFlow Collector e vários QRadar Event Collectors. Um filtro de fluxo controla qual fluxo um componente recebe. O parâmetro **filtro de Fluxo** está disponível na janela Configuração da Conexão de Fluxo.

Clique com o botão direito na seta entre o componente que você deseja configurar para a filtragem de fluxo e selecione **Configurar**.

A tabela a seguir descreve os parâmetros avançados do QRadar QFlow Collector:

Procedimento

1. Na página Visualização de Eventos ou Visualização do Sistema, selecione o QRadar QFlow Collector que você deseja configurar.
2. Clique em **Ações** > **Configurar**.
3. Insira os valores para os parâmetros a seguir:

Parâmetro	Descrição
Conexões do Coletor de Eventos	O componente Coletor de eventos que está conectado a este QRadar QFlow Collector. A conexão é exibida no seguinte formato: *<Host IP Address>*:*<Port>*. Se o QRadar QFlow Collector não estiver conectado a um Coletor de eventos, o parâmetro estará vazio.
ID do Coletor de QFlow	Um ID exclusivo para o QRadar QFlow Collector.

Parâmetro	Descrição
Captura de Conteúdo Máxima	O comprimento da captura, em bytes, para anexar a um fluxo. O intervalo é de 0 a 65535. Um valor 0 desativa a captura do conteúdo. O padrão é 64 bytes. QRadar QFlow Collectors capturam um número configurável de bytes no início de cada fluxo. A transferência de grandes quantidades de conteúdo através da rede pode afetar a rede e o desempenho. Em hosts gerenciados nos quais os QRadar QFlow Collectors estão em links de alta velocidade próximos, você pode aumentar o comprimento da captura do conteúdo. **Importante:** Aumentar o comprimento da captura de conteúdo aumenta os requisitos de armazenamento em disco para dotação de disco sugerida.
Detecção Automática do Alias	A opção **Sim** permite que o QRadar QFlow Collector detecte aliases de fonte de fluxo externos. Quando um QRadar QFlow Collector recebe tráfego a partir de um dispositivo com um endereço IP, mas nenhum alias atual, o QRadar QFlow Collector tenta uma consulta reversa de DNS para determinar o nome do host do dispositivo. Se a consulta for bem-sucedida, o QRadar QFlow Collector incluirá essas informações no banco de dados e relatará estas informações para toda a sua implementação. A opção **Não** impede que o QRadar QFlow Collector detecte aliases de fontes de fluxo externos.

4. Na barra de ferramentas, clique em **Avançado** para exibir os parâmetros avançados.
5. Insira os valores para os parâmetros avançados, conforme necessário.

Tabela 55. Parâmetros Avançados do QRadar QFlow Collector:

Parâmetro	Descrição
Conexões do Coletor de Eventos	O Coletor de eventos conectado a este QRadar QFlow Collector. A conexão é exibida no seguinte formato: *<Host IP Address>:<Port>*. Se o QRadar QFlow Collector não estiver conectado a um Coletor de eventos, o parâmetro estará vazio.

Tabela 55. Parâmetros Avançados do QRadar QFlow Collector: (continuação)

Parâmetro	Descrição
Modo de Roteamento de Fluxo	A opção **0** ativa o **Modo de Distribuidor**, que permite QRadar QFlow Collectoragrupar fluxos que possuem propriedades semelhantes. A opção **1** ativa o **Modo de Fluxo**, o que impede o empacotamento de fluxos
Máximo de Captura de Dados/Pacote	O número de bytes e pacotes que você deseja que o QRadar QFlow Collector capture.
Endereço IP do Servidor de Sincronização de Tempo	O endereço IP ou o nome do host do servidor de tempo.
Período de Tempo Limite de Sincronização de Tempo	A duração de tempo que você deseja que o host gerenciado continue tentando sincronizar o tempo antes de exceder o tempo limite. O padrão é 15 minutos.
Configuração da Placa de Interface DAG Endace	Os parâmetros do Endace da placa da interface de monitoramento de rede. Para obter informações adicionais sobre a entrada necessária para este parâmetro, consulte o Website de Suporte IBM (www.ibm.com/support).
Tamanho do Buffer de Fluxo	A quantidade de memória, em MB, que você deseja reservar para armazenamento de fluxo. O padrão é 400 MB.
Número Máximo de Fluxos	O número máximo de fluxos que você deseja enviar do QRadar QFlow Collector para um Coletor de eventos.
Remover fluxos duplicados	A opção **Sim** permite que o QRadar QFlow Collector remova fluxos duplicados. A opção **Não** impede que o QRadar QFlow Collector remova fluxos duplicados.
Verificar Números de Sequência do Fluxo de Rede	**Sim** permite que o QRadar QFlow Collector verifique os números de sequência de NetFlow recebido para garantir que todos os pacotes estejam presentes e na ordem. Uma notificação é exibida se um pacote está ausente ou recebido fora da ordem.

Tabela 55. Parâmetros Avançados do QRadar QFlow Collector: (continuação)

Parâmetro	Descrição
Método de Deduplicação do Fluxo Externo	O método que você deseja utilizar para remover origens de fluxo externo duplicadas (deduplicação): • A **Origem** permite que o QRadar QFlow Collector compare as fontes de fluxo de origem. Este método compara o endereço IP do dispositivo que exportou o registro de fluxo externo atual para aquele do endereço IP do dispositivo que exportou o primeiro registro externo do fluxo específico. Se os endereços IP não corresponderem, o registro atual de fluxo externo será descartado. • A opção **Registro** permite que o QRadar QFlow Collector compare registros de fluxo externo individuais. Este método registra uma lista de cada registro de fluxo externo que é detectado por um dispositivo específico e compara cada registro subsequente para essa lista. Se o registro atual for localizado na lista, esse registro será descartado.
Janela de Transporte do Fluxo	O número de segundos antes do final de um intervalo que você deseja que fluxos unilaterais sejam mantidos até o próximo intervalo do fluxo. Esta configuração permite tempo para o lado inverso do fluxo chegar antes de ele ser relatado.

Tabela 55. Parâmetros Avançados do QRadar QFlow Collector: (continuação)

Parâmetro	Descrição
Máscara de comparação do registro do fluxo externo	• Este parâmetro é válido somente se você digitou **Registro** no parâmetro **Método de Deduplicação do Fluxo Externo**. Os campos de registro do fluxo externo que você deseja utilizar para remover fluxos duplicados incluem as seguintes opções: • **D** (direção) • **B** (ByteCount) • **P** (PacketCount) É possível combinar essas opções. As possíveis combinações das opções incluem as seguintes: • A opção **DBP** utiliza direção, contagem de bytes e contagem de pacotes quando compara registros de fluxo. • A opção **XBP** utiliza contagem de bytes e contagem de pacotes quando compara registros de fluxo. • A opção **DXP** utiliza direção e contagem de pacotes quando compara registros de fluxo. • A opção **DBX** utiliza direção e contagem de bytes quando compara registros de fluxo. • A opção **DXX** utiliza direção quando compara registros de fluxo. • A opção **XBX** utiliza contagem de bytes quando compara registros. • A opção **XXP** utiliza contagem de pacotes quando compara registros.
Criar Superfluxos	A opção **Sim** permite que o QRadar QFlow Collector crie superfluxos a partir de fluxos de grupo que possuem propriedades semelhantes. A opção **Não** impede a criação de superfluxos.

Tabela 55. Parâmetros Avançados do QRadar QFlow Collector: (continuação)

Parâmetro	Descrição
Superfluxos Tipo A	O limite para superfluxos tipo A. Um superfluxo tipo A é um grupo de fluxos a partir de um host para vários hosts. Este fluxo é um fluxo unidirecional que é um agregado de todos os fluxos que possuem hosts de destino diferentes, mas os parâmetros a seguir são iguais: • Protocolo • Bytes de Origem • Hosts de Origem • Rede de Destino • Porta de Destino (apenas fluxos de TCP e UDP) • Sinalizadores de TCP (apenas fluxos de TCP) • Tipo de ICMP e código (apenas fluxos de ICMP)
Superfluxos tipo B	O limite para superfluxos tipo B. Um superfluxo tipo B é um grupo de fluxos a partir de vários hosts para um host. Este fluxo é fluxo unidirecional que é um agregado de todos os fluxos que possuem hosts de origem diferentes, mas os parâmetros a seguir são iguais: • Protocolo • Bytes de Origem • Pacotes de Origem • Host de Destino • Rede de Origem • Porta de Destino (apenas fluxos de TCP e UDP) • Sinalizadores de TCP (apenas fluxos de TCP) • Tipo de ICMP e código (apenas fluxos de ICMP)

Tabela 55. Parâmetros Avançados do QRadar QFlow Collector: (continuação)

Parâmetro	Descrição
Superfluxos de Tipo C	O limite para superfluxos tipo C. Superfluxos tipo C são um grupo de fluxos de um host para um outro host. Este fluxo é um fluxo unidirecional que é um agregado de todos os fluxos não ICMP que possuem portas de origem ou destino diferentes, mas os parâmetros a seguir são iguais: • Protocolo • Host de Origem • Host de Destino • Bytes de Origem • Bytes de Destino • Pacotes de Origem • Pacotes de Destino
Recombinar Superfluxos Assimétricos	Em algumas redes, o tráfego está configurado para utilizar caminhos alternativos para o tráfego de entrada e de saída. Esse roteamento é chamado de roteamento assimétrico. É possível combinar os fluxos que são recebidos de um ou mais QRadar QFlow Collector. No entanto, se desejar combinar fluxos de diversos componentes do QRadar QFlow Collector, você deverá configurar fontes de fluxo no parâmetro **Interface(s) de Fonte de Fluxo Assimétrico** na configuração do QRadar QFlow Collector. • A opção **Sim** permite que o QRadar QFlow Collector recombine os fluxos assimétricos. • A opção **Não** evita que o QRadar QFlow Collector recombine fluxos assimétricos.
Ignorar Superfluxos Assimétricos	A opção **Sim** permite que o QRadar QFlow Collector criar superfluxos enquanto fluxos assimétricos são ativados. A opção **Não**impede que o QRadar QFlow Collector crie superfluxos enquanto fluxos assimétricos são ativados.
Mínimo de Dados em Buffer	A quantidade mínima de dados, em bytes, que você deseja que o Endace da placa da interface de monitoramento de rede receba antes que dados capturados sejam retornados para o processo do QRadar QFlow Collector. Se este parâmetro for 0 e nenhum dado estiver disponível, o Endace da placa da interface de monitoramento de rede permitirá o comportamento sem bloqueio.

Tabela 55. Parâmetros Avançados do QRadar QFlow Collector: (continuação)

Parâmetro	Descrição
Tempo de Espera Máximo	A quantidade máxima de tempo, em microssegundos, que você deseja que o Endace da placa da interface de monitoramento de rede aguarde pela quantidade mínima de dados. A quantidade mínima de dados é especificada no parâmetro **Mínimo de Dados em Buffer**.
Intervalo de Pesquisa	O intervalo, em microssegundos, que você deseja que o Endace da placa da interface de monitoramento de rede aguarde antes de verificar mais dados. Um intervalo de pesquisa evita tráfego de pesquisa excessivo para a placa e, portanto, preserva a largura de banda e o tempo de processamento.

6. Clique em **Salvar**.
7. Repita para todos os QRadar QFlow Collectors em sua implementação que você deseja configurar.

Conceitos relacionados:

"Visualizações de eventos dos componentes QRadar em sua implementação" na página 142

Configurando um Coletor de eventos

Utilize o editor de implementação para configurar um Coletor de eventos.

Procedimento

1. Na página Visualização de Eventos ou Visualização do Sistema, selecione o Coletor de eventos que você deseja configurar.
2. Clique em **Ações** > **Configurar**.
3. Insira os valores para os parâmetros a seguir:

Parâmetro	Descrição
Processador de Evento de Destino	Especifica o componente do Processador de eventos que está conectado a este Coletor de eventos. A conexão é exibida no seguinte formato: *<Host IP Address>:<Port>*.
Porta de Atendimento do Fluxo	A porta de atendimento para fluxos.
Porta de Atendimento de Encaminhamento de Eventos	A porta de encaminhamento de eventos do Coletor de eventos.
Porta de Atendimento de Encaminhamento de Fluxo	A porta de encaminhamento de fluxo do Coletor de eventos.

4. Na barra de ferramentas, clique em **Avançado** para exibir os parâmetros avançados.
5. Configure os parâmetros avançados, conforme necessário.

Tabela 56. Parâmetros Avançados do Coletor de eventos

Parâmetro	Descrição
Coletor Primário	**True** especifica que o Coletor de eventos está em um sistema do Console. **False** especifica que o Coletor de eventos está em um sistema diferente de Console.
Detecção Automática Ativada	**Sim** permite que o Coletor de eventos analise e aceite automaticamente o tráfego de fontes de log anteriormente desconhecidas. As portas de firewall apropriadas são abertas para ativar a Detecção Automática para receber eventos. Essa opção é a padrão. **Não** impede que o Coletor de eventos analise e aceite automaticamente o tráfego de fontes de log anteriormente desconhecidas. Para obter informações adicionais, consulte *Guia de gerenciamento de origens de log*.
Filtro de Deduplicação de Fluxo	A quantidade de tempo em segundos que os fluxos são armazenados em buffer antes de serem encaminhados.
Filtro de Fluxo Assimétrico	A quantidade de tempo em segundos em que o fluxo assimétrico é armazenado em buffer antes de ser encaminhado.
Encaminhar Eventos Já Vistos	**True** permite que o Coletor de eventos encaminhe eventos que foram detectados no sistema. **False** impede que o Coletor de eventos encaminhe eventos que foram detectados no sistema. Esta opção impede o loop de eventos em seu sistema.

6. Clique em **Salvar**.
7. Repita para todos os QRadar Event Collectors em sua implementação que você deseja configurar.

Conceitos relacionados:

"Visualizações de eventos dos componentes QRadar em sua implementação" na página 142

Configurando um Processador de eventos

Utilize o editor de implementação para configurar um Processador de eventos.

Procedimento

1. Na página Visualização de Eventos ou Visualização do Sistema, selecione o Processador de eventos que você deseja configurar.
2. Clique em **Ações** > **Configurar**.
3. Insira os valores para os parâmetros:

Tabela 57. Valores de Parâmetro para o Processador de eventos

Parâmetro	Descrição
Porta de Atendimento de Conexões do Coletor de Eventos	A porta em que o Processador de eventos monitora conexões de entrada do Coletor de eventos. O valor padrão é a porta 32005.
Porta de Atendimento de Conexões do Processador de Eventos	A porta em que o Processador de eventos monitora conexões recebidas do Processador de eventos. O valor padrão é a porta 32007.

4. Na barra de ferramentas, clique em **Avançado** para exibir os parâmetros avançados.
5. Insira os valores para os parâmetros, conforme necessário.

Tabela 58. Parâmetros Avançados do Processador de eventos

Parâmetro	Descrição
Testar Regras	A lista **Testar Regras** está disponível apenas para Processadores de Eventos não do Console. Se uma regra for configurada para testar localmente, a opção **Globalmente** não substituirá a configuração da regra. Se você selecionar **Localmente**, as regras serão testadas no Processador de eventos e não compartilhadas com o sistema. Se você selecionar **Globalmente**, regras individuais para cada Processador de eventos serão compartilhadas e testadas no sistema todo. Cada regra pode ser comutada para **Global** para detecção por qualquer Processador de eventos no sistema. Por exemplo, você pode criar uma regra para alertá-lo quando houver cinco tentativas de login com falha dentro de 5 minutos. Quando o Processador de eventos que contém a regra de local observa cinco tentativas de login com falha, a regra gera uma resposta. Se a regra no exemplo está configurada como Global, quando cinco tentativas de login com falha dentro de 5 minutos são detectadas em qualquer Processador de eventos, a regra gera uma resposta. Quando as regras são compartilhados globalmente, a regra pode detectar quando uma tentativa de login com falha vem de cinco processadores de eventos. Testar as regras globalmente é o padrão para Processador de eventos não do Console com cada regra no Processador de eventosconfigurada para testar localmente.

Tabela 58. Parâmetros Avançados do Processador de eventos (continuação)

Parâmetro	Descrição
Limite de Roteamento de Eventos de Estouro	Digite o limite de eventos por segundo que o Processador de eventos pode gerenciar. Eventos acima desse limite são colocados no cache.
Limite de Roteamento de Fluxo de Estouro	Digite o limite de fluxos por minuto que o Processador de eventos pode gerenciar. Fluxos acima desse limite são colocados no cache.
Caminho do banco de dados de eventos	Digite o local em que você deseja armazenar eventos. O padrão é **/store/ariel/events**.
Comprimento do banco de dados de cargas úteis	O local em que você deseja armazenar informações de carga útil. O padrão é **/store/ariel/payloads** .

6. Clique em **Salvar**.
7. Repita para todos os Processadores de Eventos em sua implementação que você deseja configurar.

Conceitos relacionados:

"Visualizações de eventos dos componentes QRadar em sua implementação" na página 142

Configurando o Magistrate

Utilize o editor de implementação para configurar um componente Funcionário Público.

Procedimento

1. Na página Visualização de Eventos ou Visualização do Sistema, selecione o Funcionário Público que você deseja configurar.
2. Clique em **Ações** > **Configurar**.
3. Na barra de ferramentas, clique em **Avançado** para exibir os parâmetros avançados.
4. No campo **Limite de Roteamento de Estouro**, digite o limite de eventos por segundo que o Funcionário Público pode gerenciar.

   Eventos acima desse limite são colocados no cache.

   O padrão é 20.000.
5. Clique em **Salvar**.

Conceitos relacionados:

"Visualizações de eventos dos componentes QRadar em sua implementação" na página 142

Configurando uma Origem Externa

Utilize o editor de implementação para configurar uma origem externa.

Sobre Esta Tarefa

Para evitar erros de conexão, quando você configurar os componentes de origem e destino externos, implemente o QRadar Console com a primeira origem externa. Em seguida, implemente o QRadar Console com o destino externo.

Procedimento

1. Na página Visualização de Eventos ou Visualização do Sistema, selecione o Coletor de eventos que você deseja configurar.
2. Clique em **Ações** > **Configurar**.
3. Digite os valores de parâmetro.

Parâmetro	Descrição
Receber Eventos	**True** permite que o sistema receba eventos do host de origem externa. **False** impede que o sistema receba eventos do host de origem externa.
Receber Fluxos	**True** permite que o sistema receba fluxos a partir do host de origem externa. **falso** impede que o sistema receba fluxos a partir do host de origem externa.

4. Clique em **Salvar**.
5. Repita para todas as origens externas em sua implementação que você deseja configurar.

Conceitos relacionados:

"Visualizações de eventos dos componentes QRadar em sua implementação" na página 142

Configurando um Destino Externo

Utilize o editor de implementação para configurar um destino externo.

Sobre Esta Tarefa

Para evitar erros de conexão, quando você configurar os componentes de origem e destino externos, implemente o QRadar Console com a primeira origem externa. Em seguida, implemente o QRadar Console com o destino externo.

Procedimento

1. Na página Visualização de Eventos ou Visualização do Sistema, selecione o Coletor de eventos que você deseja configurar.
2. Clique em **Ações** > **Configurar**.
3. Insira os valores para os parâmetros:

Parâmetro	Descrição
Porta de Atendimento do Coletor de Eventos	A porta de atendimento do Coletor de eventos para receber dados do evento. A porta padrão para eventos é 32004.
Porta de Atendimento do Coletor de Fluxo	A porta de atendimento do Coletor de eventos para receber dados de fluxo. A porta padrão para os fluxos é 32000.

4. Clique em **Salvar**.

Conceitos relacionados:

"Visualizações de eventos dos componentes QRadar em sua implementação" na página 142

Capítulo 12. Gerenciamento de fonte de fluxos

Use a janela Fontes de Fluxos para gerenciar as fontes de fluxos em sua implementação.

É possível incluir, editar, ativar, desativar ou excluir fontes de fluxos.

Conceitos relacionados:

Capítulo 12, “Gerenciamento de fonte de fluxos”
Use a janela Fontes de Fluxos para gerenciar as fontes de fluxos em sua implementação.

Fontes de Fluxo

Para IBM Security QRadar dispositivos, IBM Security QRadar SIEM automaticamente são adicionados fonte de fluxos para portas físicas no dispositivo. QRadar SIEM também incluem uma fonte de fluxo padrãoNetFlow.

Se QRadar SIEM for instalado em seu próprio hardware, QRadar SIEM tentará automaticamente detectar e incluir origens de fluxo padrão para quaisquer dispositivos físicos, como uma placa de interface de rede (NIC). Além disso, quando você designar um QRadar QFlow Collector, QRadar SIEM inclui um padrão, NetFlow e fluxo de origem.

Com o QRadar SIEM é possível integrar fontes de fluxo.

Fluxo de fontes são classificados como, interna ou externa:

fontes de fluxo internos
Inclui qualquer hardware adicional que são instalados em um host gerenciado, como uma placa da interface de rede (NIC). Dependendo da configuração de hardware do host gerenciado, o fluxo interno de origens podem incluir as seguintes origens:

- Placa da interface de rede
- Endace da placa da interface de monitoramento de rede
- Interface Napatech

fluxo de origens externas
Não inclui nenhum fluxo de origens externas que enviam os fluxos de mensagens para o QRadar QFlow Collector. Se o QRadar QFlow Collector recebe várias origens de fluxo, você pode atribuir cada fonte de fluxo um nome distinto. Quando o fluxo de dados externos é recebido pelo mesmo QRadar QFlow Collector, um nome distinto ajuda a distinguir os dados de origem de fluxo externo uns dos outros.

fluxo de origens externas pode incluir as seguintes origens:

- NetFlow
- IPFIX
- sFlow
- J-Flow
- Packeteer
- Flowlog arquivo

QRadar SIEM pode encaminhar fluxos de dados externos de origem utilizando o spoofing ou não spoofing de método:

Spoofing

Reenvia os dados de entrada que é recebida a partir de fontes de fluxo para um destino secundário. Para garantir que os dados de origem de fluxo são enviadas para um destino secundário, configure o parâmetro **Interface de Monitoramento** na configuração de fonte de fluxo para a porta na qual os dados são recebidos (porta de gerenciamento). Quando você utiliza uma interface específica, o QRadar QFlow Collector utiliza uma captura de modo promíscuo para obter dados de fonte de fluxo, em vez de a porta de atendimento do UDP padrão na porta 2055. Como resultado, QRadar QFlow Collector pode capturar os pacotes fonte de fluxo e redirecionar os dados.

Não-Spoofing

Para não spoofing de método, configure o parâmetro **Interface de Monitoramento** na configuração de fonte de fluxo como `Quaisquer`. O QRadar QFlow Collector abre a porta de atendimento, que é a porta que está configurado como o **de Monitoramento de Porta** para aceitar dados da origem do fluxo. Os dados são processadas e encaminhados para outro destino de fonte de fluxo. O endereço de IP de origem no fna fonte de fluxo torna o endreço de do sistema QRadar SIEM, não o roteador original que enviou os dados.

NetFlow

NetFlow é uma tecnologia proprietária de contabilidade que é desenvolvida pela Cisco Systems. NetFlow monitora os fluxos de tráfego por meio de um comutador ou roteador, interpreta o cliente, servidor, o protocolo e a porta que é utilizada, conta o número de bytes e pacotes, e envia esses dados para um coletor. NetFlow

O processo de envio de dados do NetFlow é, geralmente referida ao exportador de dados NetFlow(NDE). É possível configurar o IBM Security QRadar SIEM para acessar os NDEs e assim, tornar o NetFlow um coletor. QRadar SIEMsuporte NetFlow versões 1, 5, 7, e 9. Para obter informações adicionais em NetFlow,consulte o web site Cisco (http://www.cisco.com).

Enquanto expandir a NetFlowquantia de rede que é monitorada, NetFlow use uma conexão de baixo protocolo (UDP) para entregar NDEs. Após um NDE ser enviado a partir de um comutador ou roteador, o NetFlow registro será limpo. Como UDP é utilizado para enviar estas informações e não garante o fornecimento dos dados, NetFlow inexacta a gravação de registros e recursos de alerta reduzida. Apresentações inexatas de ambos os volumes de tráfego e fluxos bidirecionais podem resultar.

Quando você configura uma fonte de fluxo externo para NetFlow, você deve executar as seguintes tarefas:

- Certifique-se de que as regras de firewall apropriadas estejam configuradas. Se você alterar seu parâmetro **Porta de Monitoramento de Fonte de Fluxo Externo** na configuração QRadar QFlow Collector, você também deverá atualizar a sua configuração de acesso do firewall.
- Certifique-se de que as portas apropriadas são configurados para seu QRadar QFlow Collector.

Se você estiver utilizando a versão NetFlow 9, certifique-se de que o NetFlow modelo do NetFlow de origem inclui os seguintes campos:

- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES ou OUT_BYTES
- IN_PKTS ou OUT_PKTS
- TCP_FLAGS (apenas fluxos de TCP)

Conceitos relacionados:

Capítulo 11, “Editor de implementação”, na página 139
Use o editor de implementação para gerenciar os componentes individuais do seu QRadar. Após a configuração de sua implementação, é possível acessar e configurar os componentes individuais de cada host gerenciado em sua implementação.

IPFIX

O protocolo da internet de Fluxo de informações de exportação (IPFIX) é uma tecnologia de contabilidade. IPFIX monitora os fluxos de tráfego por meio de um comutador ou roteador, interpreta o cliente, o servidor, o protocolo e a porta que é utilizada, conta o número de bytes e pacotes, e envia esses dados para um coletor IPFIX.

IBM Security Network Protection XGS 5000, uma nova geração de sistema de proteção e intrusão (IPS), e um exemplo de dispositivo que envia fluxo de dados em um formato IPFIX.

O processo de envio de dados IPFIX é freqüentemente referido como um Exportar Dados NetFlow (NDE). IPFIX providencia mais fluxos de informação, mais fundos na percepção do que o NetFlow v9. Você pode aceitar configurar o IBM Security QRadar SIEM para NDEs e, portanto, se tornar um coletor IPFIX. IPFIX utiliza o UDP (User Datagram Protocol) para entregar NDEs. Após um NDE ser enviado a partir do dispositivo de redirecionamento IPFIX, o registro IPFIX pode ser limpo.

Para configurar o QRadar SIEM para aceitar o fluxo do tráfego IPFIX, você deve incluir um NetFlow fluxo de origem. A NetFlow fonte de fluxo processa os fluxos IPFIX mensagens usando o mesmo processo.

O fluxo de orígem QRadar SIEM do sistema pode incluir um padrão NetFlow; portanto, você não pode ser requisitado a configurar um NetFlow fluxo de origem. Para confirmar que o seu sistema inclui um NetFlow fluxo de origem padrão, selecione as fontes de fluxo **Admin** > . Se **default_Netflow** está listado na lista de fonte de fluxo, IPFIX já está configurado.

Ao configurar uma fonte de fluxo externo para IPFIX, você deve executar as seguintes tarefas:

- Certifique-se de que as regras de firewall apropriadas estejam configuradas. Se você alterar seu parâmetro **Porta de Monitoramento de Fonte de Fluxo Externo** na configuração QRadar QFlow Collector, você também deverá atualizar a sua

configuração de acesso do firewall. Para obter informações adicionais sobre a configuração QRadar QFlow Collector , consulte o *Guia de Administração do IBM Security QRadar SIEM*.

- Assegure-se de que as portas apropriadas são configurados para seu QRadar QFlow Collector.
- Verifique se o modelo IPFIX da origem IPFIX inclui os seguintes campos:
- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES ou OUT_BYTES
- IN_PKTS ou OUT_PKTS
- TCP_FLAGS (apenas fluxos de TCP)

sFlow

sFlow é um multi-vendor e de usuário padrão para a amostragem tecnologia que permite o monitoramento contínuo do nível de aplicação dos fluxos de tráfego em todas as interfaces simultaneamente.

Um sFlow combina os contadores de interface e amostras de fluxo em datagramas sFlow que são enviados pela rede para um coletor sFlow. IBM Security QRadar SIEM sFlow suporta versões 2, 4, e 5. o tráfego sFlow é baseado em dados de amostra e, portanto, não pode representar todo o tráfego de rede. Para obter mais informações, veja o website do sFlow (www.sflow.org).

sFlow utiliza uma conexão sem o protocolo (UDP). Quando os dados são enviados a partir de um comutador ou roteador, o registro sFlow é limpo. A UDP é usada para enviar essas informações e não garantem a entrega de dados, sFlow registra gravação imprecisa e reduzida, alertando capacidades. Apresentações inexatas de ambos os volumes de tráfego e fluxos bidirecionais podem resultar.

Ao configurar uma fonte de fluxo externo para sFlow, você deve executar as seguintes tarefas:

- Certifique-se de que as regras de firewall apropriadas estejam configuradas.
- Certifique-se de que as portas apropriadas são configurados para seu QRadar VFlow Collector.

J-Flow

Uma tecnologia de contabilidade proprietário usado pelo Juniper Networks que permite que você colete estatísticas do fluxo de tráfego IP. J-Flow permite que você exporte dados para uma porta UDP em um coletor J-Flow. Utilizando J-Flow, você também pode ativar J-Flow em um roteador ou interface para coletar estatísticas de rede para locais específicos em sua rede. Observe que o tráfego J-Flow é baseado em dados de amostra e, portanto, não pode representar todo o tráfego de rede. Para obter informações adicionais sobre J-Flow, consulte o Website Juniper Networks (www.juniper.net).

J-Flow utiliza uma conexão sem o protocolo (UDP). Quando os dados são enviados a partir de um comutador ou roteador, o registro J-Flow está limpo. Como UDP é utilizado para enviar estas informações e não garante o fornecimento dos dados, J-Flow imprecisos a gravação de registros e recursos de alerta reduzido. Isto pode resultar em apresentações impreciso de ambos os volumes de tráfego e fluxos bidirecionais.

Ao configurar uma fonte de fluxo externo para J-Flow, você deve:

- Certifique-se de que as regras de firewall apropriadas estejam configuradas.
- Certifique-se de que as portas apropriadas são configurados para o Coletor de QFlow.

Packeteer

Packeteerdispositivos da coleta, agregam e armazenam dados de desempenho da rede. Depois de configurar uma fonte de fluxo externo para Packeteer, é possível enviar informações do fluxo a partir de um dispositivo para Packeteer IBM Security QRadar SIEM.

Packeteerutilizam uma conexão sem protocolo (UDP). Quando os dados são enviados a partir de um comutador ou roteador, o registro será limpo. Packeteer Como UDP é utilizado para enviar essas informações e não garante o fornecimento dos dados, Packeteer inexacta a gravação de registros e recursos de alerta reduzidos. Apresentações inexatas de ambos os volumes de tráfego e os fluxos bidirecionais podem ocorrer.

Para configurar Packeteer como uma fonte de fluxo externa, é necessário executar as seguintes tarefas:

- Certifique-se de que as regras de firewall apropriadas estejam configuradas.
- Certifique-se de que você configurar dispositivos para exportar registros de fluxo detalhe Packeteer e configure o QRadar QFlow Collector como o destino para a exportação de dados.
- Certifique-se de que as portas apropriadas são configurados para seu QRadar QFlow Collector.
- Assegure-se que a ID da classe dos dispositivos Packeteer d sejam automaticamente detectadas peloQRadar QFlow Collector.
- Para obter informações adicionais, consulte o *de mapeamento Technical Note aplicativos em Packeteer QRadar* .

Arquivo flowlog

Um arquivo flowlog é gerado do fluxo de log do IBM Security QRadar SIEM.

Interface Napatech

Se um adaptador de rede for instalado Napatech em seu sistema IBM Security QRadar SIEM a opção **Interface Napatech** é exibida como pacote baseado em fonte de fluxo na interface de usuário QRadar SIEM. O adaptador de rede Napatech fornece a próxima geração de rede programável inteligente e adaptável para sua rede. Para obter informações adicionais, consulte a documentação do Napatech .

Incluindo ou Editando uma fonte de fluxo

Utilize a janela de Fluxo de Origem para incluir uma fonte de fluxo.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. No menu de navegação, clique em **Fluxos**.
4. Clique em **Fontes de Fluxo**.
5. Execute uma das ações a seguir:
   - Para incluir uma origem de fluxo, clique em **Incluir** .
   - Para editar uma origem de fluxo, selecione a fonte de fluxo e clique em **Editar**.
6. Para criar esta fonte de fluxo a partir de uma fonte de fluxo existente, selecione a opção **Construir a partir do fluxo de origem existentes** caixa de opções e selecione uma fonte de fluxo a partir da lista **Utilize como Modelo**.
7. Insira o nome para o **de Fonte de Fluxo de Name**.

   Dica: Se a origem do fluxo externo for um dispositivo físico, use o nome do dispositivo como nome de fonte de fluxo. Se a origem do fluxo não é um dispositivo físico, utilize um nome reconhecível.
   Por exemplo, se você quiser utilizar o tráfego IPFIX, digite **ipf1**. Se desejar utilizar o tráfego NetFlow, digite **nf1**.
8. Selecione uma origem de fluxo de lista **Fluxo de tipo de origem**e configure as propriedades.
   - Se você selecionar a opção **de Flowlog de Arquivo** , assegure que você configure o local do arquivo Flowlog para o parâmetro **Caminho do Arquivo de Origem** .
   - Se você selecionar as opções **JFlow**, **Netflow**, **Packeteer FDR**ou **sFlow** no parâmetro **Fluxo de tipo de origem**,assegure que você está configurando uma porta disponível para o parâmetro **Monitoramento de Porta**.

     O padrão de porta para a primeira NetFlow fonte de fluxo é aquela configurada em sua rede como 2055 Para cada fluxo de orígem adicional NetFlow, o número da porta padrão é incrementado por 1. Por exemplo, o NetFlow fluxo de origem padrão para o segundo fluxo de origem é 2056. NetFlow
   - Se você selecionar a opção **Napatech Interface** , digite o **Interface de Fluxo de** que você deseja atribuir à origem de fluxo.

     Restrição: O **Napatech Interface** opção é exibida somente se você tiver instalado o Napatech Network Adapter em seu sistema.
   - Se você selecionar a opção **Network Interface** , para a configuração de **Interface de Fluxo** , apenas uma origem de log para cada interface Ethernet.

     Restrição: Não é possível enviar fluxo de tipos diferentes para a mesma porta.
9. Se o tráfego na rede é configurado para ter caminhos alternativos para o tráfego de entrada e de saída, selecione a caixa de opções **Ativar Fluxos Assimétricos** .
10. Clique em **Salvar**.
11. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Ativando e Desativando uma Fonte de Fluxo

Utilizando a janela Fonte de Fluxo, é possível ativar ou desativar uma fonte de fluxo.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. No menu de navegação, clique em **Fluxos**.
4. Clique no ícone **Fontes de Fluxo**.
5. Selecione a fonte de fluxo que você deseja ativar ou desativar.

   A coluna **Ativado** indica se a fonte de fluxo está ativada ou desativada.

   Os seguintes status são exibidos:
   - True indica que a fonte de fluxo está ativada.
   - False indica que a fonte de fluxo está desativada agora.
6. Clique em **Ativar/Desativar**.
7. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Excluir uma Fonte de Fluxo

Utilize a janela Fonte de Fluxo para excluir uma fonte de fluxo.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. No menu de navegação, clique em **Fluxos**.
4. Clique em **Fontes de Fluxo**.
5. Selecione a fonte de fluxo que deseja excluir.
6. Clique em **Excluir**.
7. Clique em **OK**.
8. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Fluxo de origem de aliases de gerenciamento

Você pode utilizar a janela Fonte de fluxo de Alias para configurar nomes virtuais, ou aliases, para seu fluxo de fontes.

Você pode identificar várias origens que são enviadas para o mesmo QRadar QFlow Collector , utilizando o endereço IP de origem e nome virtual. Com um alias, uma QRadar QFlow Collector pode identificar exclusivamente e o processamento de origens de dados que são enviadas para a mesma porta.

Quando QRadar QFlow Collector recebe tráfego de um dispositivo que possui um endereço IP, mas não tem um alias atual, o QRadar QFlow Collector tenta uma consulta DNS reversa. A consulta é utilizada para determinar o nome do host do dispositivo. Se a consulta for bem-sucedida, o QRadar QFlow Collector inclui essas informações no banco de dados e relata as informações para todos os componentes em sua implementação. QRadar QFlow Collector

Utilize o editor de implementação para configurar o QRadar QFlow Collector para detectar automaticamente os aliases de fonte de fluxo.

Incluindo um alias da fonte de fluxo.

Use a janela Alias da fonte de fluxo para incluir um alias da fonte de fluxo.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. No menu de navegação, clique em **Fluxos**.
4. Clique no ícone **Aliases de Fonte de Fluxo**.
5. Execute uma das ações a seguir:
   - Para incluir um alias da fonte de fluxo, clique em **Incluir** e digite os valores para os parâmetros.
   - Para editar um alias da fonte de fluxo existente, selecione o alias da fonte de fluxo, clique em **Editar** e atualize os parâmetros.
6. Clique em **Salvar**.
7. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Excluindo um Alias de Fonte de Fluxo

Utilize a janela Alias de Fonte de Fluxo para excluir um alias de fonte de fluxo.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. No menu de navegação, clique em **Fluxos**.
4. Clique no ícone **Aliases de Fonte de Fluxo**.
5. Selecione o alias de fonte de fluxo que você deseja excluir.
6. Clique em **Excluir**.
7. Clique em **OK**.
8. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Capítulo 13. Configuração de rede remota e serviços.

Utilize a rede remota e grupos de serviço para representar a atividade de tráfego em sua rede para um perfil específico. Grupos de redes remotas exibem o tráfego do usuário que se origina de redes remoto nomeado.

Todos os grupos de rede remota e grupo de serviços têm grupos de serviços e níveis de foha de objetos. É possível editar a rede remota e grupos de serviços ao incluir objetos em grupos existentes ou alterando as propriedades pré-existentes para adequar ao seu ambiente.

Se um objeto existente for movido para outro grupo, o nome do objeto é movido do grupo existente para o grupo recém-selecionado. No entanto, quando as alterações de configuração são implementadas, os dados do objeto que está armazenado no banco de dados for perdida e o objeto deixa de funcionar. Para resolver esse problema, crie uma nova visualização e recrie o objeto que existe com outro grupo.

Na guia **Admin**, é possível agrupar remoto de redes e serviços para uso no mecanismo de regras customizadas, fluxo e procuras de eventos. É possível também agrupar as redes e serviços em IBM Security QRadar Risk Manager, se estiver disponível.

Grupos de rede remota padrão

IBM Security QRadar SIEMIncluem grupos de rede remota padrão:

As tabelas a seguir descrevem os grupos de redes remotas padrão

Tabela 59. Grupos de rede remota padrão

Grupo	Descrição
BOT	Especifica o tráfego que se origina a partir de aplicativos BOT.
Bogon	Especifica o tráfego proveniente de endereços IP não-designado. Para obter informações adicionais, consulte a referência bogon no website Team CYMRU (http://www.team-cymru.org/Services/Bogons).
HostileNets	Especifica o tráfego que origina-se de redes nocivas conhecidas. Os HostileNets têm uma configuração de 20 (rank 1 - 20 inclusive) faixas CIDR configuráveis.
Vizinhos	Este grupo fica em branco por padrão. Você deve configurar esse grupo para classificar o tráfego que se origina de redes vizinhas.

Tabela 59. Grupos de rede remota padrão (continuação)

Grupo	Descrição
Smurfs	Especifica o tráfego que se origina de ataques de smurf. Um ataque smurf é um tipo de ataque de negação que inunda um sistema da destino com transmissão falsa de mensagens ping.
Superflows	Esse grupo é não configurável. Um superflow é um fluxo que seja um agregado de um número de fluxos de mensagens que possuem um conjunto de elementos semelhantes predeterminado.
TrustedNetworks	Este grupo fica em branco por padrão. Você deve configurar esse grupo para classificar o tráfego que se origina de redes confiáveis.
Watchlists	Este grupo fica em branco por padrão. Você pode configurar esse grupo para classificar o tráfego que se origina de redes que deseja monitorar.

Grupos e objetos que incluem superflows são apenas para fins informativos e não pode ser editado. Grupos e objetos que incluem bogons são configurados pela função de atualização automática.

Padrão de grupos de serviço remoto

IBM Security QRadar SIEM incluem os grupos de serviço remoto padrão.

A tabela a seguir descreve os grupos padrões de serviço remoto.

Tabela 60. Grupos de rede remota padrão

Parâmetro	Descrição
IRC_Servers	Especifica o tráfego que se origina de endereços comumente conhecido como servidores de bate-papo.
Serviços_Online	Especifica origina a partir de endereços online comumente conhecido que o tráfego de serviços que podem envolver a perda de dados.
pornografia	Especifica o tráfego que se origina de endereços explícito comumente conhecido para conter material pornográfico.
Proxies	Especifica trafego que é originado dos servidores de proxy conhecidos comumente abertos.
Reserved_IP_ Intervalos	Especifica o tráfego que se origina em intervalos de endereços IP reservado.

Tabela 60. Grupos de rede remota padrão (continuação)

Parâmetro	Descrição
Spam	Especifica o tráfego que se origina comumente conhecido para produzir SPAM ou endereços de email indesejadas.
Spy_Adware	Especifica o tráfego que se origina de spyware ou adware comumente conhecido para conter endereços.
Superflows	Especifica o tráfego originado de endereços comumente conhecido para produzir que superflows.
Warez	Especifica o tráfego que se origina de endereços comumente conhecido para conter software pirateados.

Recomendações para recursos de rede

Dar as complexibilidades e recursos de rede que são solicitadas pelo IBM Security QRadar SIEM em grandes redes de estruração, siga as orientações sugeridas.

A lista a seguir descreve algumas das práticas que podem ser seguidas:

- Use Objetos do pacote configurável e as guias **Atividade de rede** e **Atividade de log** para analizar a sua rede. data.

  Poucos objetos criam menos entrada/saída em seu disco.
- Normalmente, para requirimentos do sistema padrão, não exceda mais de 200 objetos por grupo.

  Mais objetos devem impactar a energia de processo quando você investigar seu trafego.

Gerenciando objetos redes remotas

Depois de criar grupos de rede remota, é possível agregar resultados da procura de fluxo e eventos no grupo de rede remora. Você também pode criar regras que testam a atividade em grupos de rede remota.

Utilize a janela de Redes Remotas, onde é possível incluir ou editar um objeto redes remotas.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração de Redes e Serviços Remotos**.
3. Clique no ícone **Networks Remoto**.
4. Para incluir um objeto redes remotas, clique em **Incluir** e digite valores para os parâmetros.
5. Para editar objeto redes remotas, clique no grupo que você deseja que sejam exibidas, clique em **Editar**e, em seguida, alterar os valores.
6. Clique em **Salvar**.
7. Clique em **Retornar**.
8. Feche a janela Networks Remoto.
9. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Gerenciando objetos de serviços remotos

organizar grupos de serviços que se originam de intervalos de tráfego de rede remota definidos pelo usuário ou o servidor de atualização automática do IBM. Depois de criar grupos de serviço remoto, será possível agregar fluxo e resultados da procura de eventos, e criar regras que testam a atividade em grupos de serviço remoto.

Utilize a janela Remote Services para incluir ou editar um objeto serviços remotos.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração de Redes e Serviços Remotos**.
3. Clique no ícone **Remote Services**.
4. Para incluir um objeto serviços remotos, clique em **Incluir** e digite os valores de parâmetro.
5. Para editar um objeto serviços remotos, clique no grupo que você deseja exibir, clique no ícone **Editar** e alterar os valores.
6. Clique em **Salvar**.
7. Clique em **Retornar**.
8. Feche a janela Remote Services.
9. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Visão geral do mapa QID

Use o utilitário de mapa QRadar Identifier (QID) para criar, exportar, importar ou modificar entradas de mapa QID definidas pelo usuário.

O mapa QID associa um evento em um dispositivo externo a um (QID).

Veja as seguintes tarefas para gerenciamento do QID:

- "Criando uma entrada de mapa QID" na página 187
- "Modificando uma entrada de mapa QID" na página 187
- "Importando entradas do mapa Qid" na página 188
- "Exportando as entradas do mapa QID" na página 189

Para executar o utilitário, utilize a seguinte sintaxe:

```
qidmap_cli.sh [-l|-c|-m|-i[-f <filename>]|-e[-f <filename>]|-d]
```

A tabela a seguir descreve as opções da linha de comandos para o utilitário de mapa QID.

Tabela 61. Opções de utilitário de mapa QID

Opções	Descrição
-l	Lista a categoria de nível inferior.
-c	Cria uma entrada de mapa QID
-m	Modifica uma entrada de mapa QID existente definida pelo usuário.
-i	Importa entradas de mapa QID.

Tabela 61. Opções de utilitário de mapa QID (continuação)

Opções	Descrição
-e	Exporta entradas de mapa QID existentes definidas pelo usuário.
-f <filename>	Se você incluir a opção -i ou -e, especifica um nome de arquivo para importar ou exportar as entradas de mapa QID.
-d	Se você incluir a opção -i ou -e, especifica um delimitador para o arquivo de importação ou exportação. O padrão é uma vírgula.
-h	Exibe as opções de ajuda.

Criando uma entrada de mapa QID

Crie uma Entrada de Mapa QRadar Identifier (QID) para mapear um evento de um dispositivo externo para QID.

Procedimento

1. Usando o SSH, efetue login no QRadar como o usuário raiz.
2. Para localizar a categoria de nível inferior para a entrada de mapa QID que você deseja criar, digite o seguinte comando:

   ```
   /opt/qradar/bin/qidmap_cli.sh -l
   ```

   Se você deseja procurar uma categoria de nível inferior específica, é possível usar o comando `grep` para filtrar os resultados:

   ```
   /opt/qradar/bin/qidmap_cli.sh -l | grep <text>
   ```

3. Digite o comando a seguir:

   ```
   qidmap_cli.sh -c --qname <name> --qdescription <description>
   --severity <severity> --lowlevelcategoryid <ID>
   ```

   A tabela a seguir descreve as opções da linha de comandos para o utilitário de mapa QID:

Opções	Descrição
-c	Cria uma entrada de mapa QID.
--qname <name>	O nome que você deseja associar a esta entrada de mapa QID. O nome pode ter até 255 caracteres de comprimento, sem espaços.
--qdescription <description>	A descrição para esta entrada de mapa QID. A descrição pode ter até 2048 caracteres de comprimento sem espaços.
--severity <severity>	O nível de severidade que você deseja designar a esta entrada de mapa QID. O intervalo válido é de 1 a 10.
--lowlevelcategoryid <ID>	O ID da categoria de nível inferior que você deseja designar a esta entrada de mapa QID. Para obter mais informações, consulte o Guia de Administração QRadar.

Modificando uma entrada de mapa QID

Modifique uma entrada de mapa QRadar Identifier (QID) existente definida pelo usuário.

Procedimento

1. Usando o SSH, efetue login no QRadar como o usuário raiz.
2. Digite o comando a seguir:

```
qidmap_cli.sh -m --qid<QID> --qname <name> --qdescription <description>
--severity <severity>
```

A tabela a seguir descreve as opções da linha de comandos para o utilitário de mapa QID:

Opções	Descrição
-m	Modifica uma entrada de mapa QID existente definida pelo usuário.
--qid<QID>	O QID que deseja modificar.
--qname <name>	O nome que você deseja associar a esta entrada de mapa QID. O nome pode ter até 255 caracteres de comprimento sem espaços.
--qdescription <description>	A descrição para esta entrada de mapa QID. A descrição pode ter até 2048 caracteres de comprimento sem espaços.
--severity <severity>	O nível de severidade que você deseja designar a esta entrada de mapa QID. O intervalo válido é 0-10.

Importando entradas do mapa Qid

Usando o utilitário de mapa QRadar Identifier (QID), é possível importar entradas de mapa QID de um arquivo .txt.

Procedimento

1. Crie um arquivo `.txt` que inclua as entradas de mapa QID definidas pelo usuário que você deseja importar. Certifique-se de que cada entrada no arquivo seja separada por uma vírgula. Escolha uma das seguintes opções:
   - Se você deseja importar uma nova lista de entradas de mapa QID definidas pelo usuário, crie o arquivo com o seguinte formato para cada entrada:

     ```
     ,<name>,<description>,<severity>,<category>
     ```

     Exemplo:

     ```
     ,buffer,buffer_QID,7,18401 ,malware,malware_misc,8,18403
     ```
   - Se você deseja importar uma lista existente de entradas de mapa QID definidas pelo usuário, crie o arquivo com o seguinte formato para cada entrada:

     ```
     <qid>,<name>,<description>,<severity>
     ```

     Exemplo: `2000002,buffer,buffer_QID,7 2000001,malware,malware_misc`

   A tabela a seguir descreve as opções de linha de comandos do utilitário QID.

Opções	Descrição
<qid>	O QID existente para a entrada. Essa opção será requerida se você quiser importar uma lista exportada existentes de entradas QID. Para importar novas entradas QID, não use essa opção. O utilitário de mapa QID designa um identificador (QID) para cada entrada no arquivo.

Opções	Descrição
--qname <name>	O nome que você deseja associar a esta entrada de mapa QID. O nome pode ter até 255 caracteres de comprimento sem espaços.
--qdescription <description>	A descrição para esta entrada de mapa QID. A descrição pode ter até 2048 caracteres de comprimento sem espaços.
--severity <severity>	O nível de severidade que você deseja designar a esta entrada de mapa QID. O intervalo válido é 0-10.
--lowlevelcategoryid <ID>	O ID da categoria de nível inferior que você deseja designar a esta entrada de mapa QID. Essa opção é necessária apenas se você deseja importar uma nova lista de entradas QID.

2. Salve e feche o arquivo.
3. Usando SSH, efetue login no QRadar como usuário raiz:
4. Para importar o arquivo de mapa QID, digite o seguinte comando:

   ```
   /opt/qradar/bin/qidmap_cli.sh -i -f
   <filename.txt>
   ```

   A opção *<filename.txt>* é o caminho do diretório e o nome do arquivo que contém as entradas de mapa QID. Se qualquer uma das entradas no arquivo causar um erro, nenhuma entrada no arquivo será aplicada.

Exportando as entradas do mapa QID

Usando o utilitário de mapa QRadar Identifier (QID), é possível exportar entradas de mapa QID definidas pelo usuário para um arquivo `.txt` .

Procedimento

1. Usando o SSH, efetue login no QRadar como o usuário raiz.
2. Para exportar o arquivo de mapa QID, digite o seguinte comando:

   ```
   /opt/qradar/bin/qidmap_cli.sh -e -f
   <filename.txt>
   ```

   A opção *<filename.txt>* é o caminho do diretório e o nome do arquivo que você deseja que contenha as entradas do mapa QID.

Capítulo 14. Descoberta do servidor

A função **Descoberta do Servidor** usa o ativo banco de dados do perfil para descobrir deferentes tipos de servidores que são baseados em definições de portas. Assim, é possível selecionar os servidores para adicionar um servidor-tipo building blocks para regras.

A função **Descobrindo Servidores**é baseada em servidores-tipo building block. Portas são usadas para definir o tipo de servidor. Desta forma, o servidor tipo building block trabalha como filtro port-based quando você busca pelo banco de dados perfil de recurso.

Para mais informações sobre building blocks, consulte o *IBM Security QRadar SIEM Users Guide*.

Descobrindo Servidores

Utilize a guia **Ativos** para descobrir servidores em sua rede.

Procedimento

1. Clique na guia **Ativos**
2. No menu de navegação, clique em **Descoberta do Servidor**.
3. Na lista **Tipo de Servidor**, selecione o tipo de servidor que você deseja descobrir.
4. Selecione uma das seguintes opções para determinar os servidores que você deseja descobrir:
   - Para utilizar o **Tipo de Servidor** atualmente selecionado para procurar todos os servidores em sua implementação, selecione **Todos**.
   - Para procurar servidores em sua implementação que foram designados para o **Tipo de Servidor** atualmente selecionado, selecione **Designados**.
   - Para procurar servidores em sua implementação que não estão designados, selecione **Não Designados**.
5. A partir da lista **Rede**, selecione a rede que você deseja procurar.
6. Clique em **Descobrir Servidores**.
7. Na tabela **Servidores Correspondentes**, selecione as caixas de seleção de todos os servidores que você deseja designar à função de servidor.
8. Clique em **Aprovar Servidores Selecionados**.

Capítulo 15. Segmentação de domínio

A segmentação da rede em domínios diferentes ajuda a assegurar que informações relevantes estejam disponíveis apenas para os usuários que precisam delas.

Você pode criar perfis de segurança para limitar as informações que estão disponíveis para um grupo de usuários dentro desse domínio. Os perfis de segurança fornecem aos usuários autorizados acesso apenas às informações que são necessárias para concluir suas tarefas diárias. Você modifica apenas o perfil de segurança dos usuários afetados e não cada usuário individualmente.

É possível também usar domínios para gerenciar intervalos de endereço IP sobrepostos. Este método é útil quando você está usando uma infraestrutura de IBM Security QRadar compartilhada para coletar dados de várias redes. Ao criar domínios que representam um espaço de endereço particular na rede, vários dispositivos que estão em domínios separados podem ter o mesmo endereço IP e ainda ser tratados como dispositivos separados.

Endereços IP sobrepostos

Um endereço IP sobreposto é um endereço IP que é designado a mais de um dispositivo ou unidade lógica, como um tipo de fonte de evento, em uma rede. Sobrepor intervalos de IP pode causar problemas significativos para empresas que mesclam redes após aquisições corporativas ou para Managed Security Service Providers (MSSPs) que estão trazendo novos clientes.

O IBM Security QRadar deve ser capaz de diferenciar eventos e fluxos que vêm de diferentes dispositivos e que têm o mesmo endereço IP. Se o mesmo endereço IP for designado a mais de uma origem de eventos, você poderá criar domínios para distingui-los.

Por exemplo, vamos examinar uma situação em que a Empresa A adquire a Empresa B e deseja usar uma instância compartilhada do QRadar para monitorar os ativos da nova empresa. A aquisição tem uma estrutura de rede semelhante que resulta no uso do mesmo endereço IP para diferentes fontes de log em cada empresa. As fontes de log que têm o mesmo endereço IP causam problemas com correlação, relatório, procura e criação de perfil de ativo.

Para distinguir a origem dos eventos e fluxos que entram no QRadar a partir da fonte de log, você pode criar dois domínios e designar cada fonte de log a um domínio diferente. Se necessário, você pode também designar cada coletor de eventos e coletor de fluxo ao mesmo domínio que a fonte de log que envia eventos a eles.

Para visualizar os eventos recebidos pelo domínio, crie uma procura e inclua as informações de domínio nos resultados da procura.

Definição e identificação de domínio

Os domínios são definidos com base nas origens de entrada do QRadar. Quando eventos e fluxos entram no QRadar, as definições de domínio são avaliadas e os eventos e fluxos são identificados com informações de domínio.

Especificando domínios para eventos

Estas são as maneiras para especificar domínios para eventos:

Coletores de eventos
Se um coletor de eventos for dedicado a um segmento de rede específico ou a um intervalo de endereços IP, você poderá sinalizar esse coletor de eventos inteiro como parte desse domínio.

Todas as fontes de log que chegam a esse coletor de eventos pertencem ao domínio; portanto, todas as novas fontes de log detectadas automaticamente são automaticamente incluídas no domínio.

Fontes de log
É possível configurar fontes de log específicas para que pertençam a um domínio.

Este método de domínios de identificação é uma opção para implementações nas quais um coletor de eventos pode receber eventos de vários domínios.

Grupos de fontes de log
Você pode designar grupos de fontes de log a um domínio específico. Esta opção permite maior controle sobre a configuração da fonte de log.

Todas as novas fontes de log que são incluídas no grupo de fonte de log obtêm automaticamente a identificação de domínio associada ao grupo de fonte de log.

Propriedades customizadas
É possível aplicar propriedades customizadas às mensagens de log que vêm de uma fonte de log.

Para determinar a qual domínio pertencem essas mensagens de log específicas, o valor da propriedade customizada é consultado em relação a uma tabela definida pelo usuário.

Esta opção é usada para fontes de log de intervalo com vários endereços ou vários locatários, como servidores de arquivos e repositórios de documentos.

Especificando domínios para fluxos

Estas são as maneiras de especificar domínios para fluxos:

Coletores de fluxo
Você pode designar coletores QFlow específicos a um domínio.

Todas as fontes de fluxo que chegam a esse coletor de fluxo pertencem ao domínio; portanto, qualquer fonte nova de fluxo detectada automaticamente é automaticamente incluída no domínio.

Fontes de Fluxo
Você pode designar fontes de fluxo específicas a um domínio.

Esta opção é útil quando um único coletor QFlow está coletando fluxos de vários segmentos de rede ou roteadores que contêm intervalos de endereço IP sobrepostos.

Especificando domínios para resultados da varredura

Você também pode designar scanners de vulnerabilidade a um domínio específico para que os resultados da varredura sejam adequadamente sinalizados como pertencentes àquele domínio. Uma definição de domínio pode consistir em todas as origens de entrada do QRadar.

Para obter informações sobre como designar sua rede a domínios pré-configurados, consulte “Hierarquia de Rede” na página 65.

Ordem de precedência para a avaliação de critérios de domínio

Quando eventos e fluxos entram no sistema QRadar, os critérios de domínio são avaliados com base na granularidade da definição de domínio.

Se a definição de domínio for baseada em um evento, o evento recebido é primeiro verificado para ver se há alguma propriedade customizada que seja mapeada para a definição de domínio. Se o resultado de uma expressão regular definida em uma propriedade customizada não corresponder a um mapeamento de domínio, o evento será automaticamente designado ao domínio padrão.

Se o evento não corresponder à definição de domínio para propriedades customizadas, a seguinte ordem de precedência será aplicada:

1. origem do log
2. grupo de fontes de log
3. coletor de eventos

Se o domínio for definido com base em um fluxo, que está disponível apenas em implementações do QRadar SIEM, a seguinte ordem de precedência será aplicada:

1. fonte de fluxo
2. coletor de fluxo

Se um scanner tiver um domínio associado, todos os recursos descobertos pelo scanner serão automaticamente designados ao mesmo domínio que o scanner.

Encaminhando dados a outro sistema QRadar

As informações de domínio são removidas quando os dados são encaminhados a outro sistema QRadar. Eventos e fluxos que contêm informações de domínio são automaticamente designados ao domínio padrão no sistema QRadar de recebimento. Para identificar quais eventos e fluxos são designados ao domínio padrão, você pode criar uma pesquisa customizada no sistema de recebimento. Você pode querer redesignar esses eventos e fluxos a um domínio definido pelo usuário.

Criando domínios

Use a janela Gerenciamento de Domínios para criar domínios com base em origens de entrada do IBM Security QRadar.

Sobre Esta Tarefa

Use as diretrizes a seguir ao criar domínios:

- Tudo o que não é designado a um domínio definido pelo usuário é automaticamente designado ao domínio padrão. Os usuários que têm acesso de domínio limitado não devem ter privilégios administrativos porque esse privilégio concede acesso ilimitado a todos os domínios.
- Você pode mapear a mesma propriedade customizada para dois domínios diferentes, no entanto, o resultado da captura deve ser diferente para cada um.
- Você não pode designar uma origem de log, grupo de origem de log ou coletor de eventos a dois domínios diferentes. Quando um grupo de origem de log é designado a um domínio, cada um dos atributos mapeados está visível na janela Gerenciamento de Domínios.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Gerenciamento de Domínios**.
4. Para incluir um domínio, clique em **Incluir** e digite um nome exclusivo e uma descrição para o domínio.

   Dica: Você pode procurar nomes exclusivos digitando o nome na caixa de procura **Nome de domínio de entrada**.
5. Dependendo dos critérios de domínio a serem definidos, clique na guia apropriada.
   - Para definir o domínio com base em uma propriedade customizada, grupo de origem de log, origem de log ou coletor de eventos, clique na guia **Eventos**.
   - Para definir o domínio com base em uma fonte de fluxo ou coletor de fluxo, clique na guia **Fluxos**.
   - Para definir o domínio com base em um scanner, incluindo os scanners IBM Security QRadar Vulnerability Manager, clique na guia **Scanners**.
6. Para designar uma propriedade customizada a um domínio, na caixa **Resultado da Captura**, digite o texto que corresponde ao resultado do filtro de expressão regular (regex).

   Importante: Você deve marcar a caixa de seleção **Otimizar análise para regras, relatórios e procuras** na janela Propriedades de Eventos Customizados para analisar e armazenar a propriedade do evento customizado. A segmentação de domínio não ocorrerá se esta opção não estiver marcada.
7. Na lista, selecione os critérios de domínio e clique em **Incluir**.
8. Depois de incluir os itens de origem no domínio, clique em **Criar**.

O que Fazer Depois

Crie perfis de segurança para definir quais usuários têm acesso aos domínios. Depois de criar o primeiro domínio em seu ambiente, você deve atualizar os perfis de segurança para todos os usuários não administrativos para especificar a designação do domínio. Em ambientes cientes do domínio, os usuários não administrativos cujo perfil de segurança não especifica uma designação de domínio não verão nenhuma atividade de log ou de rede.

Você pode também usar a ferramenta Hierarquia de Rede para designar sua rede aos domínios pré-configurados. Para obter informações adicionais, consulte “Hierarquia de Rede” na página 65.

Privilégios de domínio que são derivados de perfis de segurança

É possível usar perfis de segurança para conceder privilégios de domínio e assegurar que as restrições de domínio sejam completamente respeitadas em todo o sistema IBM Security QRadar. Os perfis de segurança também facilitam o gerenciamento de privilégios para um grande grupo de usuários quando seus requisitos de negócios mudam repentinamente.

Os usuários podem ver dados apenas dentro dos limites de domínio que são configurados para os perfis de segurança que são designados a eles. Os perfis de segurança incluem domínios como um dos primeiros critérios avaliados para restringir o acesso ao sistema. Quando um domínio é designado a um perfil de segurança, ele tem prioridade sobre outras permissões de segurança. Depois que as restrições de domínio são avaliadas, os perfis de segurança individuais são avaliados para determinar as permissões de rede e de log para esse perfil particular.

Por exemplo, um usuário recebe privilégios para Domain_2 e acesso à rede 10.0.0.0/8. Esse usuário pode ver apenas ofensas, ativos, eventos e fluxos que vêm de Domain_2 e contêm um endereço da rede 10.0.0.0/8.

Como administrador do QRadar, você pode ver todos os domínios e pode designar domínios a usuários não administrativos. Não designe privilégios administrativos a usuários a quem você deseja limitar a um domínio particular.

Ao designar domínios a um perfil de segurança, você pode conceder acesso aos seguintes tipos de domínios:

Domínios definidos pelo usuário
Você pode criar domínios que são baseados em fontes de entrada usando a ferramenta Gerenciamento de Domínio. Para obter mais informações, consulte *Criando domínios*. Criando domínios.

Domínio padrão
Tudo o que não é designado a um domínio definido pelo usuário é automaticamente designado ao domínio padrão. O domínio padrão contém eventos de todo o sistema.

Importante: Os usuários que têm acesso ao domínio padrão podem ver eventos de todo o sistema sem restrição. Certifique-se de que esse acesso seja aceitável antes de designar acesso de domínio padrão aos usuários. Todos os administradores têm acesso ao domínio padrão.

Toda fonte de log que é descoberta automaticamente em um coletor de eventos compartilhado (um que não seja explicitamente designado a um domínio) é descoberta automaticamente no domínio padrão. Essas fontes de log requerem intervenção manual. Para identificar essas fontes de log, você deve executar periodicamente uma procura no domínio padrão que é agrupado por fonte de log.

Todos os domínios
Os usuários que são designados a um perfil de segurança que tem acesso a **Todos os Domínios** podem ver todos os domínios ativos dentro do sistema, o domínio padrão e todos os domínios que foram anteriormente excluídos em todo o sistema. Eles também podem ver todos os domínios que são criados no futuro.

Se você excluir um domínio, ele não poderá ser designado a um perfil de segurança. Se o usuário tiver a designação **Todos os domínios** ou se o domínio foi designado ao usuário antes de ele ser excluído, o domínio excluído será retornado nos resultados da procura histórica para eventos, fluxos, ativos e ofensas. Você não pode filtrar por domínios excluídos ao executar uma procura.

Os usuários administrativos podem ver quais domínios são designados aos perfis de segurança na guia **Resumo** na janela Gerenciamento de Domínio.

Modificações de regras em ambientes que reconhecem o domínio

As regras podem ser visualizadas, modificadas ou desativadas por qualquer usuário que tenha as permissões **Manter Regras Customizadas** e **Visualizar Regras Customizadas**, independentemente de a qual domínio esse usuário pertença.

Importante: Ao incluir o recurso **Atividade de log** para uma função de usuário, as permissões **Manter regras customizadas** e **Visualizar regras customizadas** são concedidas automaticamente. Os usuários que possuem essas permissões têm acesso a todos os dados do log para todos os domínios. Eles podem editar regras em todos os domínios, mesmo se suas configurações de perfil de segurança tiverem restrições de nível de domínio. Para evitar que os usuários do domínio possam acessar os dados de log e modificar regras em outros domínios, edite a função de usuário e remova as permissões **Manter Regras Customizadas** e **Visualizar Regras Customizadas**.

Procuras cientes do domínio

É possível usar domínios como critérios de procura em procuras customizadas. Seu perfil de segurança controla quais domínios você pode procurar.

Os eventos de todo o sistema e os eventos que não são designados a um domínio definido pelo usuário são automaticamente designados ao domínio padrão. Administradores, ou usuários que tenham um perfil de segurança que forneça acesso ao domínio padrão, podem criar uma procura customizada para ver todos os eventos que não são designados a um domínio definido pelo usuário.

Ofensas e regras específicas do domínio

Uma regra pode funcionar no contexto de um único domínio ou no contexto de todos os domínios. Regras cientes do domínio fornecem a opção de incluir o teste **E Domínio É**.

É possível restringir uma regra para que ela seja aplicada apenas aos eventos que estão acontecendo dentro de um domínio especificado. Um evento que tem uma identificação de domínio diferente do domínio que é configurado na regra não aciona uma resposta do evento.

Em um sistema IBM Security QRadar que não tem domínios definidos pelo usuário, uma regra cria uma ofensa e mantém a contribuição para ele cada vez que a regra é disparada. Em um ambiente ciente do domínio, uma regra cria uma nova ofensa cada vez que a regra é acionada no contexto de um domínio diferente.

Regras que funcionam no contexto de todos os domínios são mencionadas como regras de todo o sistema. Para criar uma regra de todo o sistema que testa

condições em todo o sistema, selecione **Qualquer domínio** na lista de domínios para o teste **E Domínio É**. Uma regra **Qualquer domínio** cria uma ofensa **Qualquer domínio**.

Regra de domínio único
Se a regra for uma regra stateful, os estados serão mantidos separadamente para cada domínio. Quando á regra é acionada, as ofensas são criadas separadamente para cada domínio envolvido e as ofensas são identificadas com esses domínios.

Ofensa de domínio único
A ofensa é identificada com o nome de domínio correspondente. Ela pode conter apenas eventos que são identificados com esse domínio.

Regra de todo o sistema
Se a regra for uma regra stateful, um único estado será mantido para todo o sistema e as identificações de domínio serão ignoradas. Quando a regra é executada, ela cria ou contribui para uma única ofensa de todo o sistema.

Ofensa de todo o sistema
A ofensa é identificada com **Qualquer domínio**. Ela contém apenas eventos que são identificados com todos os domínios.

A tabela a seguir fornece exemplos de regras cientes do domínio. Os exemplos usam um sistema que tem três domínios que são definidos: Domain_A, Domain_B e Domain_C.

Tabela 62. Regras cientes do domínio

Texto de domínio	Explicação	Resposta da regra
domínio é um dos seguintes: Domain_A	Procura apenas nos eventos que são identificados com `Domain_A` e ignora regras que são identificadas com outros domínios.	Cria ou contribui com uma ofensa que é identificada com `Domain_A`.
domínio é um dos seguintes: Domain_A e um teste stateful que é definido como **quando o fluxo HTTP é detectado 10 vezes em 1 minuto**	Procura apenas nos eventos que são identificados com `Domain_A` e ignora regras que são identificadas com outros domínios.	Cria ou contribui com uma ofensa que é identificada com `Domain_A`. Um único estado, um contador de fluxo HTTP, é mantido para Domain_A.
domínio é um dos seguintes: Domain_A, Domain_B	Procura apenas nos eventos que são identificados com `Domain_A` e `Domain_B` e ignora eventos que são identificados com `Domain_C`. Esta regra se comporta como duas instâncias independentes de uma regra de domínio único e cria ofensas separadas para domínios diferentes.	Para dados que são identificados com `Domain_A`, cria ou contribui com uma ofensa de domínio único que é identificada com `Domain_A`. Para dados que são identificados com `Domain_B`, cria ou contribui com uma ofensa de domínio único que é identificada com `Domain_B`.

Tabela 62. Regras cientes do domínio (continuação)

Texto de domínio	Explicação	Resposta da regra
domínio é um dos seguintes: Domain_A, Domain_B e um teste stateful que é definido como **quando o fluxo HTTP é detectado 10 vezes em 1 minuto**	Procura apenas nos eventos que são identificados com `Domain_A` e `Domain_B` e ignora eventos que são identificados com `Domain_C`. Esta regra se comporta como duas instâncias independentes de uma regra de domínio único e mantém dois estados separados (contadores de fluxo HTTP) para dois domínios diferentes.	Quando a regra detecta 10 fluxos HTTP que são identificados com `Domain_A` em um minuto, ela cria ou contribui com uma ofensa que é identificada com `Domain_A`. Quando uma regra detecta 10 fluxos HTTP que são identificados com `Domain_B` em um minuto, ela cria ou contribui com uma ofensa que é identificada com `Domain_B`.
Nenhum teste de domínio definido	Procura por eventos que são identificados com todos os domínios e cria ou contribui com ofensas em uma base por domínio.	Cada domínio independente tem ofensas que são geradas para ele, mas as ofensas não contêm contribuições de outros domínios.
Uma regra tem um teste stateful que é definido como **quando o fluxo HTTP é detectado 10 vezes em 1 minuto** e nenhum teste de domínio é definido	Procura por eventos que são identificados com `Domain_A`, `Domain_B` ou `Domain_C`.	Mantém estados separados e cria ofensas separadas para cada domínio.
domínio é um dos seguintes: Qualquer domínio	Procura por todos os eventos, independentemente de com qual domínio ele seja identificado.	Cria ou contribui com uma única ofensa de todo o sistema que é identificada com `Qualquer domínio`.
domínio é um dos seguintes: Qualquer domínio e um teste stateful que é definido como **quando o fluxo HTTP é detectado 10 vezes em 1 minuto**	Procura por todos os eventos, independentemente de com qual domínio ele seja identificado, e mantém um único estado para todos os domínios.	Cria ou contribui com uma única ofensa de todo o sistema que é identificada com `Qualquer domínio`. Por exemplo, se ele detectar 3 eventos identificados com `Domain_A`, 3 eventos identificados com `Domain_B` e 4 eventos identificados com `Domain_C` em 1 minuto, ele cria uma ofensa porque detectou 10 eventos no total.
domínio é um dos seguintes: Qualquer domínio, Domain_A	Funciona da mesma maneira que uma regra que tem **domínio é um dos seguintes: Qualquer domínio**.	Quando o teste de domínio inclui `Qualquer domínio`, qualquer domínio único listado é ignorado.

Ao visualizar a tabela de ofensa, você pode classificar as ofensas clicando na coluna **Domínio**. O **Domínio padrão** não está incluído na função de classificação, portanto, ele não aparece em ordem alfabética. No entanto, ele aparece na parte superior ou na parte inferior da lista **Domínio**, dependendo de a coluna estar classificada em ordem crescente ou decrescente. **Qualquer domínio** não aparece na lista de ofensas.

Exemplo: Designações de privilégio de domínio com base nas propriedades customizadas

Se seus arquivos de log contiverem informações que você deseja usar em uma definição de domínio, você poderá expor as informações como uma propriedade de evento customizado.

Você designa uma propriedade customizada a um domínio com base no resultado da captura. É possível designar a mesma propriedade customizada a vários domínios, mas os resultados da captura devem ser diferentes.

Por exemplo, uma propriedade de evento customizado, como `userID`, pode ser avaliada para um único usuário ou para uma lista de usuários. Cada usuário pode pertencer a apenas um domínio.

No diagrama a seguir, as fontes de log contêm informações de identificação do usuário que são expostas como uma propriedade customizada, `userID`. Os resultados da captura retornam uma lista de quatro usuários e cada usuário é designado a apenas um domínio. Neste caso, dois usuários são designados ao Domínio A e dois usuários são designados ao Domínio B.

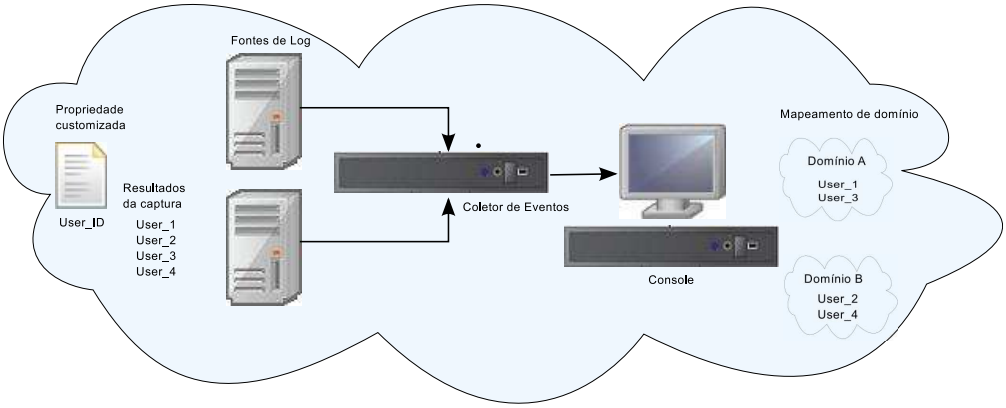

Figura 2. Designando domínios usando a propriedade de evento customizado

Se os resultados da captura retornarem um usuário que não é designado a um domínio específico definido pelo usuário, esse usuário será automaticamente designado ao domínio padrão. Designações de domínio padrão requerem intervenção manual. Execute procuras periódicas para assegurar que todas as entidades no domínio padrão sejam designadas corretamente.

Importante: Antes de usar uma propriedade customizada em uma definição de domínio, certifique-se de que a opção **Otimizar análise para regras, relatórios e procuras** esteja marcada na janela **Propriedades do Evento Customizado**. Esta opção assegura que a propriedade de evento customizado seja analisada e armazenada quando o QRadar recebe o evento pela primeira vez. A segmentação de domínio não ocorrerá se esta opção não estiver marcada.

Capítulo 16. Desvio de crescimento do ativo

Às vezes, as origens de dados do ativo produzem atualizações que não podem ser manipuladas corretamente pelo IBM Security QRadar sem uma correção manual.

Dependendo da causa do crescimento anormal do ativo, é possível corrigir a origem de dados do ativo que está causando o problema ou bloquear as atualizações de ativos provenientes dessa origem de dados.

Os *desvios de crescimento do ativo* ocorrem quando o número de atualizações de ativos para determinado dispositivo cresce além do limite configurado pelo limite de retenção de um tipo específico de informação de identidade. O QRadar usa o modelo de ativo para conectar as infrações ocorridas na implementação aos ativos físicos ou virtuais na rede. A manipulação correta dos desvios de crescimento de ativos é muito importante para a manutenção de um modelo de ativo preciso.

Na raiz de cada desvio de crescimento de ativo está uma origem de dados de ativo cujos dados são suspeitos para a atualização do modelo de ativo. Quando um possível desvio de crescimento de ativo é identificado, deve-se consultar a origem das informações, para determinar se há uma explicação razoável para que o ativo acumule grandes quantidades de dados de identidade.

Independentemente da correção da origem do problema ou do bloqueio das atualizações do ativo, deve-se limpar o banco de dados de ativos, removendo os dados de ativos inválidos e as entradas da lista de bloqueio de ativos.

Notificações do sistema para desvios de crescimento do ativo

O IBM Security QRadar gera notificações do sistema para ajudar a identificar e gerenciar os desvios de crescimento do ativo no ambiente.

Os desvios de crescimento de ativos, que são crescimentos anormais de dados de ativos, são específicos para um ambiente.

Quando um ativo que mostra um desvio de crescimento é identificado, uma notificação do sistema aparece na lista **Mensagens** no canto superior direito do QRadar Console. As notificações também aparecem em **Notificações do Sistema** no painel **Monitoramento de Sistemas**.

As mensagens do sistema a seguir indicam que o QRadar identificou possíveis desvios de crescimento de ativos:

- `O sistema detectou perfis de ativos que excedem o limite de tamanho normal`
- `As regras de lista de bloqueio do ativo incluíram novos dados de ativos às listas de bloqueio de ativos`

As mensagens de notificação do sistema incluem links para relatórios, que ajudam a identificar os ativos que têm desvios de crescimento.

Resolução de problemas de perfis de ativos que excedem o limite de tamanho normal

O IBM Security QRadar gera as notificações do sistema a seguir quando o acúmulo de dados em um único ativo excede os limites configurados para os dados de identificação.

`The system detected asset profiles that exceed the normal size threshold`

Explicação

A carga útil da notificação mostra uma lista dos cinco desvios de ativos mais frequentes e por que o sistema marcou cada ativo como um desvio de crescimento. Conforme mostrado no exemplo a seguir, a carga útil também mostra o número de vezes em que o ativo tentou crescer além de seu limite de tamanho.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

Quando os dados do ativo excedem o limite configurado, o QRadar bloqueia o ativo das atualizações futuras. Essa intervenção impede que o sistema receba mais dados corrompidos e reduz os impactos de desempenho que podem ocorrer se o sistema tentar reconciliar as atualizações recebidas com um perfil de ativo anormalmente grande.

Ação do usuário necessária

Use as informações na carga útil da notificação para identificar os ativos que estão contribuindo para o desvio de crescimento do ativo e para determinar o que está causando o crescimento anormal. A notificação fornece um link para um relatório de todos os ativos que passaram por um desvio de crescimento de ativo durante as últimas 24 horas.

Depois de resolver o desvio de crescimento de ativo no ambiente, é possível executar o relatório novamente.

1. Clique na guia **Atividade de Log** e clique em **Procurar** > **Nova Procura**.
2. Selecione a procura salva **Desvio de Crescimento de Ativos: Relatório de Ativos**.
3. Use o relatório para identificar e reparar dados de ativos imprecisos que foram criados durante o desvio.

Se os dados do ativo forem válidos, os administradores do QRadar podem aumentar os limites para endereços IP, endereços de Controle de Acesso à Mídia, nomes de host NetBIOS e nomes de host DNS na **Configuração do Gerenciador de Perfis do Ativo** na guia **Administrador** do QRadar.

Conceitos relacionados:

"Dados de ativos antigos" na página 206
Os dados de ativos antigos podem ser problemáticos quando a taxa de criação de novos registros de ativos excede a taxa de remoção dos dados de ativos antigos. O controle e gerenciamento dos limites de retenção de ativos é a chave para tratar os desvios de crescimento causados pelos dados de ativos antigos.

Inclusão de novos dados de ativos nas listas de bloqueio de ativos

O IBM Security QRadar gera as notificações do sistema a seguir quando uma parte dos dados do ativo exibe um comportamento que é consistente com o desvio de crescimento do ativo.

`The asset blacklist rules have added new asset data to the asset blacklists`

Explicação

As regras de exclusão de ativos monitoram a consistência e integridade dos dados de ativos. As regras controlam partes específicas de dados do ativo ao longo do tempo, para garantir que estejam sendo consistentemente observadas, com o mesmo subconjunto de dados, dentro de um prazo razoável.

Por exemplo, se uma atualização de ativo incluir um endereço de Controle de Acesso à Mídia e um nome de host DNS, o endereço de Controle de Acesso à Mídia será associado a esse nome de host DNS durante um período determinado. As atualizações de ativos subsequentes que contiverem esse endereço de Controle de Acesso à Mídia também conterão esse mesmo nome de host DNS, quando a atualização de ativo incluir um. Se, repentinamente, o endereço de Controle de Acesso à Mídia for associado a um nome de host DNS diferente por um curto período de tempo, a mudança será monitorada. Se for alterado novamente em um curto período de tempo, o endereço de Controle de Acesso à Mídia será sinalizado como contribuinte para uma instância de desvio ou anormalidade no crescimento do ativo.

Ação do usuário necessária

Use as informações na carga útil de notificação para identificar as regras usadas para monitorar os dados do ativo. Clique no link **Desvios de ativo por origem de log** na notificação para ver os desvios de ativos ocorridos nas últimas 24 horas.

Se os dados do ativo forem válidos, os administradores do QRadar poderão configurar o QRadar para solucionar o problema.

- Caso as listas de bloqueio estejam sendo preenchidas muito rapidamente, é possível ajustar as regras de exclusão de reconciliação de ativos que as preenchem.
- Se você desejar incluir os dados no banco de dados de ativos, é possível remover os dados do ativo da lista de bloqueio e incluí-los na lista de desbloqueio de ativos correspondente. A inclusão dos dados do ativo na lista de desbloqueio impede que eles reapareçam erroneamente na lista de bloqueio.

Conceitos relacionados:

"Ajuste avançado das regras de exclusão de reconciliação de ativos" na página 212
É possível ajustar as regras de Exclusão de Reconciliação de Ativos para refinar a definição de desvio de crescimento de ativos em uma ou mais regras.

"Modificando listas de bloqueio e de desbloqueio de ativos" na página 215
As listas de bloqueio e de desbloqueio de ativos são conjuntos de referência. É possível visualizar e modificar os dados das listas de bloqueio e de desbloqueio de ativos, usando a ferramenta Gerenciamento do Conjunto de Referência no QRadar Console.

Prevenção de desvios de crescimento do ativo

Após a confirmação da legitimidade do crescimento do ativo relatado, existem diversas maneiras de impedir que o IBM Security QRadar acione mensagens de desvio de crescimento para esse ativo.

Use a lista a seguir para ajudá-lo a decidir como impedir desvios no crescimento do ativo:

- Entenda como o QRadar manipula dados de ativo antigos.
- Ajuste as configurações de retenção do gerenciador de perfis do ativo para limitar o período de tempo de retenção dos dados do ativo.
- Ajuste o número de endereços IP permitidos para um único ativo
- Crie procuras de exclusão de identidade para excluir determinados eventos do fornecimento de atualizações sobre o ativo.
- Ajuste as regras de Exclusão de Reconciliação de Ativo para refinar a definição de desvio de crescimento do ativo.
- Crie listas de desbloqueio do ativo para impedir que determinados dados reapareçam nas listas de bloqueio do ativo.
- Modifique as entradas nas listas de desbloqueio e de bloqueio do ativo.
- Certifique-se de que as DSMs estejam atualizadas. O QRadar fornece uma atualização semanal automática que pode conter atualizações de DSM e correções para problemas de análise sintática.

O crescimento do ativo pode ser causado por grandes volumes de dados do ativo, o que altera a legitimidade, como nas situações a seguir:

- Um dispositivo móvel que frequentemente percorre vários escritórios e recebe um novo endereço IP sempre que efetua login.
- Um dispositivo que se conecta a um wifi público com concessões curtas de endereços IP, como em um campus universitário, pode coletar grandes volumes de dados ao longo de um semestre.

O QRadar pode relatar erroneamente essa atividade como um desvio de crescimento do ativo.

Conceitos relacionados:

"Atualizações Automáticas" na página 69
Você pode automaticamente ou manualmente atualizar os arquivos de configuração para assegurar que os arquivos de configuração contêm as mais recentes informações de segurança de rede.

Dados de ativos antigos

Os dados de ativos antigos podem ser problemáticos quando a taxa de criação de novos registros de ativos excede a taxa de remoção dos dados de ativos antigos. O controle e gerenciamento dos limites de retenção de ativos é a chave para tratar os desvios de crescimento causados pelos dados de ativos antigos.

Dados de ativos antigos são dados de ativos históricos que não são observados ativamente ou passivamente dentro de um prazo especificado. Os dados de ativos antigos são excluídos ao excederem o período de retenção configurado.

Os registros históricos se tornam novamente ativos se forem observados pelo QRadar passivamente, por meio de eventos e fluxos ou ativamente, por meio de scanners de porta e de vulnerabilidade.

A prevenção de desvios no crescimento do ativo requer o encontro do equilíbrio correto entre o número de endereços IP permitidos para um único ativo e o período de tempo em que o QRadar retém os dados do ativo. Antes de configurar o QRadar para acomodar altos níveis de retenção de dados do ativo, deve-se considerar as perdas e ganhos de desempenho e gerenciamento. Embora a adoção de períodos de retenção mais longos e limites mais altos por ativo possa parecer mais vantajosa a maior parte do tempo, uma melhor abordagem é determinar uma configuração de linha de base aceitável para o ambiente e testar essa configuração. Assim, é possível aumentar aos poucos os limites de retenção até atingir o equilíbrio correto.

Tarefas relacionadas:

"Ajustando as configurações de retenção do Gerenciador de Perfis do Ativo" na página 209
O IBM Security QRadar utiliza as configurações de retenção de ativos para gerenciar o tamanho dos perfis de ativos.

"Ajustando o número de endereços IP permitidos para um único ativo" na página 210
O IBM Security QRadar monitora o número de endereços IP acumulados por um único ativo ao longo do tempo.

Listas de bloqueio de ativos

Uma *lista de bloqueio de ativos* é uma coleção de dados considerados suspeitos pelo IBM Security QRadar, com base nas regras de exclusão de reconciliação de ativos. Os dados contidos na lista de bloqueio possivelmente contribuirão para que haja desvios de crescimento do ativo e o QRadar impede a inclusão desses dados no banco de dados de ativos.

Cada atualização de ativo no QRadar é comparada com as listas de bloqueio de ativos. Os dados dos ativos incluídos na lista de bloqueio são aplicados globalmente para todos os domínios. Se a atualização de ativo contiver informações de identidade (endereço de Controle de Acesso à Mídia, nome do host NetBIOS, nome do host DNS ou endereço IP) que se encontram em uma lista de bloqueio, a atualização de entrada será descartada e o banco de dados de ativos não será atualizado.

A tabela a seguir mostra o nome e o tipo da coleção de referência para cada tipo de dado de ativo de identidade.

Tabela 63. Nomes da coleção de referência para dados da lista de bloqueio de ativos

Tipo de dado de identidade	Nome da coleção de referência	Tipo da coleção de referência
Endereços IP (v4)	Lista de bloqueio de IPv4 de reconciliação de ativo	Conjunto de referência [Tipo de Conjunto: IP]
Nomes de host DNS	Lista de bloqueio de DNS de reconciliação de ativo	Conjunto de referência [Tipo de Conjunto: ALNIC*]
Nomes de host NetBIOS	Lista de bloqueio de NetBIOS de reconciliação de ativo	Conjunto de referência [Tipo de Conjunto: ALNIC*]
Endereços de Controle de Acesso à Mídia	Lista de bloqueio de MAC de reconciliação de ativo	Conjunto de referência [Tipo de Conjunto: ALNIC*]

* ALNIC é um tipo alfanumérico que pode acomodar valores de nomes de host e de endereços de Controle de Acesso à Mídia.

Conceitos relacionados:

"Listas de desbloqueio de ativos"
É possível usar listas de desbloqueio de ativos para impedir que dados de ativos do IBM Security QRadar reapareçam por engano nas listas de bloqueio de ativos.

Listas de desbloqueio de ativos

É possível usar listas de desbloqueio de ativos para impedir que dados de ativos do IBM Security QRadar reapareçam por engano nas listas de bloqueio de ativos.

Uma *lista de desbloqueio de ativos* é uma coleção de dados de ativos que substitui a lógica do mecanismo de reconciliação de ativos quanto aos dados que serão incluídos em uma lista de bloqueio de ativos. Ao identificar uma correspondência de lista de bloqueio, o sistema verifica a lista de desbloqueio para ver se o valor existe. Se a atualização de ativo corresponder aos dados existentes na lista de desbloqueio, a mudança é reconciliada e o ativo é atualizado. Os dados dos ativos incluídos na lista de desbloqueio são aplicados globalmente para todos os domínios.

Exemplo de um caso de uso de lista de desbloqueio

A lista de desbloqueio é útil quando existem dados de ativos que continuam a aparecer nas listas de bloqueio quando representam uma atualização de ativo válida. Por exemplo, é possível que haja um balanceador de carga round robin DNS configurado para girar em um conjunto de cinco endereços IP. As regras de Exclusão de Reconciliação de Ativos podem determinar que os vários endereços IP associados ao mesmo nome do host DNS sejam indicativos de um desvio no crescimento de ativos e o sistema pode incluir o balanceador de carga DNS na lista de bloqueio. Para resolver esse problema, é possível incluir o nome do host DNS na Lista de Desbloqueio de DNS de Reconciliação de Ativos.

Entradas em massa na lista de desbloqueio de ativos

Um banco de dados de ativos preciso facilita a conexão das infrações acionadas no sistema com os ativos físicos ou virtuais na rede. A não consideração dos desvios de ativos, por meio da inclusão de entradas em massa na lista de desbloqueio de ativos, não ajuda na construção de um banco de dados de ativos preciso. Em vez de incluir entradas em massa na lista de desbloqueio, revise a lista de bloqueio de ativos, para determinar o que está contribuindo para o desvio no crescimento de ativos e então determine como corrigir isso.

Tipos de listas de desbloqueio de ativos

Cada tipo de dado de identificação é mantido em uma lista de desbloqueio separada. A tabela a seguir mostra o nome e o tipo da coleção de referência para cada tipo de dado de ativo de identidade.

Tabela 64. Nome da coleção de referência para dados da lista de desbloqueio de ativos

Tipo de dado	Nome da coleção de referência	Tipo da coleção de referência
endereços IP	Lista de desbloqueio de IPv4 de reconciliação de ativos	Conjunto de referência [Tipo de Conjunto: IP]
Nomes de host DNS	Lista de desbloqueio de DNS de reconciliação de ativos	Conjunto de referência [Tipo de Conjunto: ALNIC*]
Nomes de host NetBIOS	Lista de desbloqueio de NetBIOS de reconciliação de ativos	Conjunto de referência [Tipo de Conjunto: ALNIC*]

Tabela 64. Nome da coleção de referência para dados da lista de desbloqueio de ativos (continuação)

Tipo de dado	Nome da coleção de referência	Tipo da coleção de referência
Endereços de Controle de Acesso à Mídia	Lista de desbloqueio de MAC de reconciliação de ativos	Conjunto de referência [Tipo de Conjunto: ALNIC*]

* ALNIC é um tipo alfanumérico que pode acomodar valores de nomes de host e de endereços de Controle de Acesso à Mídia.

Conceitos relacionados:

"Listas de bloqueio de ativos" na página 207
Uma *lista de bloqueio de ativos* é uma coleção de dados considerados suspeitos pelo IBM Security QRadar, com base nas regras de exclusão de reconciliação de ativos. Os dados contidos na lista de bloqueio possivelmente contribuirão para que haja desvios de crescimento do ativo e o QRadar impede a inclusão desses dados no banco de dados de ativos.

Ajustando as configurações de retenção do Gerenciador de Perfis do Ativo

O IBM Security QRadar utiliza as configurações de retenção de ativos para gerenciar o tamanho dos perfis de ativos.

O período de retenção padrão para a maioria dos dados de ativos é de 120 dias após a última vez em que eles foram passivamente ou ativamente observados no QRadar. Os nomes de usuários são mantidos por 30 dias.

Os dados de ativos incluídos manualmente pelos usuários do QRadar geralmente não contribuem para os desvios de crescimento de ativos. Por padrão, esses dados são mantidos indefinidamente. Para todos os outros tipos de dados de ativos, o sinalizador **Manter Indefinidamente** é sugerido apenas para ambientes estáticos.

Sobre Esta Tarefa

É possível ajustar o tempo de retenção com base no tipo de dado de identificação de ativo existente no evento. Por exemplo, caso vários endereços IP sejam mesclados em um ativo, é possível alterar o período de Retenção de IP do Ativo de 120 dias para um valor inferior.

Ao alterar o período de retenção de ativos de um tipo específico de dado de ativo, o novo período de retenção é aplicado em todos os dados de ativos no QRadar. Os dados de ativos que já excedem o novo limite são removidos após a conclusão da implementação. Para garantir que sempre seja possível identificar os hosts nomeados, mesmo quando os dados do ativo estiverem além do período de retenção, o processo de limpeza de retenção de ativos não remove o último valor de nome de host conhecido de um ativo.

Antes de determinar por quantos dias você deseja manter os dados do ativo, é necessário compreender as seguintes características sobre períodos de retenção mais longos:

- fornecem uma melhor visualização histórica dos ativos.
- Criam volumes de dados maiores por ativo no banco de dados de ativos.
- Aumentam a probabilidade de que dados antigos contribuam para a criação de mensagens de desvio de crescimento de ativos.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Configuração do Gerenciador de Perfis do Ativo**.
4. Clique em **Configuração de Retenção do Gerenciador de Perfis do Ativo**.
5. Ajuste os valores de retenção e clique em **Salvar**.
6. Para que as atualizações entrem em vigor, implemente as mudanças no ambiente.

Tarefas relacionadas:

"Ajustando o número de endereços IP permitidos para um único ativo"
O IBM Security QRadar monitora o número de endereços IP acumulados por um único ativo ao longo do tempo.

Ajustando o número de endereços IP permitidos para um único ativo

O IBM Security QRadar monitora o número de endereços IP acumulados por um único ativo ao longo do tempo.

Por padrão, o QRadar gera uma mensagem do sistema quando um único ativo acumula mais de 75 endereços IP. Caso deseje que os ativos acumulem mais de 75 endereços IP, é possível ajustar o valor **Número de IPs permitidos para um único ativo** para evitar futuras mensagens do sistema.

Sobre Esta Tarefa

A configuração de um limite muito alto para o número de endereços IP impede que o QRadar detecte desvios de crescimento de ativos antes que eles tenham um impacto negativo no restante da implementação. A configuração de um limite muito baixo aumenta o número de desvios de crescimento de ativos relatados.

É possível usar a seguinte diretriz ao ajustar a configuração **Número de IPs permitidos para um único ativo** pela primeira vez.

O número de endereços IP permitidos para um único ativo = (<*retention time (days)*> x <*estimated IP addresses per day*>) + <*buffer number of IP addresses*>

Em que

- <*estimated IP addresses per day*> é o número de endereços IP que um ativo único pode acumular em um dia, em condições normais
- <*retention time (days)*> é o período de tempo preferencial para retenção dos endereços IP do ativo

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique em **Configuração do Gerenciador de Perfis do Ativo**.
4. Clique em **Configuração de Retenção do Gerenciador de Perfis do Ativo**.
5. Ajuste os valores de configuração e clique em **Salvar**.
6. Para que as atualizações entrem em vigor, implemente as mudanças no ambiente.

Tarefas relacionadas:

"Ajustando as configurações de retenção do Gerenciador de Perfis do Ativo" na página 209
O IBM Security QRadar utiliza as configurações de retenção de ativos para gerenciar o tamanho dos perfis de ativos.

Procuras de exclusão de identidade

As procuras de exclusão de identidade podem ser usadas para gerenciar ativos únicos que acumulam grandes volumes de informações de identidade semelhantes por motivos conhecidos e válidos.

Por exemplo, as origens de log podem fornecer grandes volumes de informações de identidade do ativo ao banco de dados de ativos. Elas fornecem mudanças ao IBM Security QRadar feitas quase em tempo real nas informações do ativo e podem manter o banco de dados de ativos atualizado. Mas as origens de log muitas vezes são a fonte de desvios de crescimento do ativo e outras irregularidades relacionadas aos ativos.

Quando uma origem de log enviar dados de ativos incorretos para o QRadar, tente corrigir a origem de log, para que os dados enviados possam ser utilizados pelo banco de dados de ativos. Caso não seja possível corrigir a origem de log, é possível construir uma procura de exclusão de identidade que bloqueie a entrada de informações do ativo no banco de dados de ativos.

Também é possível usar uma procura de exclusão de identidade em que `Identity_Username+Is Any Of + Anonymous Logon`, para garantir que não estejam sendo atualizados ativos relacionados a contas do serviço ou a serviços automatizados.

Diferenças entre procuras de exclusão de identidade e listas de bloqueio

Embora a funcionalidade das procuras de exclusão de identidade e das listas de bloqueio pareça ser semelhante, existem diferenças significativas.

As listas de bloqueio podem especificar apenas dados de ativos brutos, como endereços de Controle de Acesso à Mídia e nomes de host, que devem ser excluídos. As procuras de exclusão de identidade filtram os dados do ativo com base em campos de procura, como origem de log, categoria e nome do evento.

As listas de bloqueio não consideram o tipo de origem de dados que está fornecendo os dados, enquanto as procuras de exclusão de identidade podem ser aplicadas apenas a eventos. As procuras de exclusão de identidade podem bloquear atualizações de ativos com base em campos de procura de eventos comuns, como tipo de evento, nome do evento, categoria e origem de log.

Criando procuras de exclusão de identidade

Para impedir que determinados eventos forneçam dados de ativos para o banco de dados de ativos, é possível criar uma procura de exclusão de identidade do IBM Security QRadar.

Sobre Esta Tarefa

Os filtros criados para a procura devem corresponder aos eventos a serem excluídos, não aos eventos a serem mantidos.

Talvez seja útil executar a procura em relação a eventos que já estão no sistema. No entanto, ao salvar a procura, selecione **Tempo Real (fluxo)** nas opções de **Período de tempo**. Se você não escolher essa configuração, a procura não corresponderá a nenhum resultado quando for executada em relação ao fluxo atual de eventos enviados para o QRadar.

Ao atualizar a procura de exclusão de identidade salva sem alterar o nome, a lista de exclusão de identidade usada pelo Gerenciador de Perfis do Ativo é atualizada. Por exemplo, é possível editar a procura para incluir mais filtragem dos dados do ativo a serem excluídos. Os novos valores são incluídos e a exclusão de ativos é iniciada imediatamente após o salvamento da procura.

Procedimento

1. Na guia **Atividade de Log**, clique em **Procurar** > **Nova Procura**.
2. Crie a procura incluindo critérios de procura e filtros para corresponder aos eventos a serem excluídos das atualizações de ativos.
3. Na caixa **Intervalo de Tempo**, selecione **Tempo Real (fluxo)** e, em seguida, clique em **Filtrar** para executar a procura.
4. Na tela de resultados da procura, clique em **Salvar Critérios** e forneça as informações para a procura salva. É possível designar a procura salva para um grupo de procura. Existe um grupo de procuras de Exclusão de Identidade na pasta **Autenticação, Identidade e Atividade do Usuário**.

   Certifique-se de que **Tempo Real (fluxo)** esteja selecionado nas opções de **Intervalo de Tempo**.
5. Clique em **OK** para salvar a procura.
6. Clique na guia **Administrador** e clique em **Configuração do Gerenciador de Perfis do Ativo**.
7. Clique em **Gerenciar Exclusão de Identidade** na parte inferior da tela.
8. Selecione a procura de exclusão de identidade criada a partir da lista de procuras à esquerda e clique no ícone incluir (>). Se não for possível localizar a procura, digite as primeiras letras no filtro, na parte superior da lista.
9. Clique em **Salvar**.
10. Para que as atualizações entrem em vigor, implemente as mudanças no ambiente.

Tarefas relacionadas:

"Implementando mudanças" na página 4
É possível atualizar suas definições de configuração a partir da guia **Admin**. Suas mudanças são salvas em uma área temporária onde são armazenadas até serem implementadas manualmente.

Ajuste avançado das regras de exclusão de reconciliação de ativos

É possível ajustar as regras de Exclusão de Reconciliação de Ativos para refinar a definição de desvio de crescimento de ativos em uma ou mais regras.

Por exemplo, considere esse modelo normalizado de uma regra de Exclusão de Reconciliação de Ativos.

```
Apply AssetExclusion: Exclude DNS Name By IP on events which are detected
 by the Local system and NOT when any of
Identity Host Name are contained in any of
Asset Reconciliation DNS Whitelist - AlphaNumeric (Ignore Case),
```

```
 Asset Reconciliation DNS Blacklist - AlphaNumeric (Ignore Case)
 and when at least N1 events are seen with the same
Identity Host Name and different Identity IP in N2
```

Esta tabela lista as variáveis no modelo de regra que podem ser ajustadas e o resultado da mudança. Evite alterar outras variáveis no modelo.

Tabela 65. Opções para ajuste das regras de reconciliação de ativos

Variável	Valor padrão	Resultado do ajuste
N1	3	O ajuste dessa variável para um valor inferior resulta na inclusão de mais dados na lista de bloqueio, porque são necessários menos eventos com dados conflitantes para acionar a regra. O ajuste dessa variável para um valor superior resulta na inclusão de menos dados na lista de bloqueio, porque são necessários mais eventos com dados conflitantes para acionar a regra.
N2	2 horas	O ajuste dessa variável para um valor inferior reduz a janela de tempo em que os eventos N1 devem ser vistos para que a regra seja acionada. O tempo necessário para a observação de dados correspondente é reduzido, o que resulta na inclusão de menos dados na lista de bloqueio. O ajuste dessa variável para um valor superior aumenta o tempo em que os eventos N1 devem ser vistos para que a regra seja acionada. O tempo para a observação de dados correspondentes aumenta, o que resulta na inclusão de mais dados na lista de bloqueio. O aumento do período de tempo pode afetar os recursos de memória do sistema, uma vez que os dados são controlados durante períodos de tempo mais longos.

As regras de Exclusão de Reconciliação de Ativos são válidas no sistema todo. As mudanças nas regras afetam o comportamento da regra em todo o sistema.

Aplicando diferentes ajustes para regras

Pode ser necessário aplicar ajustes diferentes para regras em diferentes partes do sistema. Para aplicar ajustes diferentes para regras, deve-se duplicar as regras de Exclusão de Reconciliação de Ativos a serem ajustadas e incluir um ou mais testes para restringir as regras, para que seja possível testar apenas algumas partes do sistema. Por exemplo, você talvez deseje criar regras que testem apenas redes, origens de log ou tipos de eventos.

Sobre Esta Tarefa

Seja sempre cuidadoso ao incluir novas regras no sistema, porque algumas tarefas e regras de CRE podem afetar o desempenho do sistema. Talvez seja melhor incluir as novas regras na parte superior de cada pilha de teste, para permitir que o sistema ignore o restante da lógica de teste sempre que uma atualização de ativo corresponder aos critérios para a nova regra.

Procedimento

1. Duplique a regra.
   a. Na guia **Infrações**, clique em **Regras** e selecione a regra a ser copiada.

b. Clique em **Ações** > **Duplicar**. Pode ser útil o nome da nova regra indicar o motivo para sua duplicação.

2. Inclua um teste na regra.

   Determine um filtro a ser usado para aplicar a regra apenas a um subconjunto de dados do sistema. Por exemplo, é possível incluir um teste que corresponda apenas eventos vindos de determinada origem de log.

3. Ajuste as variáveis da regra para obter o comportamento desejado.

4. Atualize a regra original.

   a. Inclua na regra original o mesmo teste que foi incluído na regra duplicada, mas, dessa vez, inverta os operadores `AND` e `AND NOT` das regras.

      A inversão dos operadores impede que os eventos sejam acionados em ambas as regras.

Excluindo ativos inválidos

Depois de corrigir os ativos que contribuíram para o desvio de crescimento de ativos, limpe os artefatos de ativos, usando a limpeza seletiva ou reconstruindo o banco de dados de ativos.

Sobre Esta Tarefa

Limpeza seletiva

Este método destina-se a desvios de crescimento de ativos de escopo limitado. A remoção seletiva dos ativos afetados é a maneira menos invasiva de limpar os artefatos de ativos, mas, caso muitos ativos tenham sido afetados, é também a maneira mais trabalhosa.

Reconstrução do banco de dados de ativos

A reconstrução do banco de dados de ativos desde o início é o método mais eficiente e preciso para a exclusão de ativos quando os desvios de crescimento de ativos são generalizados.

Esse método gera os ativos novamente no banco de dados, de forma passiva, com base no novo ajuste que foi configurado para solucionar os problemas de crescimento de ativos. Com essa abordagem, todos os resultados de varredura e os dados de ativos residuais são perdidos, mas é possível recuperar esses dados com uma nova execução da varredura ou pela reimportação dos resultados da varredura.

Procedimento

1. Para remover seletivamente os artefatos inválidos do banco de dados de ativos, execute estas etapas:

   a. Na guia **Atividade do Log**, execute a procura de eventos **Desvio de Crescimento de Ativos: Relatório de Ativos**. Essa procura retorna um relatório de ativos que são afetados pelo desvio de crescimento de ativos e devem ser excluídos.

   b. Na guia **Ativos**, clique em **Ações** > **Excluir Ativo** Pode haver uma demora até que o ativo não mais apareça no QRadar.

2. Para reconstruir do zero o banco de dados de ativos, execute estas etapas:

   a. Use SSH para efetuar login no QRadar Console como administrador.

   b. Execute o script `/opt/qradar/support/cleanAssetModel.sh` na linha de comandos do console e selecione **Opção 1**, quando solicitado.

   A reconstrução do banco de dados de ativos reinicia o mecanismo de reconciliação de ativos.

Resultados

A limpeza de uma lista de bloqueio remove todas as entradas da lista de bloqueio, incluindo as entradas incluídas manualmente. As entradas da lista de bloqueio que foram incluídas manualmente devem ser incluídas novamente.

Excluindo entradas da lista de bloqueio

Depois de corrigir a causa das entradas da lista de bloqueio, deve-se limpar as entradas restantes. É possível remover as entradas da lista de bloqueio individualmente, embora seja melhor limpar todas as entradas da lista de bloqueio, para permitir que os valores da lista de bloqueio que não tenham relação com o desvio de crescimento de ativos sejam gerados novamente.

Procedimento

1. Para limpar uma lista de bloqueio usando o QRadar Console:
   a. Clique em **Administrador** > **Configuração do Sistema** > **Gerenciamento do Conjunto de Referência**.
   b. Selecione um conjunto de referência e, em seguida, clique em **Excluir**.
   c. Use a caixa de texto de procura rápida para procurar os conjuntos de referência a serem excluídos e, em seguida, clique em **Excluir Listados**.
2. Para limpar uma lista de bloqueio usando a interface da linha de comandos do QRadar Console:
   a. Altere o diretório para `/opt/qradar/bin`.
   b. Execute o comando a seguir.

      ```
      ./ReferenceDataUtil.sh purge "Reference Collection Name"
      ```

      em que *Reference Collection Name* é uma das listas a seguir:
      - Lista de bloqueio de NetBIOS de reconciliação de ativo
      - Lista de bloqueio de DNS de reconciliação de ativo
      - Lista de bloqueio de IPv4 de reconciliação de ativo
      - Lista de bloqueio de MAC de reconciliação de ativo

Resultados

A limpeza de uma lista de bloqueio remove todas as entradas da lista de bloqueio, incluindo as entradas incluídas manualmente. As entradas da lista de bloqueio que foram incluídas manualmente devem ser incluídas novamente.

Modificando listas de bloqueio e de desbloqueio de ativos

As listas de bloqueio e de desbloqueio de ativos são conjuntos de referência. É possível visualizar e modificar os dados das listas de bloqueio e de desbloqueio de ativos, usando a ferramenta Gerenciamento do Conjunto de Referência no QRadar Console.

Como alternativa, é possível usar a interface da linha de comandos (CLI) ou o terminal da API RestFUL para atualizar o conteúdo das listas de bloqueio e de desbloqueio de ativos.

Conceitos relacionados:

Capítulo 7, “Gerenciamento de conjuntos de referência”, na página 111
Utilizando a janela de Gerenciamento do Conjunto de Referência , é possível criar e gerenciar conjuntos de referência. Você também pode importar elementos em um

conjunto de referência a partir de um arquivo externo.

Atualizações feitas nas listas de bloqueio e de desbloqueio de ativos usando a CLI do QRadar

É possível usar a interface da linha de comandos (CLI) do IBM Security QRadar para incluir ou modificar as entradas que estão nas listas de bloqueio ou de desbloqueio de ativos.

Os comandos para a inclusão de novos valores em cada lista são descritos na tabela a seguir. O valor de parâmetro deve corresponder exatamente aos valores de atualização fornecidos pela origem de dados de ativos originária.

Tabela 66. Sintaxe de comando para modificação dos dados da lista de bloqueio e de desbloqueio de ativos

Nome	Sintaxe de comando
Lista de bloqueio de IPv4 de reconciliação de ativo	`ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Blacklist"` *IP* Por exemplo, esse comando inclui o endereço IP 192.168.3.56 na lista de bloqueio: `ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Blacklist" 192.168.3.56`
Lista de bloqueio de DNS de reconciliação de ativo	`ReferenceSetUtil.sh add "Asset Reconciliation DNS Blacklist"` *DNS* Por exemplo, esse comando inclui o nome de domínio 'misbehaving.asset.company.com' na lista de bloqueio: `ReferenceSetUtil.sh add "Asset Reconciliation DNS Blacklist" "misbehaving.asset.company.com"`
Lista de bloqueio de NetBIOS de reconciliação de ativo	`ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Blacklist"` *NETBIOS* Por exemplo, esse comando remove o nome do host NetBIOS 'deviantGrowthAsset-156384' da lista de bloqueio: `ReferenceSetUtil.sh delete "Asset Reconciliation NetBIOS Blacklist" "deviantGrowthAsset-156384"`
Lista de bloqueio de MAC de reconciliação de ativo	`ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist"` *MACADDR* Por exemplo, esse comando inclui o endereço de Controle de Acesso à Mídia '00:a0:6b:54:9f:0e' na lista de bloqueio: `ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:6b:54:9f:0e"`
Lista de desbloqueio de IPv4 de reconciliação de ativos	`ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Whitelist"` *IP* Por exemplo, esse comando exclui o endereço IP 10.1.95.142 da lista de desbloqueio: `ReferenceSetUtil.sh delete "Asset Reconciliation IPv4 Whitelist" 10.1.95.142`

Tabela 66. Sintaxe de comando para modificação dos dados da lista de bloqueio e de desbloqueio de ativos (continuação)

Nome	Sintaxe de comando
Lista de desbloqueio de DNS de reconciliação de ativos	`ReferenceSetUtil.sh add "Asset Reconciliation DNS Whitelist"` *`DNS`* Por exemplo, esse comando inclui o nome de domínio 'loadbalancer.company.com' na lista de desbloqueio: `ReferenceSetUtil.sh add "Asset Reconciliation DNS Whitelist" "loadbalancer.company.com"`
Lista de desbloqueio de NetBIOS de reconciliação de ativos	`ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Whitelist"` *`NETBIOS`* Por exemplo, esse comando inclui o nome NetBIOS 'assetName-156384' na lista de desbloqueio: `ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Whitelist" "assetName-156384"`
Lista de desbloqueio de MAC de reconciliação de ativos	`ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist"` *`MACADDR`* Por exemplo, esse comando inclui o endereço de Controle de Acesso à Mídia '00:a0:6b:54:9f:0e' na lista de bloqueio: `ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:6b:54:9f:0e"`

Tarefas relacionadas:

"Atualizando listas de bloqueio e de desbloqueio usando a API RESTful"
É possível usar a API RESTful do IBM Security QRadar para customizar o conteúdo das listas de bloqueio e de desbloqueio de ativos.

Atualizando listas de bloqueio e de desbloqueio usando a API RESTful

É possível usar a API RESTful do IBM Security QRadar para customizar o conteúdo das listas de bloqueio e de desbloqueio de ativos.

Sobre Esta Tarefa

É necessário especificar o nome exato do conjunto de referência a ser visualizado ou atualizado.

- Lista de bloqueio de IPv4 de reconciliação de ativo
- Lista de bloqueio de DNS de reconciliação de ativo
- Lista de bloqueio de NetBIOS de reconciliação de ativo
- Lista de bloqueio de MAC de reconciliação de ativo
- Lista de desbloqueio de IPv4 de reconciliação de ativos
- Lista de desbloqueio de DNS de reconciliação de ativos
- Lista de desbloqueio de NetBIOS de reconciliação de ativos
- Lista de desbloqueio de MAC de reconciliação de ativos

Procedimento

1. Digite a URL a seguir no navegador da web para acessar a interface da API RESTful:

   `https://`*`ConsoleIPaddress`*`/api_doc`

2. Na área de janela de navegação à esquerda, localize `4.0>/reference_data >/sets > /{name}`.
3. Para visualizar o conteúdo de uma lista de bloqueio ou de desbloqueio de ativos, siga estas etapas:
   a. Clique na guia **GET** e role para baixo até a seção **Parâmetros**.
   b. No campo **Valor** do parâmetro **Nome**, digite o nome da lista de bloqueio ou de desbloqueio de ativos que você deseja visualizar.
   c. Clique em **Experimentar** e visualize os resultados na parte inferior da tela.
4. Para incluir um valor em uma lista de bloqueio ou de desbloqueio, siga estas etapas:
   a. Clique na guia **POST** e role para baixo até a seção **Parâmetros**.
   b. Digite valores para os seguintes parâmetros:

Tabela 67. Parâmetros necessários para a inclusão de novos dados de ativos

Nome do parâmetro	Descrição do parâmetro
name	Representa o nome da coleção de referência a ser atualizada.
value	Representa o item de dados a ser incluído na lista de bloqueio ou de desbloqueio de ativos. Deve corresponder exatamente aos valores de atualização de ativos fornecidos pela origem de dados de ativos originária.

   c. Clique em **Experimentar** para incluir o novo valor na lista de bloqueio ou de desbloqueio de ativos.

O que Fazer Depois

Para obter mais informações sobre como usar a API RESTful para alterar os conjuntos de referência, consulte o *Guia da API do IBM Security QRadar*.

Conceitos relacionados:

"Atualizações feitas nas listas de bloqueio e de desbloqueio de ativos usando a CLI do QRadar" na página 216

É possível usar a interface da linha de comandos (CLI) do IBM Security QRadar para incluir ou modificar as entradas que estão nas listas de bloqueio ou de desbloqueio de ativos.

Capítulo 17. Configurando sistemas QRadar para encaminhar dados para outros sistemas

É possível configurar sistemas IBM Security QRadar para encaminhar dados para um ou mais fornecedores de sistema, tais como chamados ou alertas de sistema. É possível encaminhar dados para outros QRadar sistemas O sistema de destino que recebe os dados do QRadar é conhecido como um *destino de encaminhamento*.

Com exceção da identificação de domínio, os sistemas QRadar asseguram que todos os dados encaminhados permaneçam inalterados. As informações de domínio são removidas dos dados encaminhados. Eventos e fluxos que contêm informações de domínio são automaticamente designados ao domínio padrão no sistema de recebimento.

Para evitar problemas de compatibilidade ao enviar dados de evento e de fluxo, certifique-se de que a implementação que está recebendo os dados seja da mesma versão ou superior à implementação que está enviando os dados.

1. Configurar um ou mais destinos de encaminhamento.
2. Para determinar quais dados você deseja encaminhar, configurar regras de roteamento, regras customizadas, ou ambos.
3. Configure o roteamento de opções a serem aplicadas aos dados.

Por exemplo, você pode configurar todos os dados de um coletor de eventos específicos para redirecionar para um sistema de registro específico. Também é possível ignorar correlação removendo os dados que correspondem a uma regra de roteamento.

Adicionando encaminhamento de destinos

Antes de conseguir configurar em massa, ou encaminhamento de dados seletivos, deve-se adicionar destinos de encaminhamento.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Destinos de Encaminhamento**.
4. Na barra de ferramentas, clique em **Incluir**.
5. Na janela Destinos de Encaminhamento , insira valores para os parâmetros.

   A tabela a seguir descreve alguns dos parâmetros Destinos de Encaminhamento.

Tabela 68. Parâmetros Destinos de Encaminhamento

Parâmetro	Descrição
Formato de Evento	• **Carga Útil** são os dados no formato em que a fonte de log ou fonte de fluxo foram enviados. • **Normalizado** são os dados brutos que são analisados e preparados como informações legíveis para a interface com o usuário.
Endereço de Destino	O endereço IP ou o nome do host do sistema fornecedor que você deseja encaminhar dados.

Tabela 68. Parâmetros Destinos de Encaminhamento (continuação)

Parâmetro	Descrição
Protocolo	• **TCP** Utilize o **TCP** protocolo para enviar dados normalizados utilizando o protocolo TCP, deve-se criar uma origem externa no endereço de destino na porta 32004. • **UDP**
Prefixe um cabeçalho do syslog se estiver ausente ou inválido	Se um cabeçalho do syslog válido não for detectado na mensagem do syslog original, selecione esta caixa de opção. O cabeçalho de syslog prefixado inclui o endereço IP do dispositivo de origem de log originário (spoofing de endereço IP) no campo **Nome do host** do cabeçalho de syslog. Se essa caixa de opções não for selecionada, os dados são enviados sem modificação. Quando QRadar encaminha mensagens syslog, a mensagem de saída são verificadas para garantir que possui um cabeçalho do syslog válido.

6. Clique em **Salvar**.

Configurando perfis de encaminhamento

Se desejar especificar as propriedades a serem encaminhadas ao destino de encaminhamento, configure o perfil de encaminhamento.

Você deve recriar os perfis de encaminhamento JSON criados no IBM Security QRadar SIEM V7.2.3 ou anterior.

Sobre Esta Tarefa

É possível usar perfis de encaminhamento apenas quando os dados do evento são enviados no formato JSON.

É possível selecionar propriedades específicas de evento ou fluxo, incluindo propriedades customizadas, para serem encaminhadas a um destino externo. É possível aprimorar a capacidade de leitura dos dados do evento ao especificar um nome alternativo e um valor padrão para o atributo. Os nomes alternativos e os valores padrão são específicos para o perfil no qual eles estão definidos. Se os atributos forem usados em outros perfis, os nomes alternativos e os valores padrão deverão ser redefinidos.

É possível usar um único perfil que tenha vários destinos de encaminhamento. Ao editar um perfil, certifique-se de que as mudanças sejam apropriadas para todos os destinos de encaminhamento aos quais o perfil está associado.

Ao excluir um perfil, todos os destinos de encaminhamento que usaram o perfil automaticamente voltam a usar o perfil padrão.

Procedimento

1. Clique na guia **Administrador** e, na área de janela de navegação, clique em **Configuração do sistema**.
2. Clique no ícone **Destinos de Encaminhamento**.
3. Na barra de ferramentas, clique em **Gerenciador de perfil**.

4. Para criar um novo perfil, clique em **Novo**.
5. Digite um nome para o perfil e selecione a caixa de seleção próxima aos atributos que deseja incluir no conjunto de dados do evento.
6. Para alterar um perfil existente, selecione-o e clique em **Editar** ou **Excluir**.
7. Clique em **Salvar**.

Configurando regras de roteamento para encaminhamento em massa

Após você adicionar um ou mais destinos de encaminhamentos, é possível criar filtros baseados em regras ds roteamento para encaminhar grandes quantidades de dados.

Sobre Esta Tarefa

Você pode configurar regras de roteamento para encaminhar dados no modo on-line ou off-line :

- No modo**Online**, seus dados permanece atuais porque o encaminhamento é executado em tempo real. Se o destino de encaminhamento se tornar inalcançável, os dados podem ser potencialmente perdidas.
- Em **Off-** modo, todos os dados são armazenados no banco de dados e, em seguida, enviada para o destino de encaminhamento. Isso garante que nenhum dado seja perdido, no entanto, pode haver atrasos na transmissão de dados.

A tabela a seguir descreve alguns dos parâmetros Regras de Roteamento

Tabela 69. Janela parâmetros Detalhes do Usuário

Parâmetro	Descrição
Coletor de Eventos de Encaminhamento	Essa opção é exibida quando você seleciona a opção **Online**. Especifica o Coletor de eventos que você deseja processar os dados esta regra de roteamento.
Processador de Evento de Encaminhamento	Essa opção é exibida quando você seleciona a opção **Off-**. Especifica o Processador de eventos que você deseja processar os dados esta regra de roteamento. **Restrição:** Essa opção não estará disponível se **Descarte** está selecionada na janela **Opções de Roteamento**.

Tabela 69. Janela parâmetros Detalhes do Usuário (continuação)

Parâmetro	Descrição
Opções de Roteamento	• A opção **encaminhar** especifica que os dados são encaminhados para destinos de encaminhamento. Os dados também são armazenados no banco de dados e processados pelo mecanismo de Regras Customizadas (CRE). • A opção **Descarte** especifica que os dados não são armazenados no banco de dados e não é processado pelo CRE. Os dados não são redirecionados para um destino de encaminhamento, mas é processado pelo CRE. Essa opção não estará disponível se você selecionar a opção **Offline**. • A opção **Efetuar correlação bypass** especifica que dados não são processados pelo CRE, mas são armazenados no banco de dados. Essa opção não estará disponível se você selecionar a opção **Offline**. Você pode combinar duas opções: • em**Avançar** e **Descartar** Os dados são redirecionados para o destino de encaminhamento especificados. Os dados não são armazenados no banco de dados e serão processados pela CRE. • **Encaminhamento** e **Bypass Correlação** Os dados são redirecionados para o destino de encaminhamento especificados. Os dados também são armazenados no banco de dados, mas ele não é processado pelo CRE. O CRE no destino encaminhado processa os dados. Se de dados correspondem a várias regras, a melhor opção é aplicada de roteamento. Por exemplo, se os dados que correspondem a uma regra que é configurado para descartar e uma regra para ignorar o processamento de pagamentos, os dados não são eliminados. Em vez disso, os dados ignoram a CRE e é armazenado no banco de dados. Todos os eventos ou fluxos de mensagens são mantidos em armazenamento.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Regras de Roteamento**.
4. Na barra de ferramentas, clique em **Incluir**.
5. Na janela Regras de Roteamento, insira valores para os parâmetros.

a. Digite um nome e uma descrição para a regra de roteamento.
b. No campo **Modo de**, selecione uma das seguintes opções: **-line** ou **-line**.
c. Nas listas **Coletor de Eventos de Encaminhamento** ou **de Encaminhamento de Eventos do Processador**, selecione o coletor de eventos a partir do qual você deseja redirecionar dados.
d. No campo **Fontes de dados** ou na seção **Filtro de eventos** selecione quias dados você quer rotear: **Eventos** ou **Fluxos**.

   Se você selecionar a opção **Fluxo de Filtros** , o título da seção é alterado para **Fluxo de Filtros** e o **Corresponder Tudo Incoming Eventos** caixa de opções é alterado para **Corresponder Todos os Fluxos**.
e. Para encaminhar todos os dados de recebimento, selecione o **Corresponder todos os eventos recebidos** ou na caixa de listagem **Corresponder todos os fluxos recebidos** .

   Restrição: Se você selecionar essa caixa de seleção, não é possível incluir um filtro.
f. Para incluir um filtro, no **Filtros de Eventos** ou **Fluxo de Filtros** seção, selecione um filtro na lista pela primeira vez e um operando na segunda lista.
g. Na caixa de texto, digite o valor que você deseja filtrar para, e, em seguida, clique em **Incluir Filtro**.
h. Repita as duas etapas anteriores para cada filtro que você deseja incluir.
i. Para redirecionar dados do log que corresponde aos filtros atual, selecione a caixa de opções **Encaminhamento** e, em seguida, selecione a caixa de opções para cada destino de encaminhamento preferencial.

   Restrição: Se você selecionar a caixa de opções **Encaminhamento** , você também pode selecionar o **Descartar** ou **Bypass Correlação** caixas de opções, mas não ambos.

   Se você deseja editar, incluir ou excluir um destino de encaminhamento, clique no link **Gerenciar Destinos**.

6. Clique em **Salvar**.

Configurando redirecionamento seletivo

Utilize o assistente Regra Customizada para configurar o encaminhamento de dados do evento. Configure regras que encaminham os dados do evento para um ou mais destinos, como uma resposta da regra.

Sobre Esta Tarefa

Os critérios que determinam se os dados de eventos que são enviados para um destino de encaminhamento são baseados nos ensaios e blocos de construções que estão incluídos na regra. Quando a regra é configurada e ativada, todos os dados do evento que corresponde aos testes de regras são automaticamente enviados aos destinos de encaminhamento especificadas. Para obter informações adicionais sobre como editar ou incluir uma regra, consulte o *Guia do Usuário* para seu produto.

Procedimento

1. Clique na guia **Ofensas Atividade de log**.
2. No menu de navegação, selecione **Regras**.

3. Edite ou adicione uma regra. Na página Resposta de regra, no assistente Regra, assegure-se que opção **Enviar para Destinos de Encaminhamento** foi selecionada.

Visualizando Destinos de Encaminhamento

A janela Destinos de Encaminhamento fornece informações valiosas sobre o encaminhamento de destinos. Estatísticas para os dados enviados para cada destino de encaminhamento são exibidas.

Por exemplo, é possível consultar as informações a seguir:

- O número total de eventos e fluxos que foram vistos para este destino de encaminhamento.
- O número de eventos ou fluxos que foram enviados para este destino de encaminhamento.
- O número de eventos ou fluxos que foram eliminados antes que o destino de encaminhamento fosse atingido.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Destinos de Encaminhamento**.
4. Visualize as estatísticas para seus destinos de encaminhamento.

Visualizando e Gerenciando Destinos de Encaminhamento

Utilize a janela Destino de Encaminhamento para visualizar, editar e excluir destinos de encaminhamento.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Destinos de Encaminhamento**.

   Estatísticas para os dados enviados para cada destino de encaminhamento são exibidas. Por exemplo, é possível consultar as informações a seguir:

   - O número total de eventos e fluxos que foram vistos para este destino de encaminhamento.
   - O número de eventos ou fluxos que foram enviados para este destino de encaminhamento.
   - O número de eventos ou fluxos que foram eliminados antes que o destino de encaminhamento fosse atingido.
4. Na barra de ferramentas, clique em uma ação, conforme descrito na tabela a seguir.

Tabela 70. Descrição das Ações da Barras de Ferramentas Destino de Encaminhamento

Ação	Descrição
Reconfigurar Contadores	Reconfigura os contadores para os parâmetros **Vistos**, **Enviados** e **Eliminados** para zero e os contadores começam a acumular novamente. **Dica:** É possível reconfigurar os contadores para fornecer uma visualização mais direcionada do desempenho de seus destinos de encaminhamento.
Editar	Altera o nome configurado, o formato, o endereço IP, a porta ou o protocolo.
Excluir	Exclui um destino de encaminhamento Se o destino de encaminhamento estiver associado a quaisquer regras ativas, você deverá confirmar que você deseja excluir o destino de encaminhamento.

Visualizando e Gerenciando Regras de Roteamento

A janela Regras de Roteamento de Evento fornece informações valiosas sobre suas regras de roteamento. É possível visualizar ou gerenciar filtros e ações configurados quando dados correspondem a cada regra.

Utilize a janela Regras de Roteamento de Evento para editar, ativar, desativar ou excluir uma regra. É possível editar uma regra de roteamento para alterar o nome configurado, Coletor de eventos, filtros ou opções de roteamento.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Regras de Roteamento**.
4. Selecione a regra de roteamento que você deseja gerenciar.
5. Para editar a regra de roteamento, na barra de ferramentas, clique em **Editar** e atualize os parâmetros.
6. Para remover a regra de roteamento, na barra de ferramentas, clique em **Excluir**.
7. Para ativar ou desativar a regra de roteamento, na barra de ferramentas, clique em **Ativar/Desativar**.

   Se você ativar uma regra de roteamento que está configurada para eliminar eventos, uma mensagem de confirmação será exibida.

Capítulo 18. Evento de armazenar e encaminhar

Utilize o recurso de Armazenamento e Encaminhamento para gerenciar planejamentos para o redirecionamento de eventos a partir de seus aparelhos dedicados a Coletor de eventos Processador de eventoscomponentes em sua implementação.

O recurso Armazenamento e Encaminhamento é suportado no Coletor de Eventos 1501 e Event Collector 1590. Para obter informações adicionais sobre blocos de construção, consulte o *QRadar Hardware Guide*.

Uma dedicado Coletor de eventos não processa eventos e ele não inclui um sistema Processador de eventos. Por padrão, um dedicado Coletor de eventos continuamente, encaminha os eventos para um Processador de eventos que você deve conectar utilizando o **Editor de implementação**. Utilize o recurso de Armazenamento e Encaminhamento para planejar um intervalo de tempo para quando você deseja que o Coletor de eventos para redirecionar eventos. Durante o tempo em que os eventos não são encaminhados, os eventos são armazenados localmente no dispositivo. Os eventos não são acessíveis na QRadar Console interface do usuário.

Use o recurso de planejamento para armazenar eventos durante o horário comercial. Encaminhe os eventos para uma Processador de eventos quando a transmissão não afetar negativamente sua largura de banda larga. Por exemplo, é possível configurar uma Coletor de eventos para encaminhar eventos para uma Processador de eventos durante eventos fora do horários comercial.

Visão geral de armazenamento e encaminhamento

O recurso de armazenamento e encaminhamento é suportado nos dispositivos de coletor de eventos 1501 e coletor de eventos 1590. Para mais ionformações nesses dispositivos, consulte o *QRadar guia de Hardware*.

Um Coletor de Eventos dedicado não processa eventos e não inclui um Processador de Eventos integrado. Por padrão, um coletor de evento dedicado encaminha continuamente eventos para um processador de eventos que deve ser conectado usando o Editor de Implementação. O recurso armazenar e encaminhar lhe permite agendar uma faixa de tempo para quando você quiser que o Coletor de eventos encaminhe os eventos. Durante o período de tempo em que os eventos não forem encaminhados, os eventos são armazenados localmente, no dispositivo e não serão acessíveis usando o controle de interface.

Este recurso de planejamento permite armazenar eventos durante seu horário comercial, e em seguida encaminhar os eventos para um processador de eventos, durante um período de tempo em que a transmissão não afeta negativamente sua largura de banda da rede. Por exemplo, é possível configurar um Coletor de eventos para encaminhar para um processador de eventos apenas durante as horas não comerciais, como por exemplo, da meia noite às seis da manhã.

Visualizando a Lista de Planejamento de Armazenamento e Encaminhamento

Utilize a janela Armazenamento e Encaminhamento para ver uma lista de planejamentos. Os planejamentos incluem estatísticas que ajudam a avaliar o status, o desempenho e o progresso de seus planejamentos.

Antes de Iniciar

Você deve criar um planejamento. Por padrão, na primeira vez em que você acessar a janela Armazenamento e Encaminhamento, nenhum planejamento será listado.

Sobre Esta Tarefa

É possível usar opções na barra de ferramentas e a caixa de listagem **Exibir** para alterar sua visualização da lista de planejamentos. Altere sua visualização da lista para focar nas estatísticas de diferentes pontos de vista. Por exemplo, se você deseja visualizar as estatísticas para um determinado Coletor de Eventos, poderá selecionar **Coletores de Eventos** na lista **Exibir**. A lista, então, agrupa pela coluna **Coletor de Eventos** e torna mais fácil para você localizar o Coletor de eventos que deseja investigar.

Por padrão, a lista de Armazenamento e Encaminhamento está configurada para exibir a lista que é organizada pelo planejamento (**Exibir** > **Planejamentos**).

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Armazenamento e Encaminhamento**.
4. Na janela Armazenamento e Encaminhamento, visualize os parâmetros para cada planejamento.

   A tabela a seguir descreve alguns dos parâmetros para o planejamento.

Tabela 71. Parâmetros da Janela Armazenamento e Encaminhamento

Parâmetro	Descrição
Exibição	A opção **Planejamentos** mostra uma hierarquia do relacionamento pai-filho entre os planejamentos, Processadores de Eventoss e os QRadar Event Collectors associados. A opção **Coletores de Eventos** mostra o nível mais baixo na hierarquia, que é uma lista de QRadar Event Collectors. A opção **Processadores de Eventos** mostra uma hierarquia de relacionamento pai-filho entre os Processadores de Eventos e os QRadar Event Collectors associados.

Tabela 71. Parâmetros da Janela Armazenamento e Encaminhamento (continuação)

Parâmetro	Descrição
Nome	Para a opção **Planejamentos**, a coluna **Nome** é exibida no seguinte formato. • **Primeiro Nível** representa o nome do planejamento. • **Segundo Nível** representa o nome do Processador de eventos. • **Terceiro Nível** representa o nome do Coletor de eventos. Para a opção **Processadores de Eventos**, a coluna é exibida no formato a seguir • **Primeiro Nível** representa o nome do Processador de eventos. • **Segundo Nível** representa o nome do Coletor de eventos. **Dica:** É possível utilizar o símbolo de mais (+) e o símbolo de menos (-) ao lado do nome ou as opções na barra de ferramentas para expandir e reduzir a árvore de hierarquia. Também é possível expandir e reduzir a árvore de hierarquia utilizando as opções na barra de ferramentas.
Nome do Planejamento	Exibe o nome do planejamento para as opções **Coletores de Eventos** ou **Processadores de Eventos**. Se um Processador de eventos está associado a mais de um planejamento, o **Nome de Planejamento** mostra `Múltiplos`*n*, em que *n* é o número de planejamentos. **Dica:** Clique no símbolo de mais (+) para visualizar os planejamentos associados.

Tabela 71. Parâmetros da Janela Armazenamento e Encaminhamento (continuação)

Parâmetro	Descrição
Último Status	Exibe o status do processo de Armazenamento e Encaminhamento: • **Encaminhamento** indica que o redirecionamento de eventos está em andamento. • **Encaminhamento Concluído** indica que o encaminhamento de eventos foi concluído com êxito e os eventos estão armazenados localmente no Coletor de eventos. Os eventos armazenados são encaminhados quando o planejamento indica que o encaminhamento pode iniciar novamente. • **Aviso** indica que a porcentagem de eventos que permanecem no armazenamento excede a porcentagem de tempo restante no planejamento de Armazenamento e Encaminhamento. • **Erro** indica que o encaminhamento de eventos foi interrompido antes que todos os eventos armazenados fossem encaminhados. • **Inativo** indica que nenhum QRadar Event Collectors foi designado ao planejamento ou um QRadar Event Collectors designado não está recebendo nenhum evento. **Dica:** Mova seu ponteiro do mouse sobre a coluna **Último Status** para visualizar um resumo do status.
Eventos Encaminhados	Exibe o número de eventos (em K, M ou G) encaminhados na sessão atual. **Dica:** Mova o ponteiro do mouse sobre o valor na coluna **Eventos Encaminhados** para visualizar o número de eventos.
Eventos Restantes	Exibe o número de eventos (em K, M ou G) restantes a serem encaminhados na sessão atual. **Dica:** Mova o ponteiro do mouse sobre o valor na coluna **Eventos Restantes** para visualizar o número de eventos.
Taxa do Evento Média	Exibe a taxa média na qual os eventos estão sendo encaminhados do Coletor de eventos para o Processador de eventos. **Dica:** Mova o ponteiro do mouse sobre o valor na coluna **Taxa Média do Evento** para visualizar a média de eventos por segundo (EPS).

Tabela 71. Parâmetros da Janela Armazenamento e Encaminhamento (continuação)

Parâmetro	Descrição
Taxa de Evento Atual	Exibe a taxa na qual os eventos estão sendo encaminhados do Coletor de eventos para o Processador de eventos **Dica:** Mova o ponteiro do mouse sobre o valor na coluna **Taxa de Evento Atual** para visualizar os eventos atuais por segundo (EPS)
Limite de Taxa de Transferência	O limite de taxa de transferência é configurável. O limite de taxa de transferência pode ser configurado para exibir em Kilobit por segundo (kbps), megabits por segundo (Mbps) ou gigabits por segundo (Gbps).

Criando um Novo Planejamento de Armazenamento e Encaminhamento

Utilize o assistente Planejamento de Armazenamento e Encaminhamento para criar um planejamento que controla quando o Coletor de eventos inicia e para o encaminhamento de dados para um Processador de eventos.

É possível criar e gerenciar vários planejamentos para controlar o encaminhamento de eventos a partir de vários QRadar Event Collectors em uma implementação distribuída geograficamente.

Antes de Iniciar

Assegure que seu Coletor de eventos dedicado seja incluído em sua implementação e conectado a um Processador de eventos. A conexão entre um Coletor de eventos e um Processador de eventos é configurada no **Editor de Implementação**.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Armazenamento e Encaminhamento**.
4. Clique em **Ações** > **Criar**.
   a. Clique em **Avançar** para acessar a página Selecionar Coletores.
   b. Na página Selecionar Coletores, configure os parâmetros.

      Se o Coletor de eventos que você deseja configurar não estiver listado, ele não poderá ser incluído em sua implementação. Se isso acontecer, utilize o **Editor de Implementação** para incluir o Coletor de eventos e, em seguida, continue.
   c. Na página Opções de Planejamento, configure os parâmetros.

      Para configurar a taxa de transferência de encaminhamento, a taxa de transferência mínima é 0. A taxa de transferência máxima é 9.999.999. Um valor 0 significa que a taxa de transferência é ilimitada.
   d. Conclua a configuração.

Agora é possível visualizar o planejamento na janela Armazenamento e Encaminhamento. Depois de criar um novo planejamento, pode demorar até 10 minutos para que as estatísticas iniciem a exibição na janela Armazenamento e Encaminhamento.

Editando um Planejamento de Armazenamento e Encaminhamento

É possível editar um planejamento de **armazenamento e encaminhamento** para incluir ou remover QRadar Event Collectors e alterar o parâmetro de planejamento. Depois da edição de um planejamento de **armazenamento e encaminhamento**, as estatísticas que são exibidas na lista **Armazenamento e Encaminhamento** são reconfiguradas.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do sistema**.
3. Clique no ícone **Armazenamento e Encaminhamento**.
4. Selecione o planejamento que você deseja editar.
5. Clique em **Ações** > **Editar**.

   Também é possível clicar duas vezes em um planejamento para edição.
6. Clique em **Avançar** para acessar a página Selecionar Coletores.
7. Na página Selecionar Coletores, edite os parâmetros.
8. Clique em **Avançar** para ir para a página Opções de Planejamento.
9. Na página Opções de Planejamento, edite os parâmetros de planejamento.
10. Clique em **Avançar** para ir para a página Resumo.
11. Na página Resumo, confirme as opções que você editou para este planejamento.

    Depois de editar um planejamento, pode demorar até 10 minutos para que as estatísticas se atualizem na janela Armazenamento e Encaminhamento.

Excluindo um planejamento de Armazenamento e Encaminhamento

É possível excluir um planejamento de **Armazenamento e Encaminhamento**.

Procedimento

1. No menu de navegação, clique em **Configuração do sistema**.
2. Clique no ícone **Armazenamento e Encaminhamento**.
3. Selecione o planejamento que deseja excluir.
4. Clique em **Ações** > **Excluir**.

   Depois que o planejamento for excluído, o QRadar Event Collectors associado continuará o encaminhamento contínuo de eventos para seu Processador de eventos designado.

Capítulo 19. Visão geral da Ferramenta de Gerenciamento de Conteúdo

Utilizando a Ferramenta de Gerenciamento de Conteúdo (CMT), você pode exportar o conteúdo de segurança e de configuração do IBM Security QRadar em um formato externo, portátil.

é possível importar o conteúdo exportado para o que você exportou a partir do mesmo sistema ou em outro sistema. QRadar SIEM

Essa nota técnica é destinada a uso pelo Suporte ao Cliente IBM, Serviços Professional e selecione clientes com conhecimento avançado do QRadar SIEM .

Você pode exportar e importar o seguinte conteúdo:

- Painéis
- Relatórios
- Grupos
- Procuras Salvas
- Coletas de Dados de Referência, incluindo Sets Reference
- Customizadas e Propriedades Calculado
- Regras Customizadas e Building Blocks)
- Fonte de Log
  - tipos de Origem de Log
  - Efetue de Origem categorias
  - extensões de origem de log
  - Grupos de Fontes de Log
- Grupos de Regras/Blocos de Construção
- Grupos de Relatórios
- Pesquisar Grupos
  - Grupos de Procura de Evento
  - Grupos de Procura de Fluxo

Você não pode utilizar CMT para importar e exportar critérios de procura salvos para Ofensa, Ativos, e Vulnerabilidade.

Os seguintes parâmetros sempre se comportam da mesma, independentemente do valor do parâmetro `--ação` que você utiliza.

Tabela 72. Parâmetros para CMT

Parâmetro	Descrição
`-h [--help] ACTIONTYPE`	Exibe ajuda que é específico para a opção ACTIONTYPE ou mensagem de ajuda geral se nenhuma opção ACTIONTYPE está especificado.
`-q [--quiet]`	Nenhuma saída aparece na tela quando CMT é executado.
`-v [--verbose]`	Utilizar nível de verbose quando você efetuar login para visualizar informações CMT padrão no nível da.

Tabela 72. Parâmetros para CMT (continuação)

Parâmetro	Descrição
`-d [--debug]`	Utilize o nível de depuração quando você efetuar login para ver informações mais detalhadas, como logs para suporte ao cliente.

Se nenhuma opção ACTIONTYPE válido estiver disponível, o CMT exibe ajuda geral. Se o ACTIONTYPE é válido, a CMT exibe a ajuda específicos da ação.

Ao importar e exportar *conteúdo customizado*, a CMT verificações de conteúdo dependências e, em seguida, inclui o conteúdo associado na importação ou exportação. Por exemplo, quando o CMT detecta que um relatório customizado está associado a procuras salvas customizadas, as procuras salvas customizadas também são exportadas.

Exportando todos os conteúdo customizado

Exportar todo o conteúdo customizado em uma única ação com a Ferramenta de Gerenciamento de Conteúdo (CMT).

Procedimento

1. Utilizando o SSH, efetue login no IBM Security QRadar como o usuário raiz.
2. Vá para `/opt/qradar/bin` diretório e exportar o conteúdo:

   `/opt/qradar/bin cd`

   - Para exportar todo o conteúdo que exclui as referências de acumulação de dados, digite o seguinte comando:

     `./contentManagement.pl -a exportar todos os -c`

   - Para exportar todo o conteúdo que inclui dados acumulados, digite o seguinte comando:

     `./contentManagement.pl -o [directory_path] -a exportar -c todos -g`

   Se nenhum diretório de saída for especificado quando você utiliza a opção `-o` , o conteúdo é exportado para o diretório atual do usuário. Se o diretório especificado não existir, ele será criado.

   O conteúdo exportado é compactado em um arquivo .tar.gz e exportados para o diretório especificado. O exemplo a seguir mostra um nome de arquivo .tar.gz : `report-ContentExport-20120419101803.tar.gz`. Você pode manualmente alterar o nome do arquivo exportado. A tabela a seguir descreve os parâmetros utilizados nos comandos para exportar todos os conteúdo customizado.

Tabela 73. parâmetros de Exportar (todo o conteúdo customizado)

Parâmetro	Descrição
`-a export`	A ação a ser executada.
`-o PATH`	O diretório no qual o conteúdo é gravado. Se o diretório não for especificado, o diretório atual do usuário será utilizado.
`-g`	Incluir dados acumulados na exportação.

Exportando todas as conteúdo customizado de um tipo específico

Exportar todo o conteúdo customizado de um tipo específico em uma ação, em vez de exportar itens de conteúdo individualmente.

Procedimento

1. Utilizando o SSH, efetue login no IBM Security QRadar como o usuário raiz.
2. Vá para `/opt/qradar/bin` e exportar o conteúdo de um tipo específico :
   - Para exportar todo o conteúdo customizado de um tipo específico, digite o seguinte comando:

     ```
     ./contentManagement.pl --action export --content-type Content_Type --id todos
     ```
   - Para exportar todo o conteúdo customizado que inclui dados acumulados, digite o seguinte comando:

     ```
     ./contentManagement.pl --action export --content-type Content_Type
      --id todos ---visualização global
     ```

   A tabela a seguir descreve os parâmetros em comandos para exportar o conteúdo customizado de um tipo específico.

Tabela 74. Parâmetros de Exportação (de conteúdo customizado de um tipo específico)

Parâmetro	Descrição
`-c` *CONTENT_TYPE*	O tipo de conteúdo que você deseja importar ou exportar. Você pode digitar o tipo de conteúdo como uma cadeia de texto ou digite o identificador numérico correspondente. Consulte Tipos de conteúdo.
`-o` *PATH*	O diretório no qual o conteúdo é gravado. Se não for especificado o diretório atual do usuário será utilizado.
`-i`	O identificador de uma instância específica de conteúdo customizado, como um único relatório ou um conjunto de referências único. Especifique `Todos` para exportar todo o conteúdo da condição de tipo de conteúdo.
`-g`	Incluir dados acumulados na exportação.

Tabela 75. Tipos de conteúdo

Tipo de Conteúdo Customizado	Cadeia de Texto	Identificador numérico
Todo o conteúdo customizado	`todas as`	n/a
lista de conteúdo customizado	`pacote`	n/a
Painel	`Painel`	4
Relatórios	`relatório`	10
Procuras Salvas	`search`	1
FGroup[1]	`fgroup`	12
FGroup Digite	`fgrouptype`	13
Custom Rules	`customrule`	3
Propriedades customizadas	`customproperty`	6
Fonte de Log	`sensordevice`	17
Tipo de Origem de Log	`sensordevicetype`	24
Categoria de Origem de Log	`sensordevicecategory`	18
Extensões de Fonte de Log	`deviceextension`	16

Tabela 75. Tipos de conteúdo (continuação)

Tipo de Conteúdo Customizado	Cadeia de Texto	Identificador numérico
Coleções dos dados de referência	`referencedata`	28
[1]Um FGroup representa um grupo de conteúdo dentro de QRadar SIEM, como um grupo de origens de log, grupo de relatórios, ou grupo de procura. Esses grupos podem ser grupos de procura de eventos de atividade de log, fluxo de grupos de procura, grupos de crime, grupos de recursos, grupos de relatórios, grupos de procura de gerenciamento de vulnerabilidades, ou grupos de fonte de log.		

O pacote configurável de exportação contém mais itens de dados que o usuário selecionado, porque cada item das exportações com todas as dependências.

O conteúdo exportado é compactado em um arquivo .tar.gz e exportados para o diretório especificado. É possível também alterar manualmente o nome do arquivo exportado.

Procurando Conteúdo

Utilize o comando **procura** para consultar seu conteúdo customizado para os valores de cadeia sejam exclusivos. Você precisará destas informações quando você exporta uma instância específica de conteúdo customizado como um único relatório ou um conjunto de referência única, ou se um pacote contiver diferentes content-type IDs.

Procedimento

1. Utilizando o SSH, efetue login no IBM Security QRadar como o usuário raiz.
2. Vá para `/opt/qradar/bin` e procure conteúdo customizado :

   `./contentManagement.pl procura -a -c` *`content-type`* `-r` *`regex`*

   Exemplo:

   ```
   # /opt/qradar/bin/contentManagement.pl --action search
   --content-type  customrule --regex "PCI.*"
   /opt/qradar/bin/contentManagement.pl --action search
   --content-type dashboard --regex "Overview.*"
   ```

   A tabela a seguir descreve os parâmetros utilizados no Content Management Tool (CMT) de comandos.

Tabela 76. Parâmetros de Procura

Parâmetro	Descrição
`-c ou --content-type` *`content-type`*	A cadeia de texto ou identificador numérico do tipo de conteúdo para exportação. O valor pode ser qualquer coisa a partir da tabela de tipo de conteúdo.
`-r ou --regex` *`regex`*	A expressão regular (regex) é utilizado para procurar um content-type. Todo o conteúdo correspondentes é exibida.

Tabela 77. Os tipos de conteúdo CMT

tipo de conteúdo customizado	Sequência de texto	Identificador numérico
Painel	console	4
Relatórios	relatório	10
Procuras Salvas	pesquisar	1
FGroup	fgroup	12
FGroup Digite	fgrouptype	13
Custom Rules	customrule	3
Propriedades customizadas	customproperty	6
Fonte de Log	sensordevice	17
Tipo de Origem de Log	sensordevicetype	24
Categoria de Origem de Log	sensordevicecategory	18
Extensões de Fonte de Log	deviceextension	16
Coleções dos dados de referência	referencedata	28

Exportando vários itens de conteúdo customizado

Exportar vários itens de conteúdo customizado na mesma ação, como regras customizadas, com a Ferramenta de Gerenciamento de Conteúdo (CMT).

Procedimento

1. Utilizando o SSH, efetue login no IBM Security QRadar como o usuário raiz.
2. Crie um arquivo do pacote, incluindo todos os itens requeridos conteúdo customizado. Cada item de conteúdo customizado é composto de um tipo de conteúdo de exportação, seguido por uma lista separada por vírgula de IDs.

   Exemplo: Um usuário deseja exportar dois painéis, que possuem ID 5 e ID 7, todas as regras customizadas, e um grupo. O arquivo que está armazenado no diretório `/root/myPackage` contém as seguintes entradas:

   ```
   dashbord, 5,7
   customrule,tudo
   fgroup, 77
   ```

3. Vá para `/opt/qradar/bin`, e exportar e salvar todos os itens:
   - Se você desejar exportar todos os itens no arquivo `/root/myPackage` e salvar o conteúdo exportado no diretório atual, digite o seguinte comando:

     ```
     ./contentManagement.pl -f /root/myPackage -a -c pacote de exportação
     ```

   - Se você desejar exportar todos os itens no arquivo `/root/myPackage` , que inclui dados acumulados e salvar a saída no diretório `/store/cmt/exports` , digite o seguinte comando:

     ```
     ./contentManagement.pl --action export --content-type package --file
     /root/myPackage --output-directory /store/cmt/exports --global-view
     ```

   O conteúdo exportado é compactado para um `.tar.gz` e exportado no diretório especificado, ou o diretório atual do usuário. Você pode manualmente alterar o nome do arquivo exportado.

Depois de utilizar um arquivo de pacote, um modelo de pacote é gravado em `/store/cmt/packages`. Um arquivo de pacote é reutilizável, e pode ser armazenado em qualquer lugar.

Tabela 78. Exportar parâmetros (customizados vários itens de conteúdo)

Parâmetro	Descrição
`-a [--ação] exportar`	A ação a ser executada.
`-c [--content-type] pacote`	O tipo de conteúdo a ser exportado. A opção "pacote" é o necessário de tipo de conteúdo.
`-f [--file] FILE`	O caminho do arquivo e o nome do arquivo, como `/root/myPackage` do arquivo do pacote, que contém itens de conteúdo customizado. Insira um arquivo para cada linha. O tipo de exportação é seguido por uma lista de um ou mais IDs.
`-o [-output-directory] PATH`	O diretório no qual o conteúdo é gravado. Se o diretório não for especificado, o diretório atual do usuário será utilizado.

Exportando um item de conteúdo único customizado

Exportar um único item de conteúdo customizado, como uma regra customizada ou um critério de procura customizado.

Procedimento

1. Utilizando o SSH, efetue login no IBM Security QRadar como o usuário raiz.
2. Vá para o `/opt/qradar/bin cd` e exportar um item de conteúdo customizada única :
   - Para exportar um item de conteúdo customizada única que exclui dados acumulados, digite o seguinte comando:

     ```
     ./contentManagement.pl -a export -o <directory_path> -c
     <content_type> -i string_ID_value
     ```
   - Para exportar um item de conteúdo customizado único que inclui dados acumulados, digite o seguinte comando:

     ```
     ./contentManagement.pl -a export -o <directory_path> -c
     <content_type> -i string_ID_value -g
     ```

Tabela 79. Parâmetros de Exportação (item de conteúdo único)

Parâmetros	Descrição
`-o` *`directory_path`*	O diretório para o qual você deseja exportar o conteúdo. Se um diretório de saída não for especificado, o conteúdo é exportado para o diretório atual do usuário.
`-c` *`content_type`*	O tipo de conteúdo que você deseja exportar. Você pode digitar o tipo de conteúdo como uma cadeia de texto ou digite o identificador numérico correspondente. Consulte Tipos de Conteúdo.
`-a`	Especifica se você deseja exportar o conteúdo customizado especificado.

Tabela 79. Parâmetros de Exportação (item de conteúdo único) (continuação)

Parâmetros	Descrição
`-i` *`string_ID_value`*	O identificador da instância específica de conteúdo customizado, como um único relatório ou um único conjunto de referências. Você pode localizar o `string_ID_value` , consultar o banco de dados postgreSQL com a opção de procura CMT.

O conteúdo exportado é compactado em um arquivo `.tar.gz` e exportado para o diretório especificado. Você pode manualmente alterar o nome do arquivo exportado.

Importando conteúdo customizado

Você pode importar conteúdo customizado exportadas no mesmo sistema que você exportou a partir do IBM Security QRadar SIEM ou outro sistema QRadar SIEM.

Antes de Iniciar

Se você deseja importar o conteúdo em outro sistema QRadar SIEM , você deve transferir o arquivo de saída para o outro sistema antes de continuar com este procedimento.

Sobre Esta Tarefa

O Content Management Tool (CMT) converte arquivos importados para o local QRadar SIEM versão, se necessário. A ação importar importa o conteúdo que ainda não esteja no sistema. Ao importar pacotes de conteúdo que possuem origens de log, confirme se os RPMs DSM e o protocolo são instalados e atual no sistema de destino.

Nota: Não iniciar várias importações no mesmo sistema ao mesmo tempo.

Procedimento

1. Utilizando o SSH, efetue login no QRadar SIEM como o usuário raiz.
2. Acesse o diretório no qual você exportou o arquivo de conteúdo.
   `cd` *`directory_name`*
3. Para listar os arquivos no diretório, digite o seguinte comando:
   `ls-al`
   A saída deste comando é semelhante ao exemplo a seguir :

```
raiz de drwxr-xr-x 16:39 18/04 fgroup-ContentExport-20120418163707 24576 raiz do 2
 -rw-r-r- 1 root root 324596 18/04 16:39 fgroup-ContentExport-20120418163707.tar.gz
 raiz de drwxr-xr-x 16:56 18/04 report-ContentExport-20120418165529 4096 raiz do 2
 -rw-r-r- 1 root root 42438 18/04 16:56 report-ContentExport-20120418165529.tar.gz
 raiz de drwxr-xr-x 10:18 19/04 report-ContentExport-20120419101803 4096 raiz do 2
 -rw-r-r- 1 root root 3295 19/04 10:18 report-ContentExport-20120419101803.tar.gz
```

   Neste exemplo, `report-ContentExport-20120419101803.tar.gz` é um nome do arquivo de exportação.

Se você descompactar o arquivo .tar.gz manualmente enquanto o arquivo está no diretório de exportação padrão ou customizado, você deve mover os arquivos e diretórios extraídos para outro local antes de importar o arquivo tar.gz.

4. Digite o comando a seguir:

   ```
   /opt/qradar/bin/contentManagement.pl -a importar -f export_file_path
   ```

   Exemplo:

   ```
   /opt/qradar/bin/contentManagement.pl --action import
    --arquivo fgroup-ContentExport-20120418163707.tar.gz
   ```

Tabela 80. Parâmetros de Importação

Parâmetro	Descrição
`-a`	A ação a ser executada.
`-f export_file_path`	O arquivo que contém os dados de conteúdo exportado. Este arquivo é um arquivo compactado `tar.gz`, ou um arquivo que contém a representação XML do conteúdo exportado. Se os arquivos estão descritos no arquivo representação XML, relatório ou logotipo, ou ambos, os arquivos também deve aparecer em um subdiretório. Utilize o caminho incluído na representação XML. A opção de arquivo é um caminho absoluto ou um caminho relativo para o diretório de usuários atual.

CMT utiliza os seguintes parâmetros para confirmar que importa o registro correto.

Tabela 81. Parâmetros de Importação

tipo de conteúdo customizado	chave de Exclusividade
Painel	Nome e proprietário
Relatórios	N/A, os relatórios são sempre exclusivos
customviewparams – Procura Salva	ID
Grupo (FGroup)	Nome e parent_id
Tipo de Grupo (tipo de FGroup)	Nome
Regra Customizada	UUID
Propriedades customizadas	propertyname
Fonte de Log	devicename e eccomponentid
Tipo de Origem de Log	devicetypename
Categoria de Origem de Log	ID
extensões de origem de log	Nome
Dados de referência	ID

- Se a lista de usuários no sistema de origem é diferente da lista de usuários no sistema de destino, CMT inclui todos os dados para o sistema de destino.
- CMT exibe o seguinte erro quando você importar e atualizar Referência de Dados: `violação de restrição de chave estrangeira`. Este erro é causado

por dados ativamente coletado durante a exportação de dados de referência. Para evitar esse problema, execute o processo de exportação quando nenhum dado de referência está sendo coletada.

Atualizando Conteúdo

Utilize a ação de atualização para atualizar o conteúdo existente, e incluir o novo conteúdo para o sistema.

Antes de Iniciar

Quando você importa pacotes configuráveis de conteúdo que tenham origens de log, confirme se os RPMs de DSM e de Protocolo estão instalados e estão atualmente no sistema de destino.

Procedimento

1. Utilizando o SSH, efetue login no IBM Security QRadar como o usuário raiz.
2. Para atualizar o arquivo exportado, vá para o diretório em que você exportou o arquivo de conteúdo e digite o seguinte comando:

   ```
   /opt/qradar/bin/contentManagement.pl update -a -f export_file_path
   ```

   Exemplo:

   ```
   /opt/qradar/bin/contentManagement.pl
   update -a --arquivo fgroup-ContentExport-20120418163707.tar.gz
   ```

Tabela 82. Atualizar parâmetros

Parâmetro	Descrição
`-a` ou `--action update`	Altera as informações no sistema.
`-f` ou `--file`	O arquivo `tar.gz` compactado que contém os dados de conteúdo exportados. A opção de arquivo pode ser um caminho absoluto ou relativo para o diretório atual do usuário.

Detalhes da Ferramenta de Gerenciamento de Conteúdo de auditoria

Utilize os eventos de auditoria gerados pela ferramenta de gerenciamento de conteúdo (CMT) para confirmar o conteúdo correto exportações e importações.

Detalhes de auditoria para todas as ações

A tabela a seguir lista eventos de auditoria que são criados para exportar, importar, procurar e atualizar ações. A saída de auditoria contém informações para os eventos de auditoria a seguir :

- Usuário de shell
- IP Remoto
- Lista de argumentos que são transmitidos como a carga útil do evento

Os campos de evento normalizado para a auditoria são `Source IP = Remote IP = Usuário Shell do Usuário`.

Tabela 83. Detalhes de auditoria

Ação/ nome do evento de auditoria	Nome do Evento	Descrição de evento
ExportInitiated	Exportar Conteúdo Iniciado	O usuário iniciou conteúdo de exportação
ExportComplete **Nota:** Também inclui lista de argumentos que são exportadas na saída de auditoria	Conteúdo de Exportação Concluída	exportação de conteúdo está concluída
ImportInitiated	Conteúdo de Importação Iniciado	importar conteúdo iniciada pelo usuário
ImportComplete	Importação Concluída Conteúdo	importação de conteúdo está concluída
UpdateInitiated	Início de Atualização de Conteúdo	atualizar conteúdo iniciada pelo usuário
UpdateComplete	Conteúdo de Atualização Concluída	atualização de conteúdo está concluída
SearchInitiated	Iniciado Content Search	O usuário iniciou conteúdo de procura

eventos de auditoria para ações de importação e atualização

Os eventos de auditoria a seguir são gerados quando você importa ou atualizar o conteúdo.

Tabela 84. os eventos de auditoria de importação e atualização

Ação / nome do evento de auditoria	Nome do Evento	detalhes de Saída, representação de cadeia
ArielProperty	ArielPropertyAdded	o que foi incluído
ArielProperty	ArielPropertyModified	o que foi modificado
QidMap	QidMapEntryAdded	o que foi incluído
QidMap	QidMapEntryModified	o que foi modificado
DeviceExtension	DeviceExtensionAdded	o que foi incluído
DeviceExtension	DeviceExtensionModified	o que foi modificado
DeviceExtension	DeviceExtension AssociationModified	o que foi modificado

Tabela 84. os eventos de auditoria de importação e atualização (continuação)

Ação / nome do evento de auditoria	**Nome do Evento**	**detalhes de Saída, representação de cadeia**
DeviceExtension	DeviceExtension AssociationModified	o que foi modificado
Sensordevice	SensorDeviceAdded	o que foi incluído
Sensordevice	SensorDeviceModified	o que foi modificado
ReferenceData	ReferenceDataCreated	o que foi incluído
ReferenceData	ReferenceDataUpdated	o que foi atualizado
Fgroup	FgroupAdded	o que foi incluído
Fgroup	FgroupModified	o que foi modificado
Fgroup	FgroupItemsAdded	o que foi incluído
CRE	RuleAdded	o que foi incluído
CRE	RuleModified	o que foi modificado
Retenção	RetentionSettingsUpdated	o que foi modificado
Painel	DashboardAdded	o que foi incluído
Relatórios	ReportAdded	o que foi incluído
Relatórios	ReportModified	o que foi modificado

Capítulo 20. Configuração de trap SNMP

No IBM Security QRadar, é possível configurar uma regra para gerar uma resposta da regra que envia um trap SNMP quando as condições configuradas são atendidas. O QRadar age como um agente para enviar os traps SNMP para outro sistema.

Um trap de Protocolo Simples de Gerenciamento de Rede (SNMP) é uma notificação de evento ou de ofensa que o QRadar envia para um host SNMP configurado para processamento adicional.

Customize os parâmetros de configuração do SNMP no assistente de regras customizadas e modifique os traps SNMP que o mecanismo de regras customizadas envia para outro software para gerenciamento. O QRadar fornece dois traps padrão. No entanto, é possível incluir traps customizados ou modificar os traps existentes para usar novos parâmetros.

Para obter mais informações sobre o SNMP, acesse o website The Internet Engineering Task Force (http://www.ietf.org/) e digite `RFC 1157` no campo de procura.

Customizando as informações de trap SNMP enviadas para outro sistema

No IBM Security QRadar, você pode editar os parâmetros de trap SNMP para customizar as informações que são enviadas para outro sistema de gerenciamento SNMP quando uma condição de regra é atendida.

Restrição: Os parâmetros de trap SNMP serão exibidos no assistente de regras customizadas apenas se o SNMP estiver ativado nas configurações do sistema QRadar.

Procedimento

1. Use SSH para efetuar login no QRadar como o usuário raiz.
2. Acesse o diretório `/opt/qradar/conf` e faça cópias de backup dos seguintes arquivos:
   - `eventCRE.snmp.xml`
   - `offenseCRE.snmp.xml`
3. Abra o arquivo de configuração para edição.
   - Para editar os parâmetros SNMP para regras de eventos, abra o arquivo `eventCRE.snmp.xml`.
   - Para editar os parâmetros SNMP para regras de ofensa, abra o arquivo `offenseCRE.snmp.xml`.
4. Dentro do elemento <snmp> e antes do elemento <creSNMPTrap>, insira a seguinte seção, atualizando os rótulos conforme necessário:

```
<creSNMPResponse name="snmp_response_1">
  <custom name="MyColor">
    <string label="What is your favorite color?"/>
</custom>
  <custom name="MyCategory">
    <list label="Select a category">
```

```
        <option label="Label1" value="Category1"/>
        <option label="Label2" value="Category2"/>
      </list>
    </custom>
  </creSNMPResponse>
```

5. Salve e feche o arquivo.
6. Copie o arquivo do diretório `/opt/qradar/conf` para o diretório `/store/configservices/staging/globalconfig`.
7. Efetue login na interface do QRadar.
8. Na guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.

   Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

O que Fazer Depois

Customize a saída do trap SNMP..

Customizando a saída do trap SNMP

O IBM Security QRadar usa o SNMP para enviar traps que fornecem informações quando as condições de regras são atendidas.

Por padrão, o QRadar usa a base de informações de gerenciamento (MIB) do QRadar para gerenciar os dispositivos na rede de comunicações. No entanto, você pode customizar a saída dos traps SNMP para aderir a outro MIB.

Procedimento

1. Use SSH para efetuar login no QRadar como o usuário raiz.
2. Acesse o diretório `/opt/qradar/conf` e faça cópias de backup dos seguintes arquivos:
   - `eventCRE.snmp.xml`
   - `offenseCRE.snmp.xml`
3. Abra o arquivo de configuração para edição.
   - Para editar os parâmetros SNMP para regras de eventos, abra o arquivo `eventCRE.snmp.xml`.
   - Para editar os parâmetros SNMP para regras de ofensa, abra o arquivo `offenseCRE.snmp.xml`.
4. Para alterar o trap que é usado para notificação do trap SNMP, atualize o texto a seguir com o identificador de objeto (OID) de trap apropriado:

   ```
   -<creSNMPTrap version="3" OID="1.3.6.1.4.1.20212.1.1"
   name="eventCRENotification">
   ```

5. Use a tabela a seguir para ajudá-lo a atualizar as informações de ligação de variável:

   Cada ligação de variável associa uma instância de objeto MIB particular ao seu valor atual.

Tabela 85. Tipos de valores para a ligação de variável

Tipo de valor	Descrição	Exemplo
`string`	Caracteres alfanuméricos É possível configurar vários valores.	
`integer32`	Um valor numérico	`name="ATTACKER_PORT" type="integer32">%ATTACKER_PORT%`
`oid`	Cada trap SNMP transporta um identificador que é designado a um objeto dentro do MIB	`OID="1.3.6.1.4.1.20212.2.46"`
`gauge32`	Um intervalo de valor numérico	
`counter64`	Um valor numérico que incrementa em um intervalo mínimo e máximo definido	

6. Para cada um dos tipos de valor, inclua qualquer um dos campos a seguir:

Tabela 86. Campos para as ligações de variáveis

Campo	Descrição	Exemplo
`Nativo`	Para obter mais informações sobre esses campos, consulte o arquivo `/opt/qradar/conf/snmp.help`.	**Exemplo:** [1]Se o tipo de valor for `ipAddress`, você deverá usar uma variável que é um endereço IP. O tipo de valor da sequência aceita qualquer formato.

`Customizado`	Informações de trap SNMP customizado que você configurou para o assistente de regras customizadas	**Exemplo:** [1]Se você usou as informações do arquivo padrão e deseja incluir essas informações no trap SNMP, inclua o código a seguir:
		`<variableBinding name="My Color Variable Binding" OID="1.3.6.1.4.1.20212.3.1" type="string">`
		`My favorite color`
		`is %MyColor%</variableBinding>`

[1]Circunde o nome do campo com os sinais de porcentagem (%). Dentro dos sinais de porcentagem, os campos devem corresponder ao tipo de valor.		

7. Salve e feche o arquivo.
8. Copie o arquivo do diretório `/opt/qradar/conf` para o diretório `/store/configservices/staging/globalconfig`.
9. Efetue login na interface do QRadar.
10. Na guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.

    Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Incluindo um trap SNMP customizado no QRadar

Nos produtos IBM Security QRadar, você pode criar uma nova opção para a seleção de trap SNMP no assistente de regras customizadas. Os nomes de trap que são especificados na caixa de listagem são configurados no arquivo de configuração `snmp-master.xml`.

Procedimento

1. Use SSH para efetuar login no QRadar como o usuário raiz.
2. Acesse o diretório `/opt/qradar/conf`.
3. Crie um arquivo de configurações SNMP para o novo trap.

   Dica: Copie, renomeie e modifique um dos arquivos de configurações SNMP existentes.
4. Faça uma cópia de backup do arquivo `snmp-master.xml`.
5. Abra o arquivo `snmp-master.xml` para edição.
6. Inclua um novo elemento <include>.

   O elemento <include> possui os seguintes atributos:

Tabela 87. Atributos para o elemento <include>

Atributo	Descrição
`name`	Exibido na caixa de listagem
`uri`	O nome do arquivo de configurações SNMP customizado

   Exemplo:

   ```
   <include name="Custom_Event_Name" uri="customSNMPdef01.xml"/>
   ```

   Os traps são exibidos no menu na mesma ordem em que são listados no arquivo `snmp-master.xml`.
7. Salve e feche o arquivo.
8. Copie o arquivo do diretório `/opt/qradar/conf` para o diretório `/store/configservices/staging/globalconfig`.
9. Efetue login na interface do QRadar.
10. Na guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.

    Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Enviando traps SNMP para um host específico

Por padrão, em produtos IBM Security QRadar, os traps SNMP são enviados ao host que é identificado em seu arquivo `host.conf`. É possível customizar o arquivo `snmp.xml` para enviar traps SNMP para um host diferente.

Procedimento

1. Use SSH para efetuar login no QRadar como o usuário raiz.
2. Acesse o diretório `/opt/qradar/conf` e faça cópias de backup dos seguintes arquivos:
   - `eventCRE.snmp.xml`
   - `offenseCRE.snmp.xml`

3. Abra o arquivo de configuração para edição.
   - Para editar os parâmetros SNMP para regras de eventos, abra o arquivo `eventCRE.snmp.xml`.
   - Para editar os parâmetros SNMP para regras de ofensa, abra o arquivo `offenseCRE.snmp.xml`.
4. Inclua não mais de um elemento <trapConfig> dentro do elemento <snmp> dentro do elemento <creSNMPTrap> e antes de qualquer outro elemento filho.

```
<trapConfig>
  <!-- Todos os valores de atributos são padrão -->
   <snmpHost snmpVersion="3" port="162" retries="2" timeout="500">HOST
   </snmpHost>
  <!-- Sequência de Comunidades para a Versão 2 -->
   <communityString>COMMUNITY_STRING</communityString>
  <!-- authenticationProtocol (MD5 ou SHA)securityLevel (AUTH_PRIV, AUTH_NOPRIV
  ou NOAUTH_PRIV) -->
   <authentication authenticationProtocol="MD5"securityLevel="AUTH_PRIV">
    AUTH_PASSWORD
   </authentication>
  <!-- decryptionProtocol (DES, AES128, AES192 ou AES256) -->
   <decryption decryptionProtocol="AES256">
     DECRYPTIONPASSWORD
   </decryption>
  <!-- SNMP USER-->
   <user> SNMP_USER </user>
 </trapConfig>
```

5. Use a tabela a seguir para ajudá-lo a atualizar os atributos.

Tabela 88. Os valores de atributos a serem atualizados no elemento <trapConfig>

Elemento	Descrição
`</snmpHost>`	O novo host para o qual você deseja enviar traps SNMP. O valor para o atributo `snmpVersion` para o elemento `<snmpHost>` deve ser 2 ou 3.
`<communityString>`	A sequência de comunidades para o host
`<authentication>`	Um protocolo de autenticação, nível de segurança e senha para o host.
`<decryption>`	O protocolo de decriptografia e senha para o host.
`<user>`	Usuário SNMP

6. Salve e feche o arquivo.
7. Efetue login na interface do QRadar.
8. Na guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.
   Ao implementar a configuração integral, o QRadar reinicia todos os serviços. A coleção de dados para eventos e fluxos para até que a implementação conclua.

Capítulo 21. Ofuscação de dados

Para impedir o acesso não autorizado a informações sensíveis ou identificáveis do usuário, dados ofuscação criptografa os dados do evento fazem distinção entre maiúsculas e minúsculas.

Todas as informações a partir da carga útil do evento, como nome de usuário, número do cartão, ou os campos nome do host podem ser escamoteada. Utilize dados para ajudar a atender os requisitos de ofuscação comissão regulamentar e políticas de privacidade corporativa.

Restrição: Não é possível ofuscar um campo numérico normalizado, como uma porta ou um endereço IP.

Para configurar e gerenciar dados ofuscado, execute as seguintes tarefas:

1. Gere um par de chaves privada/pública RSA.

   O processo de ofuscação requer que você crie uma chave pública e privada para o QRadar SIEM Console.

   os usuários não autorizados que tentam para consultar o banco de dados diretamente não pode visualizar dados sigilosos Ariel sem utilizar a chave de decriptografia pública e privada.

   A chave pública permanece no QRadar Console e você deve armazenar a chave privada em um local seguro. A chave privada contém a chave de decriptografia que é necessário para que os administradores visualizem os dados decriptografada.

   O script `obfuscation_updater.sh` instala a chave pública em seu sistema e configura as instruções de expressão comum (regex). O instruções regex definem os parâmetros que você deseja mascarado.

2. Configure os dados ofuscação.

   Ofuscação de dados criptografa novos eventos, assim que são processados e normalizados pelo, QRadar. O processo de ofuscação avalia a expressão de expressão de ofuscação e verifica que o novo evento bruto, e o evento normalizado, contém dados que são requeridos na para os dados máscara. Os dados que estão definidos nas expressões de ofuscação estão associados aos eventos de dados, criptografados e em seguida escritos no Ariel banco de dados

   O arquivo `obfuscation_expressions.xml` especifica declarações de expressão regular (regex) que identificam os dados que deseja ofuscar. Qualquer texto contendo um evento que marca expressões regulares que são especificadas em `obfuscation_expressions.xml` é criptografado em ambos os campos de cargas úteis do evento

3. Configure os dados ofuscação.

   Quando atividade suspeita ocorre em sua rede, você pode descriptografar os dados, para que você possa investigar todos os dados que está envolvido na atividade.

   O script decriptografa `obfuscation_decoder.sh` o valor criptografado específico que você deseja investigar.

Gerando um Par de Chaves Pública/Privada

A ofuscação e decriptografia de dados requerem um par de chaves privada/pública RSA.

Procedimento

1. Utilizando o SSH, efetue login no QRadar Console como o usuário raiz.
2. Para gerar uma chave privada RSA, digite o seguinte comando:

   `openssl genrsa [-out filename] [numbits]`

   A tabela a seguir descreve as opções de comando.

Tabela 89. Opções de Comando para Gerar a Chave Privada RSA

Opção	Descrição
[-out *filename*]	O nome do arquivo de chave privada RSA
[numbits]	Especifica o tamanho, em bits, da chave privada O tamanho padrão é 512.

Exemplo: O comando a seguir gera uma chave privada denominada `mykey.pem`. O tamanho da chave privada é 512 bits.

```
openssl genrsa -out mykey.pem 512
```

3. Para formatar a chave privada, digite o seguinte comando:

   `openssl pkcs8 [-topk8] [-inform PEM] [-outform PEM] [-in filename] [-out filename] [-nocrypt]`

   A tabela a seguir descreve as opções de comando.

Tabela 90. Opções para Formatar a Chave Privada

Opção	Descrição
[-topk8]	Lê uma chave privada no formato tradicional e grava a chave privada no formato PKCS #8
[-inform]	O formato de entrada da chave privada como Privacy Enhanced Mail (`.PEM`) **Exemplo:** `-inform PEM`
[-outform]	O formato da saída da chave privada como `.PEM` **Exemplo:** `-outform PEM`
[-in *filename*]	O nome do arquivo para a chave privada
[-out*filename*]	O nome do arquivo de saída
[-nocrypt]	Especifica que a chave privada utiliza o formato criptografado `PrivateKeyInfo`.

Exemplo: O comando a seguir grava a chave privada no formato PKCS #8 e utiliza o formato de entrada PEM. A chave privada é enviada no formato PEM, é denominada `mykey.pem`, e utiliza um formato decriptografado.

```
openssl pkcs8 -topk8 -inform PEM -outform PEM -in mykey.pem -out
private_key.pem -nocrypt
```

4. Para gerar a chave pública RSA, digite o seguinte comando:

`openssl rsa [-in filename] [-pubout] [-outform DER] [-out filename]`

A tabela a seguir descreve as opções de comando

Tabela 91. Opções de Comando para Gerar a Chave Pública

Opção	Descrição
[-in *filename*]	Especifica o nome do arquivo de entrada
[-pubout]	Gera uma chave pública
[-outform DER]	O tipo do arquivo de chave pública como arquivo de Certificado X509 Codificado DER (.DER)
[-out *filename*]	O nome do arquivo de chave pública

Exemplo: Neste exemplo, as chaves a seguir são geradas:

- `mykey.pem`
- `private_key.pem`
- `public_key.der`

```
openssl rsa -in mykey.pem -pubout -outform DER -out public_key.der
```

5. Exclua o arquivo `mykey.pem` a partir de seu sistema.
6. Para instalar a chave pública, digite o seguinte comando:

   `obfuscation_updater.sh [-k filename]`

   [-k *filename*] especifica o nome do arquivo para o arquivo de chave pública que você deseja instalar.

   Exemplo: O comando a seguir instala a chave pública denominada `public_key.der`.

   ```
   obfuscation_updater.sh -k public_key.der
   ```

   Restrição: Apenas uma chave pública pode ser instalada para cada sistema. Depois de instalar uma chave pública, a chave não pode ser sobrescrita.

   Depois de instalar a chave pública em seu QRadar Console, o QRadar Console assegura que os hosts gerenciados ofusquem os dados para corresponder aos padrões de expressão de ofuscação.

O que Fazer Depois

Para evitar o acesso não autorizado aos dados ofuscados, remova o arquivo de chave privada de seu sistema. Armazene-o em um local seguro e crie um backup da chave privada. Siga os regulamentos locais para o armazenamento da chave privada.

Configurando ofuscação de dados

Use o script `obfuscation_updater.sh` para configurar dados de ofuscação.

Restrição: Os eventos que estão no diretório `/store` antes de você ativar a ofuscação de dados permanecerão em seu estado atual.

Quaisquer extensões de fonte de log que mudem o formato da carga útil do evento pode causar problemas com os dados.

Não é possível ofuscar um campo numérico normalizado, como uma porta ou um endereço IP.

Procedimento

1. Utilizando o SSH, efetue login no QRadar Console como o usuário raíz:
2. Para configurar a ofuscação de dados, digite o seguinte comando:

   Você pode executar o script a partir de qualquer diretório em `obfuscation_updater.sh` do QRadar Console.

   `obfuscation_updater.sh [-p filename] [-e filename]`

   [`-p` *filename*] especifica o nome do arquivo de chave privada.

   [`-e` *filename*] especifica a oexpressão de fuscação XML de entrada de nome de arquivo.

   Exemplo: O comando a seguir utiliza um arquivo chamado `private_key.pem` como a chave privada e um arquivo denominado `obfuscation_expressions.xml` como o arquivo ofuscação de expressão.

   ```
   obfuscation_updater.sh -p private_key.pem -e obfuscation_expressions.xml
   ```

3. Configure os atributos do arquivo `obfuscation_expressions.xml`.

   O arquivo `obfuscation_expressions.xml` define as expressões comuns que são utilizadas para ofuscar de dados. Você pode incluir várias expressões regulares.

   A tabela a seguir descreve o atributo de arquivo `obfuscation_expressions.xml` que você pode configurar.

Tabela 92. Atributos do arquivo `obfuscation_expressions.xml`

Atributos	Descrição	tabela do banco de dados que contém o valor do atributo
<expression name>	Um nome exclusivo para identificar a expressão regular	
<regex>	A expressão regular que você deseja utilizar para extrair os dados para ofuscação	
<captureGroup>	O grupo de captura que está associado à expressão regular	
<deviceTypeId>	Identifica o tipo de **Efetue de Origem**. Identifica o evento e extrai os dados a serem ofuscados.	[1]**sensordeviceType**
<deviceId>	Identifica o **Efetue de Origem**. Identifica o evento e extrai os dados a serem ofuscados.	[1]**sensordevice**
<qidId>	Identifica o nome dos **Eventos**. Identifica o evento e extrai os dados para ofuscar.	[1]**qidmap**

Tabela 92. Atributos do arquivo `obfuscation_expressions.xml` (continuação)

Atributos	Descrição	tabela do banco de dados que contém o valor do atributo
<category>	Identifica o baixo nível da **Categoria do Evento**. Identifica o evento e extrai os dados a serem ofuscados.	[1]**Tipo**
<enabled>	Se verdadeiro, ativa a expressão regular. Se falso, desativa a expressão regular.	
[1]Você pode configurar um valor de -1 para desativar este atributo.		

Exemplos de ofuscação de dados

1. O código a seguir mostra um exemplo de carga útil do evento.

```
LEEF:1.0|VMware|EMC VMWare|5,1 Terça Oct 09 12:39:31 EDT
2012|jobEnable| usrName=john.smith msg=john.smith@1.1.1.1
src=1.1.1.1
```

2. O código a seguir mostra um exemplo de um arquivo `obfuscation_expressions.xml`.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ObfuscationExpressions>
   <expression name="VMwareUsers">
  <regex>usuário (\S)</regex>
  <deviceTypeId>-1</deviceTypeId>
  <deviceId>-1</deviceId>
  <qidId>-1</qidId>
  <category>-1</category>
  <enabled>verdadeiro</enabled>
 </expression>

 <expression name="VMwarehosts">
  <regex>ruser=(\S)</regex>
  <deviceTypeId>-1</deviceTypeId>
  <deviceId>-1</deviceId>
  <qidId>-1</qidId>
  <category>-1</category>
  <enabled>falso</enabled>
 </expression>
</ObfuscationExpressions>
```

3. O exemplo a seguir mostra as expressões regulares que podem analisar nomes de usuários.

Tabela 93. Exemplo de padrões regex que podem analisar os nomes de usuário.

Exemplo de padrões regex	Correspondentes
`usrName=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*@([0-9 a-zA-Z][-\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,20})$`	john_smith@IBM.com, jon@ibm.com, jon@us.ibm.com
`usrName=(^([\w]+[^\W])([^\W]\.?)([\w]+[^\W]$))`	john.smith, John.Smith, john, jon_smith
`^ usrName= ([a-zA-Z])[a-zA-Z_-]*[\w_-]*[\s]$\|^([um -zA-Z])[0-9_-]*[\s]$|^[a-zA-Z]*[\s]$`	johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith

Tabela 93. Exemplo de padrões regex que podem analisar os nomes de usuário (continuação).

Exemplo de padrões regex	Correspondentes
`usrName=(/S)`	Marca qualquer espaço preenchido depois do sinal de igual =. Esta expressão regular, pode levar a problemas de desempenho do sistema.
`msg=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z]))*@\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b`	Corresponde usuários com endereço IP. **Exemplo:** `john.smith@1.1.1.1`
`src=\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b`	Corresponde os formatos de endereço IP.
`host=^(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\-]*[um-zA-Z0-9])\.)*([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0-9\-]*[A-Za-z0-9])$`	`hostname.ibm.com, hostname.co.uk,`

Decriptografando Dados Ofuscados

Quando a ofuscação de dados está configurada em um sistema IBM Security QRadar SIEM, a versão criptografada dos dados é exibida nas colunas e parâmetros na interface com o usuário. Utilize o script `obfuscation_decoder.sh` para decriptografar dados ofuscados.

Procedimento

1. Efetue login na interface com o usuário do IBM Security QRadar SIEM e copie o texto ofuscado que você deseja decriptografar
2. Utilizando o SSH, efetue login no QRadar Console como o usuário raiz.

   Nome de usuário: `raiz`
3. Crie um diretório e copie as chaves pública e privada nesse diretório.
4. Vá para o diretório no qual as chaves estão localizadas.
5. Para decriptografar o texto ofuscado, digite o seguinte comando:

   `obfuscation_decoder.sh -k publickey` *`filename`* `-p privatekey` *`filename`* `-d` *`<obfuscated_text>`*

   A tabela a seguir descreve as opções de `obfuscation_decoder.sh`.

Tabela 94. Opções para o Script `obfuscation_decoder.sh`

Opção	Descrição
`-k publickey` *filename*	O nome do arquivo de chave pública
`-p privatekey` *filename*	O nome do arquivo de chave privada
`-d obfuscated` *text*	O texto ofuscado que você deseja decriptografar

Exemplo: O comando a seguir decriptografa os dados mascarados.

```
obfuscation_decoder.sh -k public_key.der -p private_key.pem -d
obfuscated_text
```

Dados do Perfil do Ativo QRadar não Exibem Dados Ofuscados Após o Upgrade

Os nomes de usuário e os dados de nome do host que fazem parte do perfil de ativo do IBM Security QRadar antes do upgrade para o QRadar V7.2 podem não exibir dados ofuscados conforme o esperado.

Procedimento

Para ofuscar dados do perfil de ativos, siga estas etapas:

1. Efetue login no QRadar Console.
2. Clique na guia **Ativos**.
3. Para remover hosts e nomes de usuários não ofuscados, clique em **Ações** > **Excluir listados**.
4. Execute o perfil de varredura manualmente ou planeje o perfil de varredura para execução.
5. Para preencher novamente os dados para blocos de construção em seu sistema QRadar, execute a ferramenta **Descoberta do Servidor**.

Capítulo 22. Log de auditoria

Mudanças que são feitas por usuários QRadar são gravadas em logs de auditoria.

É possível visualizar logs de auditoria para monitorar mudanças noQRadar e em usuários que modificaram as configurações.

Todos os logs de auditoria são armazenados em texto simples, e são arquivados e comprimidos quando o arquivo de log de auditoria atinge 200 MB. O arquivo de log atual é nomeamdo `audit.log`. Quando o arquivo atinge 200MB, 200 MB, o arquivo é comprimido e e nomeado para `audit.1.gz, audit.2.gz`. O número do arquivo é incrementado cada vez que um log de arquivo é arquivado. QRadar armazena mais de 50 logs de arquivos arquivados.

Visualizando o Arquivo de Log de Auditoria

Utilize shell seguro (SSH) para efetuar login no sistema QRadar e monitore as mudanças em seu sistema.

Sobre Esta Tarefa

É possível utilizar a guia **Atividade do Log** para visualizar os eventos de log de auditoria normalizados.

O tamanho máximo de qualquer mensagem de auditoria, exceto data, hora e nome do host, é de 1024 caracteres.

Cada entrada no arquivo de log exibe o formato a seguir:

<date_time> <host name> <user>@<IP address> (thread ID) [<category>] [<sub-category>] [<action>] <payload>

A tabela a seguir descreve as opções de formato de arquivo de log.

Tabela 95. Descrição das Partes do Formato de Arquivo de Log

Parte do Formato de Arquivo	Descrição
date_time	A data e hora da atividade no formato: Mês Data HH:MM:SS
host name	O nome do host do Console em que essa atividade foi registrada.
user	O nome do usuário que alterou as configurações.
IP address	O endereço IP do usuário que alterou as configurações.
thread ID)	O identificador do encadeamento do Java que registrou essa atividade.
category	A categoria de alto nível desta atividade.
sub-categor	A categoria de baixo nível desta atividade.
action	A atividade que ocorreu.

Tabela 95. Descrição das Partes do Formato de Arquivo de Log (continuação)

Parte do Formato de Arquivo	Descrição
payload	O registro completo, que pode incluir o registro do usuário ou a regra de evento que foi alterada.

Procedimento

1. Utilizando o SSH, efetue login no QRadar como o usuário raiz:
2. **Nome de Usuário:** `root`
3. **Senha:** *`password`*
4. Vá para o seguinte diretório:
   `/var/log/audit`
5. Abra e visualize o arquivo de log de auditoria.

Ações registradas

Entenda o conteúdo do arquivo de log de auditoria int QRadar no diretório `/var/log/audit`. O arquivo de log de auditoria contém ações registradas.

A lista a seguir descreve as categorias de ações que estão no arquivo de log de auditoria :

Autenticação do administrador

- Efetuar login no Console Administrativo
- Efetar logout do Console de Administração.

Recursos

- Excluir um recurso.
- Excluir todos os recursos.

Acesso ao log de auditoria

Uma procura que inclui eventos que possuem uma categoria de evento de alto nível de auditoria.

Backup e recuperação

- Editar a configuração.
- Iniciar o backup.
- Concluir o backup.
- Cometer falha do backup.
- Limpar o backup.
- Sincronizar o backup.
- Cancelar o backup.
- Iniciar a restauração.
- Fazer upload de um backup.
- Fazer upload de um backup inválido.
- Iniciar a restauração.
- Limpar o backup.

Propriedades customizadas

- Incluir uma propriedade de evento customizado.
- Editar uma propriedade de evento customizado.

- Excluir uma propriedade de evento customizado.
- Editar uma propriedade de fluxo customizado.
- Excluir uma propriedade de fluxo customizado.

Configuração de gráfico
Salvar configuração de grafico de evento ou fluxo.

Expressões de propriedade customizada
- Incluir uma expressão de propriedade de evento customizado.
- Editar uma expressão de propriedade de evento customizado.
- Excluir uma expressão de propriedade de evento customizado.
- Incluir uma expressão de propriedade do fluxo customizado.
- Editar uma expressão de propriedade do fluxo customizado.
- Excluir uma expressão de propriedade do fluxo customizado.

Depósitos de retenção
- Incluir um depósito.
- Excluir um depósito.
- Editar um depósito.
- Ativar ou desativar um depósito.

Fontes de fluxo
- Incluir uma fonte de fluxo.
- Editar uma fonte de fluxo.
- Excluir uma fonte de fluxo.

Grupos
- Incluir um grupo.
- Excluir um grupo.
- Editar um grupo.

Alta disponibilidade
- Incluir uma chave de licença.
- Reverter uma licença.
- Excluir uma chave de licença.

Extensão de fonte de log
- Incluir uma extensão de fonte de log
- Editar a extensão de fonte de log.
- Excluir uma extensão de fonte de log.
- Fazer upload de uma extensão de fonte de log.
- Fazer upload de uma extensão de fonte de log com êxito.
- Fazer upload de uma extensão de fonte de log inválida.
- Fazer download de uma extensão de fonte de log.
- Relatar uma extensão de fonte de log.
- Modificar uma associação de fontes de log a um tipo de dispositivo ou dispositivo.

Ofensas
- Ocultar uma ofensa.
- Fechar uma ofensa
- Fechar todas as ofensas.

- Incluir uma nota de destino.
- Incluir uma nota de origem.
- Incluir uma nota de rede.
- Incluir uma nota de ofensa.
- Incluir um motivo para fechamento de ofensas.
- Editar um motivo para fechamento de ofensas.

Configuração de protocolo

- Incluir uma configuração de protocolo.
- Excluir uma configuração de protocolo.
- Editar uma configuração de protocolo.

QIDmap

- Incluir uma entrada de mapa QID.
- Editar uma entrada de mapa QID.

QRadar Vulnerability Manager

- Criar um planejamento de scanner.
- Atualizar um planejamento de scanner.
- Excluir um planejamento de scanner.
- Iniciar um planejamento de scanner.
- Pausar um planejamento de scanner.
- Continuar um planejamento de scanner.

Conjuntos de referência

- Criar um conjunto de referência.
- Editar um conjunto de referência.
- Limpar elementos em um conjunto de referência.
- Excluir um conjunto de referência.
- Incluir elementos do conjunto de referência.
- Excluir elementos do conjunto de referência.
- Excluir todos os elementos do conjunto de referência.
- Importar elementos do conjunto de referência.
- Exportar elementos do conjunto de referência.

Relatórios

- Incluir um modelo.
- Excluir um modelo.
- Editar um modelo.
- Gerar um relatório.
- Excluir um relatório.
- Excluir conteúdo gerado.
- Visualizar um relatório gerado.
- Enviar e-mail de um relatório gerado.

Login de root

- Efetuar login no QRadar como root.
- Efetuar logout do QRadar como root.

Regras

- Incluri uma regra.
- Excluir uma regra.
- Editar uma regra.

Scanner

- Incluir um scanner.
- Excluir um scanner.
- Editar um scanner.

Planejamento de scanner

- Incluir um planejamento.
- Editar um planejamento.
- Excluir um planejamento.

Autenticação de sessão

- Criar uma sessão de administração.
- Finalizar uma sessão de administração.
- Negar uma sessão de autenticação inválida.
- Expirar uma autenticação de sessão.
- Criar uma sessão de autenticação.
- Encerrar uma sessão de autenticação

SIM Limpar um modelo SIM.

Armazenamento e encaminhamento

- Incluir um planejamento de Armazenamento e Encaminhamento.
- Editar um planejamento de Armazenamento e Encaminhamento.
- Excluir um planejamento de Armazenamento e Encaminhamento.

Encaminhamento do Syslog

- Incluir um encaminhamento de syslog.
- Excluir um encaminhamento de syslog.
- Editar um encaminhamento de syslog.

Gerenciamento de sistema

- Encerre um sistema.
- Reinicie um sistema.

Contas de usuários

- Incluir uma conta.
- Editar uma conta.
- Excluir uma conta.

Autenticação do usuário

- Efetuar login na interface com o usuário.
- Efetuar logout da interface com o usuário.

Autenticação do usuário do Ariel

- Negar uma tentativa de login.
- Incluir uma propriedade do Ariel.
- Excluir uma propriedade do Ariel.
- Editar uma propriedade do Ariel.
- Incluir uma extensão de propriedade do Ariel.

- Excluir uma extensão de propriedade do Ariel.
- Editar uma extensão de propriedade do Ariel.

Funções de usuário

- Incluir uma função.
- Editar uma função.
- Excluir uma função.

VIS

- Descobrir um novo host.
- Descobrir um novo sistema operacional.
- Descobrir uma nova porta.
- Descobrir uma nova vulnerabilidade.

Capítulo 23. Categorias de Evento

Categorias de eventos são usadas para agrupar eventos de recebimento para processamento pelo IBM Security QRadar. As categorias de eventos são pesquisáveis e ajudam a monitorar sua rede.

Eventos que ocorrem em sua rede são agregados em categorias de alto nível e de baixo nível. Cada categoria de alto nível contém categorias de baixo nível e um nível de severidade associado. É possível rever os níveis de severidade que são designados para eventos e ajustá-los às suas necessidades de política corporativa.

Categorias de eventos de alto nível

Eventos em QRadar origens de log são agrupados em categorias de alto nível. Cada evento é atribuído a uma categoria de alto nível específico.

Categorizando os eventos de entrada assegura que você pode procurar facilmente os dados.

A tabela a seguir descreve as opções de comando.

Tabela 96. Categorias de eventos de alto nível

Categoria	Descrição
"Recon" na página 266	Eventos que são relacionados à varredura e outras técnicas que são utilizados para identificar os recursos de rede, por exemplo, rede ou host varreduras de porta.
"DoS" na página 268	Eventos que são relacionados ao serviço (DoS) ou ataques de negação distribuído (DDoS) em relação a serviços ou hosts, por exemplo, força bruta rede contra ataques DoS.
"Autenticação" na página 271	Eventos que são relacionadas a controles de autenticação, grupo ou alterar privilégio, por exemplo, efetuar login ou logout.
"Acesso" na página 277	Eventos resultante de uma tentativa para acessar os recursos de rede, por exemplo, aceitar ou negar firewall.
"Explorar" na página 279	Events that are related to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.
"Malware" na página 281	Eventos que são relacionados ao vírus, Tróia, atentados a porta traseira, ou outras formas de software hostil. Eventos malware pode incluir um vírus, Tróia, software mal-intencionado, ou spyware.

Tabela 96. Categorias de eventos de alto nível (continuação)

Categoria	Descrição
"Atividade Suspeita" na página 282	A natureza da ameaça é desconhecida, mas o comportamento é suspeito. A ameaça potencialmente anomalias protocolo pode indicar evasivo técnicas que incluem, por exemplo, pacote ou técnicas de fragmentação sonegação sistema de detecção de intrusão conhecido (IDS).
"Sistema" na página 286	Os eventos que são relacionados a alterações do sistema, instalação de software, ou mensagens de status.
"Política" na página 290	Eventos corporativo ou uso indevido sobre violações de política.
"Desconhecido" na página 291	Os eventos que estão relacionados com a actividade desconhecido em seu sistema.
"CRE" na página 292	Os eventos que são gerados a partir de um ou ofensa evento de regra.
"Exploração Potencial" na página 293	Eventos relacionados ao aplicativo explora potencial e as tentativas de estouro de buffer.
"Usuário definido" na página 294	Eventos que são relacionados aos objetos definido pelo usuário.
"SIM de auditoria" na página 297	Eventos que são relacionadas à interação do usuário com o Console e as funções administrativas.
"Descoberta do Host VIS" na página 297	Eventos que são relacionados ao host, portas, ou as vulnerabilidades que o componente VIS descobre.
"Aplicação" na página 298	Os eventos que estão relacionados com a actividade de auditoria.
"Auditoria" na página 319	Os eventos que estão relacionados com a actividade de auditoria.
"Risco" na página 320	Eventos que são relacionados com a actividade risco em IBM Security QRadar Risk Manager.
"Gerenciador de risco de auditoria" na página 321	Eventos que são relacionados com a actividade de auditoria em IBM Security QRadar Risk Manager.
"Controle" na página 322	Eventos que são relacionados ao seu hardware do sistema.
"Gerenciadores de perfis ativos" na página 324	Eventos que são relacionados aos perfis de ativos.

Recon

A categoria Recon contém eventos que estão relacionados à varredura e outras técnicas que são utilizados para identificar os recursos de rede.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados a categoria recon.

Tabela 97. categorias de baixo nível e níveis de gravidade para a categoria de eventos Recon

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Forma Desconhecida de Recon	Uma forma de reconhecimento desconhecido.	2
Consulta do Aplicativo	Reconhecimento de aplicativos em seu sistema.	3
Consulta de Host	Reconhecimento para um host em sua rede.	3
Tempo de Acesso da Rede	Reconhecimento em sua rede.	4
Reconhecimento de Correio	Reconhecimento em seu sistema de correio.	3
Windows Reconhecimento	Reconhecimento para o sistema operacional Windows.	3
Portmap / RPC r\Request	Reconhecimento em sua solicitação de RPC ou portmap.	3
Varredura de Porta do Host	Indica que uma varredura ocorreu nas portas do host.	4
Dump do RPC	Indica que as informações RPC (Remote Procedure Call) é removido.	3
Reconhecimento do DNS	Reconhecimento nos servidores DNS.	3
Reconhecimento de Eventos Diversoa	Diversos eventos de reconhecimento.	2
Reconhecimento da Web	reconhecimento da Web em sua rede.	3
Reconhecimento do Banco de Dados	reconhecimento do Banco de Dados em sua rede.	3
Reconhecimento do ICMP	Reconhecimento no tráfego ICMP.	3
Reconhecimento do UDP	Reconhecimento no tráfego UDP.	3
Reconhecimento do SNMP	Reconhecimento sobre o tráfego SNMP.	3
Consulta do Host ICMP	Indica uma consulta do host ICMP.	3
Consulta do Host UDP	Indica uma consulta do host UDP.	3
Reconhecimento do NMAP	Indica de reconhecimento do NMAP.	3
Reconhecimento do TCP	Indica de reconhecimento TCP em sua rede.	3
Reconhecimento do UNIX	Reconhecimento em sua rede UNIX.	3

Tabela 97. categorias de baixo nível e níveis de gravidade para a categoria de eventos Recon (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Reconhecimento do FTP	Indica de reconhecimento de FTP.	3

DoS

A categoria contém eventos que estão relacionados aos ataques DoS de serviço (DoS) em relação a serviços ou hosts.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de gravidade associado para a categoria DoS.

Tabela 98. categorias de baixo nível e níveis de severidade para a categoria DoS eventos

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ataque DoS Desconhecido	Indica um ataque DoS desconhecido.	8
DoS do ICMP	Indica um ataque de ICMP DoS.	9
DoS do TCP	Indica um ataque DoS banco de dados.	9
DoS do UDP	Indica um ataque DoS do UDP.	9
DoS do Serviço DNS	Indica um ataque DoS do serviço DNS.	8
DoS do Serviço da Web	Indica um ataque DoS do serviço da Web.	8
DoS do Serviço de Correio	Indica um ataque DoS do servidor de correio.	8
DoS Distribuído	Indica um ataque DoS distribuído.	9
DoS Diverso	Indica um ataque diversos DoS.	8
UNIX DoS	Indica um ataque UNIX DoS.	8
Windows DoS	Indica um ataque Windows DoS.	8
DoS do Banco de Dados	Indica um ataque DoS banco de dados.	8
DoS do FTP	Indica um ataque DoS do FTP.	8
DoS de Infraestrutura	Indica um ataque DoS na infra-estrutura.	8
DoS do Telnet	Indica um ataque DoS do Telnet.	8
Força bruta Login	Indica acesso ao seu sistema por meio de métodos não autorizados.	8

Tabela 98. categorias de baixo nível e níveis de severidade para a categoria DoS eventos (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Taxa Alta TCP DoS	Indica uma alta taxa de TCP DoS do ataque.	8
Taxa Alta de DoS do UDP	Indica uma alta taxa de DoS do UDP ataque.	8
Taxa Alta DoS do ICMP	Indica uma alta taxa de ataque distribuído DoS do ICMP.	8
Taxa Alta DoS	Indica um ataque DoS taxa alta.	8
DoS do TCP Taxa média	Indica um ataque TCP taxa média.	8
DoS do UDP Taxa média	Indica um ataque UDP taxa média.	8
Taxa de DoS do ICMP Médio	Indica um ataque de ICMP taxa média.	8
DoS Taxa Média	Indica um ataque DoS taxa média distribuído.	8
DoS Taxa Média	Indica um ataque DoS taxa média distribuído.	8
Baixa Taxa de DoS do TCP	Indica uma baixa taxa TCP DoS ataque.	8
Baixa Taxa de DoS do UDP	Indica uma baixa taxa UDP DoS ataque.	8
Baixa Taxa de DoS do ICMP	Indica uma baixa taxa de ataque DoS do ICMP.	8
Baixa Taxa de DoS	Indica um ataque DoS taxa baixa.	8
Taxa Alta Distribuída DoS TCP	Indica uma taxa alta DoS do TCP ataque distribuído.	8
Distributed High Rate UDP DoS	Indica uma alta taxa de DoS do UDP ataque distribuído.	8
Distributed High Rate ICMP DoS	Indica uma alta taxa de ataque distribuído DoS do ICMP.	8
Taxa Alta DoS Distribuído	Indica um ataque distribuído de alta taxa de DoS.	8
Taxa DoS Distribuído Medium TCP	Indica uma taxa média TCP DoS do ataque distribuído.	8
Taxa DoS Distribuído Medium UDP	Indica uma taxa média UDP DoS ataque distribuído.	8
Taxa Média ICMP DoS Distribuído	Indica uma taxa baixa DoS do ICMP ataque distribuído.	8
Taxa Média DoS Distribuído	Indica um ataque DoS taxa média distribuído.	8

Tabela 98. categorias de baixo nível e níveis de severidade para a categoria DoS eventos (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Baixa Taxa TCP DoS Distribuído	Indica uma baixa taxa de DoS do TCP ataque distribuído.	8
Baixa Taxa UDP DoS Distribuído	Indica uma baixa taxa de DoS do UDP ataque distribuído.	8
Baixa Taxa ICMP DoS Distribuído	Indica uma baixa taxa de ataque ICMP DoS distribuída.	8
Baixa Taxa de DoS Distribuído	Indica uma baixa taxa de DoS distribuída.	8
Taxa Alta de varredura TCP	Indica uma taxa alta de varredura TCP.	8
Taxa Média Varredura UDP	Indica uma varredura de UDP taxa alta.	8
Taxa Alta de varredura ICMP	Indica uma taxa alta de varredura ICMP.	8
Taxa Alta Varredura	Indica uma taxa alta de varredura.	8
Taxa média de varredura TCP	Indica que uma varredura de TCP taxa média.	8
Taxa Média Varredura UDP	Indica uma varredura de UDP taxa média.	8
Taxa média de varredura ICMP	Indica que uma varredura de ICMP taxa média.	8
Taxa média de Varredura	Indica que uma varredura de taxa média.	8
Low Rate TCP Scan	Indica que uma varredura de TCP taxa baixa.	8
Baixa Taxa de UDP de Varredura	Indica uma varredura de UDP taxa baixa.	8
Baixa Taxa de ICMP de Varredura	Indica que uma varredura de ICMP taxa baixa.	8
Baixa Taxa de Varredura	Indica uma baixa taxa de varredura.	8
DoS VoIP	Indica um ataque VoIP DoS.	8
Estouro	Indica um ataque inundação.	8
TCP Inundação	Indica um ataque TCP Inundação.	8
UDP Flood	Indica um ataque flood UDP.	8
ICMP Flood	Indica um ataque ICMP flood.	8
SYN Flood	Indica um ataque SYN flood.	8
URG Flood	Indica um ataque flood com a urgência (URG) sinalizada.	8

Tabela 98. categorias de baixo nível e níveis de severidade para a categoria DoS eventos (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
SYN Flood URG	Indica um ataque flood com urgência (URG) sinalizada.	8
SYN Flood FIN	Indica um ataque flood SYN FIN.	8
SYN Flood ACK	Indica um ataque flood SYN ACK.	8

Autenticação

A acrtegoria autenticação contêm eventos que estão relacionados a autenticação, sessões e controles de acesso que monitora usuários na rede.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de autenticação.

Tabela 99. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Autenticação Desconhecida	Indica de autenticação desconhecida.	1
Login do Host Bem-sucedido	Indica um login do host bem-sucedido.	1
Login do Host com Falha	Indica que o login do host falhou.	3
Login Diverso Bem-sucedido	Indica que a sequência de login foi bem-sucedida.	1
Login Diverso com Falha	Indica que a sequência de login falhou.	3
Escalação de Privilégio com Falha	Indica que a escalação privilegiada falhou.	3
Escalação de Privilégio Bem-sucedida	Indica que a escalação de privilégio ocorreu com êxito.	1
Login de Serviço de Correio Bem-sucedido	Indica que o serviço de correio de login foi bem-sucedida.	1
Login de Serviço de Correio com Falha	Indica que o login de serviço de correio falhou.	3
Login de Servidor de Autenticação com Falha	Indica que o login do servidor de autenticação falhou.	3
Login de Servidor de Autenticação Bem-sucedido	Indica que o servidor de autenticação de login obteve êxito.	1
Login de Serviço da Web Bem-sucedido	Indica que o serviço da Web de login obteve êxito.	1

Tabela 99. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Login de Serviço da Web com Falha	Indica que o login de serviço da web falhou.	3
Login de Administrador Bem-sucedido	Indica que um login administrativo foi bem-sucedido.	1
Login de Administrador com Falha	Indica que o login do SSH falhou.	3
Nome de Usuário Suspeito	Indica que um usuário tentou acessar a rede utilizando um nome de usuário incorreto.	4
Login com padrões de nome/ senha bem-sucedidos	Indica que um usuário acessou a rede utilizando o nome de usuário e senha padrão.	4
Login com padrões de nome de usuário/ senha falhou	Indica que um usuário foi mal-sucedido ao acessar a rede utilizando o nome de usuário e senha padrão.	4
Login de FTP Bem-sucedido	Indica que o login de FTP foi bem-sucedido.	1
Login de FTP com Falha	Indica que o login de FTP falhou.	3
Login de SSH Bem-sucedido	Indica que o login do SSH foi bem-sucedido.	1
Falha de Login de SSH	Indica que o login do SSH falhou.	2
Direito de Usuário Designado	Indica que o acesso do usuário a recursos de rede foi concedido com êxito.	1
Direito de Usuário Removido	Indica que o acesso do usuário a recursos de rede foi removido com êxito.	1
Domínio Confiável Incluído	Indica que um domínio confiável foi adicionado com êxito à sua implementação.	1
Domínio Confiável Removido	Indica que um domínio confiável foi removida de sua implementação.	1
Acesso de Segurança do Sistema Concedido	Indica que o acesso de segurança do sistema foi concedido com êxito.	1
Acesso de Segurança do Sistema Removido	Indica que o acesso de segurança do sistema foi removido com êxito.	1
Política Incluída	Indica que uma política foi incluída com êxito.	1

Tabela 99. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Mudança de Política	Indica que uma política foi alterada com êxito.	1
Conta do Usuário Incluída	Indica que uma conta de usuário foi incluída com êxito.	1
Conta do Usuário Alterada	Indica uma alteração em uma conta de usuário existente.	1
Mudança de Senha com Falha	Indica que uma tentativa de alterar uma senha existente falhou.	3
Mudança de Senha Bem-sucedida	Indica que uma mudança de senha foi bem-sucedida.	1
Conta do Usuário Removida	Indica que uma conta do usuário foi removida com êxito.	1
Membro do Grupo Incluído	Indica que um membro do grupo foi incluído com êxito.	1
Membro do Grupo Removido	Indica que um membro do grupo foi removido.	1
Grupo Incluído	Indica que um grupo foi incluído com êxito.	1
Grupo Alterado	Indica uma alteração em um grupo existente.	1
Grupo Removido	Indica que um grupo foi removido.	1
Conta do Computador Incluída	Indica que uma conta do computador foi incluída com êxito.	1
Conta do Computador Alterada	Indica uma alteração em uma conta do computador existente.	1
Conta do Computador Removida	Indica que uma conta do computador foi removida com êxito.	1
Login de Acesso Remoto Bem-sucedido	Indica que o acesso a rede usando um login remoto foi concluído com sucesso.	1
Login de Acesso Remoto com Falha	Indica que uma tentativa de acessar a rede usando um login remoto falhou.	3
Autenticação Geral Bem-sucedida	Indica que o processo de autenticação foi bem-sucedida.	1
Autenticação Geral com Falha	Indica que o processo de autenticação falhou.	3

Tabela 99. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Login do Telnet Bem-sucedido	Indica que o login de telnet foi bem-sucedida.	1
Login do Telnet com Falha	Indica que o login de Telnet falhou.	3
Senha Suspeita	Indica que um usuário tentou efetuar login utilizando uma senha suspeita.	4
Login de Administrador Bem-sucedido	Indica que um usuário efetuou login com êxito no utilizando o Samba.	1
Login do Samba com falha	Indica um usuário falhou ao efetuar login utilizando Samba.	3
Sessão do Servidor de Autenticação Aberta	Indica que uma sessão de comunicação com o servidor de autenticação foi iniciado.	1
Sessão do Servidor de Autenticação Encerrada	Indica que uma sessão de comunicação com o servidor de autenticação foi fechada.	1
Sessão de Firewall Encerrada	Indica que uma sessão de firewall foi fechada.	1
Logout do Host	Indica que um host efetuou logout com êxito.	1
Logout Diverso	Indica que um usuário efetuou logout com êxito.	1
Logout do Servidor de Autenticação	Indica que o processo para efetuar logout do servidor de autenticação foi bem-sucedido.	1
Logout do Serviço da Web	oIndica que o processo para efetuar logout do serviço da Web foi bem-sucedido.	1
Logout Admin	Indica que o usuário administrativo efetuou logout com êxito.	1
Logout do FTP	Indica que o processo para efetuar logout do serviço de FTP foi bem-sucedido.	1
Logout do SSH	Indica que o processo para efetuar logout da sessão SSH foi bem-sucedido.	1
Logout de Acesso Remoto	Indica que o processo para efetuar logout do servidor de autenticação foi bem-sucedido.	1

Tabela 99. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Logout do Telnet	Indica que o processo para efetuar logout da sessão Telnet foi bem-sucedido.	1
Logout do Samba	Indica que o processo para efetuar logout do Samba foi bem-sucedido.	1
Início da Sessão SSH	Indica que a sessão de login do SSH foi iniciado em um host.	1
Conclusão de Sessão de Administrador	Indica o término de uma sessão de login do SSH em um host.	1
Sessão Admin Iniciada	Indica que uma sessão de login foi iniciada em um host, por um usuário administrativo, ou com privilégios de administrador.	1
Conclusão de Sessão de Administrador	Indica o término de uma sessão de administrador ou de usuários privilegiados em um host.	1
Login VoIP bem-sucedido	Indica um serviço de login de VoIP bem-sucedido	1
Falha de Login de VoIP	Indica uma tentativa mal-sucedida de acessar o serviço VoIP.	1
Logout de VoIP	Indica um logout do usuário,	1
Início de sessão de VoIP	Indica o início de uma sessão de VoIP.	1
Sessão VoIP finalizada	Indica o fim de uma sessão de VoIP.	1
Login Bem-sucedido banco de dados	Indica um login do banco de dados bem-sucedido.	1
Falha de Login do Banco	Indica que uma tentativa de login do banco de dados falhou.	3
Falha de Autenticação IKE	Indica que uma falha de autenticação Internet Key Exchange (IKE) foi detectada.	3
Aautenticação IKE Bem-sucedida	Indica que uma autenticação de IKE bem sucedida foi detectado.	1
Sessão Iniciada IKE	Indica que uma sessão do IKE foi iniciada.	1
Sessão IKE finalizada	Indica que uma sessão do IKE foi finalizada.	1
Erro de IKE	Indica uma mensagem de erro de IKE.	1

Tabela 99. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Status do IKE	Indica mensagem de status IKE.	1
Sessão Iniciada RADIUS	Indica que uma sessão RADIUS foi iniciada.	1
Sessão RADIUS finalizada	Indica uma sessão RADIUS foi finalizada.	1
Sessão RADIUS Negado	Indica que uma sessão RADIUS foi negada.	1
Status da Sessão RADIUS	Indica uma mensagem de status da sessão RADIUS.	1
Falha na Autenticação do RADIUS	Indica uma falha de autenticação RADIUS.	3
Autenticação RADIUS bem-sucedida	Indica uma autenticação RADIUS foi bem-sucedido.	1
Sessão TACACS iniciada	Indica uma sessão TACACS foi iniciada.	1
Sessão TACACS finalizada	Indica uma sessão TACACS foi finalizada.	1
Sessão TACACS negada	Indica que uma sessão TACACS foi negada.	1
Status da Sessão do TACACS	Indica uma mensagem de status da sessão TACACS.	1
Autenticação do TACACS bem-sucedida	Indica uma autenticação TACACS foi bem-sucedida.	1
Falha de autenticação do TACACS	Indica uma falha de autenticação TACACS.	1
Re-autenticação de host bem-sucedida	Indica que a re-autenticação de um host foi bem-sucedida.	1
Re-autenticação do Host com falha	Indica que a re-autenticação de um host falhou.	3
Estação de autenticação Bem-sucedido	Indica que o reassociação estação foi bem-sucedida.	1
Falha de autenticação da Estação	Indica que a estação de um host falhou.	3
Estação de associação de Bem-sucedido	Indica que a associação estação foi bem-sucedida.	1
Falha estação de associação	Indica que a associação estação falhou.	3
Estação de Autenticação Bem-sucedido	Indica que o reassociação de estação foi bem-sucedida.	1
Estação de Re-associação com falha	Indica que a associação estação falhou.	3
Desassociando do Host Bem-sucedido	Indica que o desassociando um host foi bem-sucedida.	1

Tabela 99. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Falha ao dessasociar o host	Indica que a desassociação de um host falhou	3
Erro SA	Indica mensagem de erro uma Associação de Segurança (SA).	5
Falha de Criação de SA	Indica falha na criação de uma Associação de Segurança (SA).	3
Estabelecida SA	Indica que a conexão uma Associação de Segurança (SA) estabelecido.	1
SA Rejeitado	Indica mensagem de erro uma Associação de Segurança (SA).	3
Deletando SA	Indica a exclusão de uma Associação de Segurança (SA).	1
A SA	Indica a criação de uma Associação de Segurança (SA).	1
Incompatibilidade de Certificado	Indica uma incompatibilidade de certificados.	3
Incompatibilidade de Credenciais	Indica uma incompatibilidade credenciais.	3
Tentativa de Login de Administrador	Indica uma tentativa de login admin.	2
Tentativa de Login do Usuário	Indica que uma tentativa de login do usuário.	2
Usuário de Login Bem-sucedido	Indica um login de usuário bem-sucedido.	1
Falha de Login do Usuário	Indica um login de usuário falhou.	3
Login SFTP Bem-sucedido	Indica uma com êxito o SSH File Transfer Protocol (SFTP) de login.	1
Falha de Login SFTP	Indica uma falha o SSH File Transfer Protocol (SFTP) de login.	3
Logout SFTP	Indica um logout o SSH File Transfer Protocol (SFTP).	1

Acesso

A categoria de acesso contém autenticação e controles de acesso que são utilizados para monitorar eventos de rede.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de acesso.

Tabela 100. Categorias de baixo nível e níveis de severidade para a categoria de eventos de acesso

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento de comunicação de rede desconhecida	Indica um evento de comunicação de rede desconhecida.	3
Permissão de firewall	Indica que o acesso ao firewall foi permitido.	0
Negação de firewall	Indica que o acesso ao firewall foi negado.	4
Resposta do contexto do fluxo	Indica eventos do mecanismo de classificação em resposta a uma solicitação SIM.	5
Evento de comunicação de rede diversa	Indica um evento de comunicações diversas.	3
Negação de IPS	Indica que o sistema de prevenção de instrusão (IPS) negou o tráfego.	4
Sessão de firewall aberta	Indica que a sessão firewall foi aberta.	0
Sessão de Firewall Encerrada	Indica que a sessão de firewall foi encerrada.	0
Conversão de endereço dinâmico bem-sucedida	Indica que a conversão de endereço dinâmico foi bem-sucedida.	0
Grupo de conversão não localizado	Indica que nenhum grupo de conversão foi localizado.	2
Autorização diversa	Indica que o acesso foi concedido a uma autenticação de diversos servidores.	2
Permissão de ACL	Indica que uma lista de controle de acesso (ACL) permitiu o acesso.	0
Negação de ACL	Indica que uma lista de controle de acesso negou o acesso.	4
Acesso permitido	Indica que o acesso foi permitido.	0
Acesso negado	Indica que o acesso foi negado.	4
Sessão aberta	Indica que uma sessão foi aberta.	1
Sessão fechada.	Indica que uma sessão foi fechada.	1
Sessão reconfigurada	Indica que uma sessão foi reconfigurada.	3

Tabela 100. Categorias de baixo nível e níveis de severidade para a categoria de eventos de acesso (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Seção encerrada	Indica que uma sessão foi permitida.	4
Sessão negada	Indica que uma sessão foi negada.	5
Sessão em andamento	Indica que uma sessão está em andamento.	1
Sessão atrasada	Indica que uma sessão está em atraso.	3
Sessão em fila	Indica que uma sessão estava em fila.	1
Entrada da sessão	Indica que uma sessão é de entrada.	1
Sessão de saída	Indica que uma sessão é de saída.	1
Tentativa de acesso não autorizado	Indica que uma tentativa de acesso não autorizado foi detectada.	6
Ação de aplicação diversa permitida	Indica que uma ação do aplicativo foi permitida.	1
Ação de aplicação diversa negada.	Indica que uma ação do aplicativo foi negada.	3
Ação do banco de dados permitida.	Indica que uma ação do banco de dados foi permitida.	1
Ação do banco de dados negada.	Indica que uma ação do banco de dados foi negada.	3
Ação de FTP permitida	Indica que uma ação de FTP foi permitida.	1
Ação de FTP negada	Indica que uma ação de FTP foi negeda.	3
Objeto em cache	Indica que um objeto foi armazenado em cache.	1
Objeto não armazenado em cache	Indica que um objeto não foi armazenado em cache.	1
Limite de taxa	Indica que o trafego de rede está em sua taxa limite.	4
Sem limite de taxa	Indica que a rede está sem taxa de tráfego limite.	0

Explorar

A categoria explorar contém eventos onde uma comunicação ou um acesso explorar ocorreu.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associado para explorar categoria.

Tabela 101. categorias de baixo nível e níveis de severidade para o explorar categoria de eventos

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ataque de Exploração Desconhecido	Indica um ataque exploit desconhecido.	9
Estouro de Buffer	Indica um estouro de buffer.	9
Exploração de DNS	Indica um DNS explorar.	9
Exploração de Telnet	Indica uma Telnet explorar.	9
Linux Explorar	Indica um explorar Linux.	9
UNIX Explorar	Indica um explorar UNIX.	9
Windows Explorar	Indica um Microsoft Windows explorar.	9
Exploração do Correio	Indica um servidor de correio explorar.	9
Exploração da Infraestrutura	Indica uma infra-estrutura de explorar.	9
Exploração Diversa	Indica uma exploração mista.	9
Exploração da Web	Indica uma explorador da web.	9
Interceptação de Sessão	Indica que uma sessão em sua rede foi extraordinário.	9
Worm Ativo	Indica um vírus ativo.	10
Dedução/Recuperação de Senha	Indica que um usuário solicitou acesso às suas informações de senha do banco de dados.	9
Exploração do FTP	Indica um servidor FTP explorar.	9
Exploração do RPC	Indica um RPC explorar.	9
Exploração do SNMP	Indica um SNMP explorar.	9
Exploração do NOOP	Indica um NOOP explorar.	9
Exploração do Samba	Indica um explorador Samba.	9
Exploração do Banco de Dados	Indica um explorador banco.	9
Exploração do SSH	Indica um SSH explorar.	9
Exploração do ICMP	Indica um ICMP explorar.	9
Exploração do UDP	Indica uma UDP explorar.	9
Exploração do Navegador	Indica uma exploração em seu navegador.	9
Exploração do DHCP	Indica um DHCP explorar.	9
Exploração de Acesso Remoto	Indicates a remote access exploit	9
Exploração do ActiveX	Indicates an exploit through an ActiveX application.	9
SQL Injection	Indica que uma injeção de SQL.	9

Tabela 101. categorias de baixo nível e níveis de severidade para o explorar categoria de eventos (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Cross-Site Scripting	Indica uma vulnerabilidade de script entre sites.	9
Vulnerabilidade de Sequência de Formatação	Indica uma vulnerabilidade da cadeia de formatação.	9
Exploração de Validação de Entrada	Indica que uma tentativa de explorar a validação de entrada foi detectado.	9
Remote Code Execution	Indica que uma tentativa de execução de código remota foi detectado.	9
Memória Distorção	Indica que um dano de memória explorar foi detectado.	9
Execução do Comando	Indicates that a remote command execution attempt was detected.	9

Malware

O software de categoria mal-intencionado a (malware) contém eventos que estão relacionados ao aplicativo e explora tentativas de estouro de buffer.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria malware.

Tabela 102. Categorias de baixo nível e níveis de severidade para categorias de eventos de malware.

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Malware Desconhecido	Indica um vírus desconhecido.	4
Porta dos Fundos Detectada	Indica que uma porta de volta para o sistema foi detectado.	9
Anexo de Correio Hostil	Indica um anexo de correio hostil.	6
Software Malicioso	Indica um vírus.	6
Download de Software Hostil	Indica um download de software hostil à sua rede.	6
Vírus Detectado	Indica que um vírus foi detectado.	8
Malware Diverso	Indica softwares maldosos diversos.	4
Cavalo de Troia Detectado	Indica que um trojam foi detectado.	7
Spyware Detectado	Indica que spyware foi detectado em seu sistema.	6

Tabela 102. Categorias de baixo nível e níveis de severidade para categorias de eventos de malware. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Varredura de conteúdo	Indica que uma tentativa de varredura de seu conteúdo foi detectado.	3
Falha de Varredura de Conteúdo	Indica que uma varredura de seu conteúdo falhou.	8
Varredura de conteúdo	Indica que uma varredura de seu conteúdo foi bem-sucedida.	3
Varredura de conteúdo em Andamento	Indica que uma varredura de seu conteúdo está em andamento.	3
Keylogger	Indica que um keylogger foi detectado.	7
Adware Detectado	Indica que Adware foi detectado.	4
Quarentena Bem-sucedida	Indicates that a quarantine action successfully completed.	3
Falha da Quarentena	Indica que uma ação de quarentena falhou.	8

Atividade Suspeita

categoria categoria suspeita contem eventos que estão relacionados a vírus, trojans, ataque as portas dos fundos, e outras formas de softwares hostis.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associadas à categoria da atividade suspeita.

Tabela 103. categorias de baixo nível e níveis de severidade para a categoria de eventos de atividades suspeitas

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento Suspeito Desconhecido	Indica um evento suspeito desconhecido.	3
Padrão Suspeito Detectado	Indica que um padrão suspeito foi detectado.	3
Conteúdo Modificado por Firewall	Indica que o conteúdo foi modificado pelo firewall.	3
Comando ou Dados Inválidos	Indica um comando ou dados inválidos.	3
Pacote Suspeito	Indica um pacote suspeito.	3
Atividade Suspeita	Indica atividade suspeita.	3
Nome do Arquivo Suspeito	Indica um nome de arquivo suspeito.	3
Atividade da Porta Suspeita	Indica atividade suspeita.	3

Tabela 103. categorias de baixo nível e níveis de severidade para a categoria de eventos de atividades suspeitas (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Roteamento Suspeito	Indica de roteamento suspeito.	3
Vulnerabilidade da Web Potencial	Indica da web vulnerabilidade em potencial.	3
Evento de Evasão Desconhecido	Indica um evento evasão desconhecido.	5
Spoof de IP	Indica um endereço IP. fraudam	5
Fragmentação de IP	Indica fragmentação de IP.	3
Sobrepondo Fragmentos de IP	Indica de sobreposição fragmentos IP.	5
Evasão do IDS	Indica uma evasão IDS.	5
Anomalia do Protocolo DNS	Indica um protocolo DNS anomalia.	3
Anomalia do Protocolo FTP	Indica um protocolo FTP anomalia.	3
Anomalia do Protocolo de Correio	Indica um protocolo de correio anomalia.	3
Anomalia do Protocolo de Roteamento	Indica um protocolo de roteamento anomalia.	3
Web Protocol Anomaly	Indica um protocolo da web anomalia.	3
Anomalia do Protocolo SQL	Indica um protocolo SQL anomalia.	3
Código Executável Detectado	Indica que um código executável foi detectado.	5
Evento Suspeito Diverso	Indica um evento suspeito diversos.	3
Fuga de Informações	Indicates an information leak.	1
Vulnerabilidade de Correio Potencial	Indica uma vulnerabilidade em potencial no servidor mail.	4
Vulnerabilidade de Versão Potencial	Indica uma vulnerabilidade em potencial na versão IBM Security QRadar SIEM.	4
Vulnerabilidade de FTP Potencial	Indica uma vulnerabilidade em potencial FTP.	4
Vulnerabilidade de SSH Potencial	Indica uma vulnerabilidade em potencial SSH.	4
Vulnerabilidade de DNS Potencial	Indica uma vulnerabilidade em potencial no servidor DNS.	4
Vulnerabilidade de SMB Potencial	Indica um potencial SMB (Samba) vulnerabilidade.	4

Tabela 103. categorias de baixo nível e níveis de severidade para a categoria de eventos de atividades suspeitas (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Vulnerabilidade de Banco de Dados Potencial	Indica uma vulnerabilidade em potencial no banco de dados.	4
Anomalia do Protocolo IP	Indica uma anomalia protocolo IP potencial	3
Endereço IP Suspeito	Indica que um endereço IP suspeita foi detectado.	2
Uso do Protocolo IP Inválido	Indica um protocolo IP inválido.	2
Protocolo Inválido	Indica um protocolo inválido.	4
Janela de eventos suspeitos	Indica um evento suspeito com uma tela em seu desktop.	2
Atividade suspeita de ICMP	Indica atividade suspeita ICMP.	2
Vulnerabilidade de NFS Potencial	Indica um sistema de arquivos de rede em potencial (NFS) vulnerabilidade.	4
Vulnerabilidade Potencial de NTTP	Indica uma potencial vulnerabilidade NNTP (Network News Transfer Protocol).	4
Potencial Vulnerabilidade de RPC	Indica uma potencial vulnerabilidade RPC.	4
Vulnerabilidade potencial de Telnet	Indica uma vulnerabilidade potencial de Telnet em seu sistema.	4
Vulnerabilidade potencial de SNMP	Indica uma vulnerabilidade em potencial SNMP.	4
Combinação de Sinalizador TCP Ilegal	Indica que uma combinação inválida de sinalizador TCP foi detectada.	5
Combinação de Sinalizador TCP Suspeita	Indica que uma combinação de sinalizador TCP potencialmente inválida foi detectada.	4
Uso de Protocolo ICMP Ilegal	Indica que um uso inválido do protocolo ICMP foi detectado.	5
Uso de Protocolo ICMP Suspeito	Indica que o uso do protocolo potencialmente inválido ICMP foi detectado.	4
Tipo de ICMP Ilegal	Indica que um tipo ICMP inválido foi detectado.	5
Código de ICMP Ilegal	Indica que um tipo ICMP inválido foi detectado.	5

Tabela 103. categorias de baixo nível e níveis de severidade para a categoria de eventos de atividades suspeitas (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Tipo de ICMP Suspeito	Indica que um tipo ICMP potencialmente inválido foi detectado.	4
Código de ICMP Suspeito	Indica que um código ICMP potencialmente inválido foi detectado.	4
porta TCP 0	Indica um pacote TCP utiliza uma porta reservada (0) para origem ou para destino.	4
Porta UDP 0	Indica um pacote UDP usa uma porta reservada (0) para orígem ou destino.	4
IP Hostil	Indica a utilização de um endereço IP hostil conhecido.	4
Lista de observação IP	Indica o uso de um endereço IP de uma lista de observação de endereços de IP.	4
IP ofensor conhecido	Indica a utilização de um endereço IP de um ofensor conhecido.	4
IP do RFC 1918 (privado)	Indica a utilização de um endereço IP a partir de um intervalo de endereços IP particulares.	4
Vulnerabilidade potencial de NTTP	Indica uma vulnerabilidade potencial VoIP.	4
Lista de bloqueio de endereços	Indica que um endereço IP está na lista de bloqueio.	8
Endereço de lista de observação	Indica que o endereço IP está na lista de endereços IP que estão sendo monitorados.	7
Darknet Endereço	Indica que o endereço IP faz parte de um darknet.	5
Endereço Botnet	Indica que o endereço é parte de uma bootnet.	7
Endereço suspeito	Indica que o endereço IP deverá ser monitorado.	5
Conteúdo inválido	Indica que conteúdo inválido foi detectado.	7
Certificado Inválido	Indica que um certificado inválido foi detectado.	7
Atividade do Usuário	Indica que a atividade do usuário foi detectado.	7
Uso de Protocolo Suspeito	Indica que um padrão suspeito foi detectado.	5

Tabela 103. categorias de baixo nível e níveis de severidade para a categoria de eventos de atividades suspeitas (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Atividade Suspeita BGP	Indica de uso suspeito do protocolo de roteamento de borda - BGP (Border Gateway Protocol) foi detectado.	5
Rotear Envenenamento	Indica que a corrupção de roteamento foi detectada.	5
Envenenamento ARP	Indica que envenenamento ARP-cache foi detectado.	5
Dispositivo Rogue Detectado	Indica que um dispositivo rouge foi detectado.	5

Sistema

A categoria do sistema contém eventos que estão relacionados a alterações do sistema, instalação de software, ou mensagens de status.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria do sistema.

Tabela 104. categorias de baixo nível e níveis de severidade para a categoria de eventos do sistema

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento do Sistema Desconhecido	Indica um evento do sistema desconhecido.	1
Inicialização do Sistema	Indica um reinício do sistema.	1
Configuração do sistema	Indica uma alteração na configuração do sistema.	1
Interrupção do Sistema	Indica que o sistema foi interrompida.	1
Falha do Sistema	Indica uma falha do sistema.	6
Status do Sistema	Indica qualquer evento de informações.	1
Erro de Sistema	Indica um erro do sistema.	3
Evento do Sistema Diverso	Indica um evento de sistema diversificadas.	1
Serviço Iniciado	Indica que os serviços do sistema foi iniciado.	1
Serviço Parado	Indica que os serviços do sistema parou.	1
Falha no Serviço	Indica uma falha do sistema.	6
Modificação de Registro Bem-sucedida	Indica que uma modificação no registro foi bem-sucedida.	1

Tabela 104. categorias de baixo nível e níveis de severidade para a categoria de eventos do sistema (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Modificação de Política do Host Bem-sucedida	Indica que uma modificação na política de host foi bem-sucedida.	1
Modificação de Arquivo Bem-sucedida	Indica que uma modificação de um arquivo foi bem-sucedida.	1
Modificação de Pilha Bem-sucedida	Indica que uma modificação para a pilha foi bem-sucedida.	1
Modificação de Aplicativo Bem-sucedida	Indica que uma modificação no aplicativo foi bem-sucedida.	1
Modificação de Configuração Bem-sucedida	Indica que uma modificação na configuração foi bem-sucedida.	1
Modificação de Serviço Bem-sucedida	Indica que uma modificação de um serviço foi bem-sucedida.	1
Modificação de Registro com Falha	Indica que uma modificação no registro falhou.	1
Modificação de Política do Host com Falha	Indica que uma modificação na política do host falhou.	1
Modificação de Arquivo com Falha	Indica que uma modificação em um arquivo falhou.	1
Modificação de Pilha com Falha	Indica que uma modificação para a pilha falhou.	1
Modificação de Aplicativo com Falha	Indica que uma modificação de um aplicativo falhou.	1
Modificação de Configuração com Falha	Indica que uma modificação na configuração falhou.	1
Modificação de Serviço com Falha	Indica que uma modificação para o serviço falhou.	1
Adição de Registro	Indica que um novo item foi incluído no registro.	1
Política do Host Criada	Indica que um novo entry foi incluído no registro.	1
Arquivo Criado	Indica que um novo foi criado no sistema.	1
Aplicativo Instalado	Indica que um novo aplicativo foi instalado no sistema.	1
Serviço Instalado	Indica que um novo serviço foi instalado no sistema.	1
Exclusão de Registro	Indica que uma entrada de registro foi excluído.	1
Política do Host Excluída	Indica que uma entrada de política de host foi excluído.	1

Tabela 104. categorias de baixo nível e níveis de severidade para a categoria de eventos do sistema (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Arquivo Excluído	Indica que um arquivo foi excluído.	1
Aplicativo Desinstalado	Indica que um aplicativo foi desinstalado.	1
Serviço Desinstalado	Indica que um serviço foi desinstalado.	1
Informativo do Sistema	Indica informações do sistema.	3
Permissão de Ação do Sistema	Indica que uma ação tentada no sistema foi autorizado.	3
Negação de Ação do Sistema	Indica que uma ação tentada no sistema foi negado.	4
Cron	Indica uma mensagem de crontab.	1
Status do Cron	Indica uma mensagem de status crontab.	1
Falha Cron	Indica uma mensagem de falha crontab.	4
Cron Bem-sucedido	Indica uma mensagem de êxito crontab.	1
Daemon	Indica uma mensagem de daemon.	1
Status do Daemon	Indica uma mensagem de status do daemon.	1
Falha do Daemon	Indicates a daemon failure message.	4
Daemon de Bem-sucedida	Indica uma mensagem de êxito do daemon.	1
Kernel	Indica uma mensagem de kernel.	1
Status do Kernel	Indica uma mensagem de status do kernel.	1
Falha Kernel	Indica uma mensagem de falha do kernel.	
Kernel Bem-sucedido	Indica uma mensagem de êxito do kernel.	1
Autenticação	Indica uma mensagem de autenticação.	1
- Informações	Indica uma mensagem informativa.	2
Nota	Indica uma mensagem de aviso.	3
Aviso	Indica uma mensagem de aviso.	5

Tabela 104. categorias de baixo nível e níveis de severidade para a categoria de eventos do sistema (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Erro	Indica uma mensagem de erro.	7
Critical	Indica uma mensagem crítica.	9
Depurar	Indica uma mensagem de depuração.	1
Mensagens	Indica uma mensagem genérica.	1
Privilégio de Acesso	Indica que o acesso privilégio foi tentado.	3
Alerta	Indica uma mensagem de alerta.	9
Emergência	Indica uma mensagem de emergência.	9
Status de SNMP	Indica uma mensagem de status SNMP.	1
Status do FTP	Indica uma mensagem de status do FTP.	1
Status do NTP	Indica uma mensagem de status do NTP.	1
A Rádio Access Point	Indica uma falha de ponto de acesso.	3
Incompatibilidade de Configuração de Protocolo de Criptografia	Indica uma incompatibilidade de configuração do protocolo de criptografia.	3
Dispositivo ou Client Authentication Server Malconfigurado	Indica que um dispositivo cliente ou servidor de autenticação não foi configurado adequadamente.	5
Espera Ativa Falha Ativar	Indica uma falha ativar hot standby.	5
Espera Ativa Falha Desativar	Indicates a hot standby disable failure.	5
Espera Ativa Ativado com êxito	Indica que um grupo foi incluído com êxito.	1
Espera Ativa Associação Perdida	Indica que uma associação hot standby foi perdida.	5
Falha de iniciação no Modo principal	falha de iniciação no modo principal.	5
MainMode Initiation Bem-sucedido	Indica que o início MainMode foi bem-sucedida.	1
MainMode de Status	Indica uma mensagem de status MainMode foi relatado.	1

Tabela 104. categorias de baixo nível e níveis de severidade para a categoria de eventos do sistema (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
QuickMode Falha Initiation	Indica que o início QuickMode falhou.	5
Quickmode Initiation Bem-sucedido	Indica que o início QuickMode foi bem-sucedida.	1
Quickmode de Status	Indica uma mensagem de status QuickMode foi relatado.	1
Licença Inválida	Indica um protocolo inválido.	3
Licença Expirada	Indica uma licença expirou.	3
New License Applied	Indica uma nova licença aplicado.	1
Erro de licença	Indica um erro de licença.	5
Status da Licença	Indica uma mensagem de status da licença.	1
Erro de configuração	Indica que foi detectado um erro de configuração.	5
Interrupção de Serviço	Indica que uma interrupção do serviço foi detectado.	5
Licença Excedido	Indica que o recursos de licença foram excedidos.	3
Status do Desempenho	Indica que o reassociação estação foi bem-sucedida.	1
Degradação do Desempenho	Indica que o desempenho estiver sendo prejudicado.	4
Configuração incorreta	Indica que uma configuração incorreta foi detectado.	5

Política

A categoria de política contém eventos que estão relacionados à administração da política de rede e ao monitoramento de recursos da rede quanto a violações de política.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de política.

Tabela 105. Categorias de baixo nível e níveis de severidade para a categoria de política

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Violação de política desconhecida	Indica uma violação de política desconhecida.	2
Violação de política da web	Indica uma violação de política da web.	2

Tabela 105. Categorias de baixo nível e níveis de severidade para a categoria de política (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Violação de política de acesso remoto	Indica uma violação de política de acesso remoto.	2
Violação de política de IRC/IM	Indica uma violação de política de mensagens instantâneas.	2
Violação de política de P2P	Indica uma violação de política ponto a ponto (P2P).	2
Violação de política de acesso de IP	Indica uma violação de política de acesso de IP.	2
Violação de política de aplicativo	Indica uma violação de política de aplicativo.	2
Violação de política de banco de dados	Indica uma violação de política de banco de dados.	2
Violação de política de limite de rede	Indica uma violação de política de limite de rede.	2
Violação de política de pornografia	Indica uma violação de política de pornografia.	2
Violação de política de jogos	Indica uma violação de política de jogos.	2
Violação de política diversa	Indica uma violação de política diversa.	2
Violação de política de conformidade	Indica uma violação de política de conformidade.	2
Violação de política de correio	Indica uma violação de política de correio.	2
Violação de política de IRC	Indica uma violação de política de IRC	2
Violação de política de IM	Indica uma violação de política que está relacionada a atividades de mensagens instantâneas (IM).	2
Violação de política de VoIP	Indica uma violação de política de VoIP	2
Com êxito	Indica uma mensagem de êxito da política.	1
Com falha	Indica uma mensagem de erro da política.	4

Desconhecido

A categoria desconhecido contém eventos que não são analisados e, portanto, não podem ser categorizados.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria desconhecido.

Tabela 106. Categorias de baixo nível e níveis de severidade para categorias desconhecidas.

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Desconhecido	Indica um evento de limite desconhecido.	3
Evento desconhecido de Snort	Indica um evento desconhecido. Snort	3
Evento do Dragon Desconhecido	Indica um evento desconhecido. Dragon	3
Evento do Pix Firewall Desconhecido	Indica um evento desconhecido. Cisco Private Internet Exchange (PIX) Firewall	3
Evento de Ponto de Mudança Desconhecido	Indica um evento desconhecido. HP TippingPoint	3
Evento do Servidor de Autenticação do Windows	Indica um evento desconhecido. Windows Auth Server	3
Evento do Nortel Desconhecido	Indica um evento desconhecido. Nortel	3
Armazenado	Indica um evento armazenado desconhecido.	3
Comportamental	Indica um evento comportamental desconhecido.	3
Limite	Indica um evento de limite desconhecido.	3
Anomalia	Indica um evento anomal desconhecido.	3

CRE

A categoria de evento de regra contêm eventos que são gerados de uma ofensa padrão, fluxo ou evento,

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria do CRE.

Tabela 107. Categorias de baixo nível

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento do CRE Desconhecido	Indica um mecanismo de regras customizadas de evento desconhecido.	5
Correspondência de Regra de Evento Único	Indica uma cruzada ofensa de eventos da regra de seqüência de correspondência.	5

Tabela 107. Categorias de baixo nível (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Correspondência de Regra de Sequência de Eventos	Indica uma correspondência de regra de sequência de eventos.	5
Correspondência de Regra de Sequência de Eventos de Ofensa Cruzado	Indica uma cruzada ofensa de eventos da regra de seqüência de correspondência.	5
Correspondência de Regra de Ofensa	Indica uma correspondência de regra de ofensa.	5

Exploração Potencial

A categoria de exploração potencial contém eventos que são relacionados a explorações potenciais de aplicativos ou tentativas de estouro de buffer.

A guia a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria de exploração potencial.

Tabela 108. Categorias de baixo nível e níveis de severidade para a categoria de exploração potencial.

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ataque potencial de exploração desconhecido	Indica que um ataque potencial de exploração foi detectado.	7
Estouro potencial de buffer	Indica que estouro potencial de buffer foi detectado.	7
Exploração potencial por meio do DNS	Indica que foi detectado um ataque potencial de exploração por meio do servidor DNS	7
Exploração potencial pelo Telnet	Indica que foi detectado um ataque de exploração potencial por meio do Telnet.	7
Exploração potencial pelo Linux	Indica que foi detectado um ataque de exploração potencial por meio do Linux	7
Exploração potencial pelo UNIX	Indica que foi detectado um ataque de exploração potencial por meio do UNIX.	7
Exploração potencial pelo Windows	Indica que foi detectado um ataque de exploração potencial por meio do Windows.	7
Exploração potencial por e-mail	Indica que foi detectado um ataque de exploração potencial por e-mail.	7

Tabela 108. Categorias de baixo nível e níveis de severidade para a categoria de exploração potencial. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Exploração potencial de infraestrutura	Indica que foi detectado um ataque de exploração potencial na infra-estrutura do sistema.	7
Exploração potencial diversa	Indica que um ataque potencial de exploração foi detectado.	7
Exploração potencial pela web	Indica que foi detectado um ataque de exploração potencial pela web.	7
Conexão potencial de Botnet	Indica que foi detectado um ataque de exploração potencial que usa botnet.	6
Atividade potencial de Worm	Indica que foi detectado um ataque de exploração potencial atividade de worm.	6

Usuário definido

A categoria Usuário definido contêm eventos que estão relacionados a objetos definidos pelo usuário

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria Usuário definido.

Tabela 109. Categorias de baixo nível e níveis de severidade da categoria Usuário definido

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sentry baixo customizado	Indica um evento com anormalidade customizado de baixa severidade.	3
Sentry médio customizado	Indica um evento com anormalidade customizado de média severidade.	5
Sentry alto customizado	Indica um evento com anormalidade customizado de alta severidade.	7
Sentry 1 customizado	Indica um evento com anormalidade customizado com um nível de severidade 1.	1
Sentry 2 customizado	Indica um evento com anormalidade customizado com um nível de severidade 2.	2
Sentry 3 customizado	Indica um evento com anormalidade customizado com um nível de severidade 3.	3

Tabela 109. Categorias de baixo nível e níveis de severidade da categoria Usuário definido (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sentry 4 customizado	Indica um evento com anormalidade customizado com um nível de severidade 4.	4
Sentry 5 customizado	Indica um evento com anormalidade customizado com um nível de severidade 5.	5
Sentry 6 customizado	Indica um evento com anormalidade customizado com um nível de severidade 6.	6
Sentry 7 customizado	Indica um evento com anormalidade customizado com um nível de severidade 7.	7
Sentry 8 Customizado	Indica um evento com anormalidade customizado com um nível de severidade 8.	8
Sentry 9 customizado	Indica um evento com anormalidade customizado com um nível de severidade 9.	9
Política baixa customizada	Indica um evento de política customizada com um nível de severidade baixo.	3
Política média customizada	Indica um evento de política customizada com um nível de severidade médio.	5
Política alta customizada	Indica um evento de política customizada com um nível de severidade alto.	7
Política 1 customizada	Indica um evento de política customizada com um nível de severidade 1.	1
Política 2 customizada	Indica um evento de política customizada com um nível de severidade 2.	2
Política 3 customizada	Indica um evento de política customizada com um nível de severidade 3.	3
Política 4 customizada	Indica um evento de política customizada com severidade de nível 4.	4
Política 5 customizada	Indica um evento de política customizada com um nível de severidade 5.	5

Tabela 109. Categorias de baixo nível e níveis de severidade da categoria Usuário definido (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Política 6 customizada	Indica um evento de política customizada com um nível de severidade 6.	6
Política 7 customizada	Indica um evento de política customizada com um nível de severidade 7.	7
Política 8 customizada	Indica um evento de política customizada com um nível de severidade 8.	8
Política 9 customizada	Indica um evento de política customizada com um nível de severidade 9.	9
Usuário baixo customizado	Indica um evento do usuário customizado com um nível de severidade baixa.	3
Usuário médio customizado	Indica um evento do usuário customizado com um nível de severidade média.	5
Usuário alto customizado	Indica um evento do usuário customizado com um nível de severidade alta.	7
Usuário 1 customizado	Indica um evento do usuário customizado com um nível de severidade 1.	1
Usuário 2 customizado	Indica um evento do usuário customizado com um nível de severidade 2.	2
Usuário 3 customizado	Indica um evento do usuário customizado com um nível de severidade 3.	3
Usuário 4 customizado	Indica um evento do usuário customizado com um nível de severidade 4.	4
Usuário 5 customizado	Indica um evento do usuário customizado com um nível de severidade 5.	5
Usuário 6 customizado	Indica um evento do usuário customizado com um nível de severidade 6.	6
Usuário 7 customizado	Indica um evento do usuário customizado com um nível de severidade 7.	7
Usuário 8 customizado	Indica um evento do usuário customizado com um nível de severidade 8.	8
Usuário 9 customizado	Indica um evento do usuário customizado com um nível de severidade 9.	9

SIM de auditoria

A categoria Auditoria SIM contém eventos que estão relacionadas à interação do usuário com o QRadar Console e recursos administrativos.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de gravidade associado para a categoria SIM de auditoria.

Tabela 110. categorias de baixo nível e níveis de gravidade para a categoria Auditoria SIM

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Autenticação do Usuário SIM	Indica um login de usuário ou logout no Console.	5
Alteração de Configuração SIM	Indica que um usuário alterou a configuração ou a implementação SIM.	3
Autenticação do Usuário SIM	Indica que um usuário iniciou um processo, como iniciar um backup ou gerar um relatório, no módulo SIM.	3
Sessão Criada	Indica que uma sessão do usuário foi criada.	3
Sessão Destruído	Indica que uma sessão do usuário foi destruída.	3
Sessão Admin Criada	Indica que uma sessão admin foi criado.	
Sessão de Administrador Destruídas	Indica que uma sessão do administrador foi destruída.	3
Sessão de Autenticação Inválida	Indica uma autenticação de sessão inválida.	5
Autenticação da Sessão Expirado	Indica que uma autenticação de sessão expirou.	3
Configuração de gerenciador de risco	Indica que um usuário alterou a configuração IBM Security QRadar Risk Manager.	3

Descoberta do Host VIS

Quando o componente VIS descobre e armazena novos hosts, portas, ou as vulnerabilidades que são detectados na rede, o componente VIS gera eventos. Esses eventos são enviados para o Coletor de eventos para ser correlato a outro evento de segurança.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a VIS categoria de descoberta de host.

Tabela 111. categorias de baixo nível e níveis de severidade para o VIS de host de descoberta da categoria

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Descoberta do Novo Host	Indica que o componente VIS detectou um novo host.	3
Nova porta descoberta	Indica que o componente VIS detectou uma nova porta aberta.	3
Nova descoberta vulnerabilidade	Indica que o componente VIS detecta uma nova vulnerabilidade.	3
Descoberta do novo do S.O.	Indica que o componente VIS detectou um novo sistema operacional em um host.	3
Massa do host descoberto	Indica que o componente VIS detectou muitos novos hosts em um curto período.	3

Aplicação

A categoria de aplicação contêm eventos que estão relacionados a atividade de aplicação, tais como email ou atividade de FTP.

A tabela abaixo descreve as categorias de evento de nível inferior associadas a níveis de severidade para categoria do aplicativo.

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo.

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Correio aberto	Indica que uma conexão de email foi estabilizada.	1
Email encerrado.	Indica que uma conexão de email foi encerrada.	1
Email reconfigurado	Indica que um email foi reconfigurado.	3
Email finalizado	Indica que uma conexão de email foi finalizada.	4
Email negado	Indica que uma conexão de email foi negada.	4
Email em andamento	Indica que uma conexão de email está sendo tentada.	1
Email atrasado	Indica que uma conexão de email foi atrasada.	4
Email na fila	Indica que uma conexão de email estava na fila.	3
Email redirecionado	Indica que uma conexão de email foi redirecionada.	1
FTP aberto	Indica que uma conexão FTP foi aberta.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
FTP fechado	Indica que uma conexão FTP foi fechada.	1
FTP reconfigurado	Indica que uma conexão FTP foi recuperada.	3
FTP Finalizado	Indica que uma conexão FTP foi finalizada.	4
FTP Negado	Indicates that an FTP connection was denied.	4
FTP em andamento	Indica que uma conexão FTP está em progresso.	1
FTP redirecionado	Indica que uma conexão FTP foi redirecionada.	3
HTTP aberto	Indica que uma conexão HTTP foi estabelecida.	1
HTTP fechado	Indica que uma conexão HTTP foi fechada.	1
Reconfiguração de HTTP	Indica que uma conexão HTTP foi reconfigurada.	3
HTTP finalizado	Indica que uma conexão HTTP foi finalizada.	4
HTTP Negado	Indica que uma conexão HTTP foi negada.	4
HTTP em andamento	Indica que uma conexão HTTP está em progresso.	1
HTTP em atraso	Indica que uma conexão HTTP está em atraso.	3
HTTP em fila	Indica que uma conexão HTTP estava em fila.	1
Redirecionamento do HTTP	Indica que que uma conexão HTTP foi redirecionada.	1
Proxy HTTP	Indica que uma conexão HTTP está entrando no servidor proxy.	1
HTTPS aberto	Indica que uma conexão HTTPS foi estabelecida.	1
HTTPS Closed	dica que uma conexão HTTPS foi encerrada.	1
HTTPS reconfigurada	Indica que uma conexão HTTPS foi reconfigurada.	3
HTTPS finalizada.	Indica que uma conexão HTTPS foi finalizada.	4
HTTPS negado	Indica que uma conexão HTTPS foi negada.	4
HTTPS em progresso	Indica que uma conexão HTTPS está em progresso.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
HTTPS em atraso.	Indica que uma conexão HTTPS está em atraso.	3
HTTPS em fila.	Indica que uma conexão HTTPS foi enfileirada.	3
HTTPS redirecionada.	Indica que uma conexão HTTPS foi redirecionada.	3
Proxy HTTPS	Indica que uma conexão HTTPS está entrando no servidor proxy.	1
SSH aberto	Indica que uma conexão SSH foi estabilizada.	1
SSH fechada	Indica que uma conexão SSH foi fechada.	1
SSH reconfigurada	Indica que uma conexão SSH foi reconfigurada.	3
SSH finalizada	Indica que uma conexão SSH foi finalizada.	4
SSH negada	Indica que uma conexão SSH foi negda.	4
SSH em progresso	Indica que uma sessão SSH está em progresso.	1
Acesso remoto aberto	Indica que uma conexão de acesso remoto foi estabelecida.	1
Acesso remoto fechado	Indica que uma conexão de acesso remoto foi fechada.	1
Reconfiguração de acesso remoto	Indica que uma conexão de acesso remoto foi reconfigurada.	3
Acesso remoto finalizado.	Indica que uma conexão de acesso remoto foi finalizada.	4
Acesso remoto negado	Indica que um acesso remoto foi negado.	4
Acesso remoto em progresso	Indica que um acesso remoto está em progresso.	1
Acesso remoto em atraso	Indica que um acesso remoto está em atraso.	3
Acesso remoto redirecionado	Indica que um acesso remoto foi redirecionado.	3
VPN aberto	Indica que uma conexão VPN foi aberta.	1
VPN fechada	Indica que uma conexão VPN foi fechada.	1
VPN reconfigurada	Indica que uma conexão VPN foi reconfigurada.	3

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
VPN finalizado	Indica que uma conexão VPN foi finalizada.	4
VPN negado	Indica que uma conexão VPN foi negada.	4
VPN em andamento	Indica que uma conexão VPN está em andamento.	1
VPN em atraso	Indica que uma conexão VPN está em atraso.	3
VPN em fila	Indica que uma conexão VPN está em fila	3
VPN redirecionada	Indica que uma conexão VPN foi redirecionada	3
RDP aberto	Indica que uma conexão RDP foi estabelecida.	1
RDP fechado	Indica que uma conexão RDP foi fechada.	1
RDP reconfigurada	Indica que uma conexão RDP foi fechada.	3
RDP finalizada	Indica que uma conexão RDP foi finalizada.	4
RDP negada	Indica que uma conexão RDP foi negada.	4
RDP em andamento	Indica que uma conexão RDP está em andamento.	1
RDP redirecionada	Indica que uma conexão RDP foi redirecionada.	3
Transferência de arquivo aberta	Indica que conexão de transferência de arquivos foi estabelecida.	1
Transferência de arquivos encerrada	Indica que conexão de transferência de arquivos foi encerrada.	1
Transferência de arquivos reconfigurada	Indica que uma transferência de arquivos foi reconfigurada.	3
Transferência de arquivos finalizada	Indica que uma conexão de transferência de arquivos foi finalizada.	4
Transferência de arquivos Negado	Indica que conexão de transferência de arquivos foi negada.	4
Transferência de arquivos em andamento	Indica que uma conexão de transferência de arquivos está em andamento.	1
Transferência de arquivos em atraso	Indica que uma conexão de transferência de arquivos foi adiado.	3

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Fila de transferência de arquivos	Indica que uma conexão de transferência de arquivos foi enfileirada.	3
Transferência de arquivos redirecionada	Indica que uma conexão de transferência de arquivo foi redirecionado.	3
Aberto de DNS	Indica que uma conexão de DNS foi estabelecida.	1
DNS fechado	Indica que uma conexão de DNS foi fechado.	1
Reconfigurar DNS	Indica que uma conexão de DNS foi reconfigurada.	5
DNS Terminated	Indica que uma conexão de DNS foi terminada.	5
DNS Negado	Indica que uma conexão de DNS foi negada.	5
DNS Em Andamento	Indica que uma conexão de DNS está em andamento.	1
DNS Atrasado	Indica que uma conexão de DNS foi adiado.	5
DNS redirecionado	Indica que uma conexão de DNS foi redirecionada.	4
Bate-papo (chat) aberto	Indica que uma conexão de bate-papo foi aberta.	1
Bate-papo Encerrado	Indica que uma conexão de bate-papo foi encerrado.	1
Bate-Papo Reconfigurado	Indica que uma conexão de bate-papo foi reconfigurada.	3
Bate-papo Terminado	Indica que uma conexão de bate-papo foi finalizada.	3
Bate-papo Negado	Indica que uma conexão de bate-papo foi negado.	3
Bate-papo em andamento	Indica que uma conexão de bate-papo está em andamento.	1
Bate-papo redirecionado	Indica que uma conexão de bate-papo foi redirecionada.	1
Banco de dados aberto	Indica que uma conexão com o banco de dados foi estabelecida.	1
Banco de dados encerrado	Indica que uma conexão com o banco de dados foi encerrada.	1
Reconfiguração do Banco de Dados	Indica que uma conexão com o banco de dados foi reconfigurado.	5

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Banco de dados finalizado	Indica que um banco de dados foi finalizado.	5
Banco de dados negado	Indica que um banco de dados foi negado.	5
Banco de dados em progresso	Indica que um banco de dados está em progresso.	1
Banco de dados redirecionado	Indica que um banco de dados foi redirecionado.	3
SMTP aberta	Indica que uma conexão SMTP foi aberta.	1
SMTP fechada	Indica que uma conexão SMTP foi fechada.	1
SMTP reconfigurada	Indica que uma conexão SMTP foi reconfigurada.	3
SMTP finalizado	Indica que uma conexão SMTP foi finalizada.	5
SMTP Negado	Indica que uma conexão SMTP foi negada.	5
SMTP em andamento	Indica que uma conexão SMTP está em andamento.	1
SMTP em atraso	Indica que uma conexão SMTP está em atraso.	3
SMTP em fila	Indica que uma conexão SMTP está em fila.	3
SMTP redirecionada	Indica que uma conexão SMTP foi redirecionada.	3
Autenticação Aberta	Indica que uma conexão do servidor de autorização foi estabelecida.	1
Autenticação Encerrada	I ndica que uma conexão do servidor de autorização foi encerrada.	1
Autenticação reconfigurada	Indica que uma conexão do servidor de autorização foi reconfigurada.	3
Autenticação finalizada	Indica que uma conexão do servidor de autorização foi finializada.	4
Autenticação negada	Indica que uma conexão do servidor de autorização foi negada.	4
Autenticação em andamento	Indica que uma conexão do servidor de autorização está em andamento.	1
Autenticação em atraso	Indica que uma conexão do servidor de autorização foi atrasada.	3

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Autenticação Enfileirada	Indica que uma conexão do servidor de autorizações foi enfileirada.	3
Autenticação Redirecionada	Indica que uma conexão do servidor de autorização foi redirecionada.	2
P2P Aberta	Indioca que uma conerxão ponto-a-ponto foi estabelecida.	1
P2P encerrada	Indica que uma conexão P2P foi encerrada.	1
P2P reconfigurada	Indica que uma conexão P2P foi reconfigurada.	4
P2P finalizada	Indica que uma conexão P2P foi finalizada.	4
P2P negada	Indica que uma conexão P2P foi negada.	3
P2P em progresso	Indica que uma conexão P2P está em progresso.	1
Web aberta	Indica que uma conexão da Web foi estabelecida.	1
Web encerrada	Indica que uma conexão da Web foi encerrda.	1
Web reconfigurada	Indica que uma conexão da Web foi reconfigurada.	4
Web encerrada	Indica que uma conexão da Web foi encerrada.	4
Web negada	Indica que uma conexão da Web foi negado.	4
Web em Andamento	Indica que uma conexão da Web está em andamento.	1
Atrasado da Web	Indica que uma conexão da Web foi atrasado.	3
Fila Web	Indica que uma conexão da Web foi enfileirada.	1
Web redirecionada	Indica que uma conexão da Web foi redirecionada.	1
Proxy da Web	Indica que uma conexão da Web entrou em proxy	1
Aberto VoIP	Indica que uma conexão de Voz sobre IP (VoIP) foi estabelecida.	1
Fechado VoIP	Indica que uma conexão VoIP foi fechado.	1
Reconfigurar VoIP	Indica que uma conexão VoIP foi reconfigurado.	3

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
VoIP finalizada	Indica que uma conexão VoIP foi finalizado.	3
VoIP negado	I ndica que uma conexão VoIP foi negada.	3
VoIP em andamento	Indica que uma conexão VoIP está em progresso.	1
VoIP Atrasado	Indica que uma conexão VoIP foi atrasado.	3
VoIP redirecionado	Indica que uma conexão VoIP foi redirecionado.	3
Sessão LDAP Iniciado	Indica uma sessão LDAP iniciada.	1
Sessão LDAP Finalizado	Indica uma sessão LDAP terminou.	1
Sessão LDAP Negado	Indica que uma sessão LDAP foi negado.	3
Status da Sessão do LDAP	Indica que uma mensagem de status de sessão LDAP foi relatado.	1
Falha de Autenticação LDAP	Indica que uma autenticação LDAP falhou.	4
Autenticação LDAP Bem-sucedido	Indica que uma autenticação LDAP foi bem-sucedida.	1
Sessão AAA Iniciada	iIndica que uma Autenticação, Autorização e sessão Contabilidade (AAA) iniciou.	1
Sessão AAA Encerrada	Indica que uma sessão AAA foi encerrada.	1
Sessão AAA Negada	Indica que uma sessão AAA foi negado.	3
Status da Sessão AAA	Indica que uma mensagem de status da sessão AAA foi relatado.	1
Falha de Autenticação AAA	Indica que uma autenticação AAA falhou.	4
Autenticação Bem-sucedido AAA	Indica que uma autenticação AAA foi bem-sucedida.	1
Falha de Autenticação IPSEC	Indica que uma autenticação da Internet Protocol Security (IPSEC) falhou.	4
IPSEC Autenticação Bem-sucedido	Indica que uma IPSEC de autenticação foi bem-sucedida.	1
Sessão Iniciada IPSEC	Indica que uma sessão IPSEC iniciado.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão Encerrada IPSEC	Indica que uma sessão IPSEC terminou.	1
Erro IPSEC	Indica que uma mensagem de erro IPSEC foi relatado.	5
Status do IPSEC	Indica que uma mensagem de status da sessão IPSEC foi relatada.	1
Sessão Aberta IM	Indica que uma sessão Instant Messenger (IM) foi estabelecida.	1
O IM Fechado Sessão	Indica que uma sessão de MI foi fechada.	1
Reconfigurar Sessão IM	Indica que uma sessão de MI foi redefinido.	3
Sessão IM Terminada	Indica que uma sessão de MI foi finalizado.	3
Sessão IM negada	Indica que uma sessão do IM foi negado.	3
Sessão IM em andamento	Indica que uma sessão de MI está em andamento.	1
Sessão IM Atrasada	Indica que uma sessão IM foi atrasada	3
Sessão IM direcionada	Indica que uma sessão de MI foi redirecionada.	3
Sessão Aberta WHOIS	Indica que uma sessão WHOIS foi estabelecida.	1
Sessão Fechado WHOIS	Indica que uma sessão WHOIS foi fechado.	1
Reconfigurar Descartar Sessão	Indica que um WHOIS sessão foi redefinido.	3
Sessão Terminada WHOIS	Indica que uma sessão WHOIS foi finalizada.	3
Sessão Negado WHOIS	Indica que uma sessão WHOIS foi negado.	3
Sessão WHOIS em andamento	Indica que uma sessão do WHOIS está em andamento.	1
Sessão WHOIS finalizada	Indica que uma sessão WHOIS foi finalizada.	3
Sessão de rastreio de rotas aberta	Indica que uma sessão de rastreio de rotas foi estabelecida.	1
Sessão de rastreio de rotas fechada	Indica que uma sessão de rastreio de rotas foi fechada.	1
Sessão de rastrio de rotas fechado	Indica que uma sessão de rastreio de rotas foi negada.	3

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão rastreio de rotas em andamento	Indica que uma sessão de rastrio de rotas está em andamento.	1
Sessão TN3270 aberta	O TN3270 é um programa de emulação de terminal, que é usado para conectar a um IBM terminal 3270. Essa categoria indica que uma sessão TN3270 foi estabelecida.	1
Sessão TN3270 Fechada	Indica que uma sessão TN3270 foi fechada.	1
Reconfigurar Sessão TN3270	Indica que uma sessão TN3270 foi reconfigurada.	3
Sessão TN3270 terminada	Indica que uma sessão TN3270 foi finalizada.	3
Sessão TN3270 Negada	Indica que uma sessão TN3270 foi negada.	3
Sessão TN3270 em andamento	Indica que uma sessão do TN3270 está em andamento.	1
Sessão TFTP aberta	Indica que uma sessão de TFTP foi estabelecida.	1
Sessão TFTP de Fechada	Indica que uma sessão de TFTP estava fechada.	1
Reconfigurar sessão TFTP	Indica que uma sessão TFTP foi reconfigurada.	3
Sessão TFTP terminada	Indica que uma sessão TFTP foi finalizada.	3
Sessão TFTP negada	Indica que uma sessão TFTP foi negada.	3
Sessão TFTP em progresso	Indica que uma sessão de TFTP está em andamento.	1
Sessão Aberta Telnet	Indica que uma sessão Telnet foi estabelecida.	1
Sessão Telnet fechada	Indica que uma sessão Telnet foi fechada.	1
Reconfigurar Sessão Telnet	Indica que uma sessão Telnet foi reconfigurada.	3
Telnet Sessão Terminada	Indica que uma sessão Telnet foi finalizado.	3
Sessão Telnet negada	Indica que uma sessão Telnet foi negada.	3
Sessão Telnet em progresso	Indica que uma sessão Telnet está em progresso.	1
Sessão syslog aberta	Indica que uma sessão syslog foi estabelecida.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão syslog encerrada	Indica que uma sessão do syslog foi fechada.	1
Sessão Syslog negada	Indica que uma sessão syslog foi negada.	3
Sessão syslog em progresso	Indica que uma sessão do syslog está em progresso.	1
Sessão SSL Aberta	Indica que uma sessão da Camada Soquete Seguro(Secure Socket Layer - SSL) foi estabelecida.	1
Sessão SSL Fechada	Indica que uma sessão SSL foi fechada.	1
Reconfigurar de Sessão SSL	Indicates that an SSL session was reset.	3
Sessão SSL Terminada	Indica que uma sessão SSL foi finalizada.	3
Sessão SSL Negada	Indica que uma sessão SSL foi negada.	3
Sessão SSL em andamento	Indica que uma sessão SSL está em andamento.	1
Sessão SNMP Aberta	Indica que uma sessão SNMP (Simple Network Management Protocol) foi estabelecida.	1
Sessão SNMP fechada	Indica que uma sessão SNMP foi fechada.	1
Sessão SNMP negada	Indica que uma sessão SNMP foi negada.	3
Sessão SNMP em andamento	Indica que uma sessão SNMP está em andamento.	1
Sessão SMB aberta	Indica que uma sessão SMB (Server Message Block) foi estabelecida.	1
Sessão SMB fechada	Indica que uma sessão SMB foi fechada.	1
Sessão SMB reconfigurada	Indica que uma sessão SMB foi redefinida.	3
Sessão SMB terminada	Indica que uma sessão SMB foi finalizada.	3
Sessão SMB negado	Indica que uma sessão SMB foi negado.	3
Sessão SMB em andamento	Indica que uma sessão SMB está em andamento.	1
Sessão de fluxo de mídia em aberto	Indica que uma sessão de fluxo de mídia está em aberto foi estabelecida.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão de fluxo de mídia fechada	Indica que uma sessão de fluxo de mídia foi fechado.	1
Sessão de reconfiguração de fluxo de mídia	Indica que uma sessão de fluxo de mídia foi redefinida.	3
Sessão de fluxo de mídia finalizada	Indica que uma sessão de fluxo de mídia foi finalizada.	3
Sessão de fluxo de mídia negada	Indica que uma sessão de fluxo de mídia foi negada.	3
Sessão de fluxo de mídia em andamento	Indica que uma sessão de fluxo de midia está em andamento.	1
Sessão RUSERS Aberta	Indica que uma sessão RUSERS foi estabelecida.	1
Sessão RUSERS fechada	Indica que uma sessão RUSERS foi fechada.	1
Sessão RUSERS negado	Indica que uma sessão RUSERS foi negada.	3
Sessão RUSERS em andamento	Indica que uma sessão RUSERS está em andamento.	1
Sessão rsh em aberto	Indica que a sessão(rsh) foi estabelecida.	1
Sessão Rsh encerrada	Indica que uma sessão rsh foi fechada.	1
Sessão Rsh reconfigurarada	Indica que uma sessão rsh foi reconfigurada.	3
Sessão Rsh terminada	Indica que uma sessão rsh foi finalizada.	3
Sessão Rsh negada	Indica que uma sessão rsh foi negada.	3
Sessão Rsh em andamento	Indica que uma sessão rsh está em andamento.	1
Sessão RLOGIN em aberto	Indica que uma sessão (RLOGIN) foi estabelecida.	1
Sessão RLOGIN encerrada	Indica que uma sessão RLOGIN foi encerrada.	1
Sessão RLOGIN reconfigurada	Indica que uma sessão RLOGIN foi reconfigurada.	3
Sessão RLOGIN finalizada	Indica que uma sessão RLOGIN foi finalizada.	3
Sessão RLOGIN negada	Indica que uma sessão RLOGIN foi negada.	3
Sessão RLOGIN em andamento	Indica que uma sessão RLOGIN está em andamento.	1
Sessão REXEC em aberto	Indica que uma sessão (Remote Execution) REXEC foi estabelecida.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão REXEC fechada	Indica que uma sessão REXEC foi fechada.	1
Reconfigurar Sessão REXEC	Indica que uma sessão foi REXEC redefinida.	3
Sessão REXEC finalizada	Indica que uma sessão REXEC foi finalizada.	3
Sessão REXEC Negada	Indica que uma sessão REXEC foi negada.	3
Sessão REXEC em andamento	Indica que uma sessão REXEC está em andamento.	1
Sessão RPC em aberto	Indica que a Chanmada de Procedimento Remoto foi estabelecida.	1
Sessão RPC fechada	Indica que uma sessão RPC foi fechada.	1
Sessão RPC recuperada	Indica que uma sessão RPC foi redefinida.	3
Sessão RPC finalizada	Indica que uma sessão RPC foi finalizada.	3
Sessão RPC negada	Indica que uma sessão RPC foi negada.	3
Sessão RPC em andamento	Indica que uma sessão RPC está em andamento.	1
Sessão NTP em aberto	Indica que uma sessão Network Time Protocol (NTP) foi estabelecida.	1
Sessão NTP fechado	Indica que uma sessão NTP foi fechada.	1
Reconfigurar sessão NTP	Indica que uma sessão NTP foi reconfigurada.	3
Sessão NTP finalizada	Indica que uma sessão NTP foi finalizado.	3
Sessão NTP negado	Indica que uma sessão NTP foi negada.	3
Sessão NTP em andamento	Indica que uma sessão de NTP está em andamento.	1
Sessão NNTP em aberto	Indica que uma sessão Network News Transfer Protocol (NNTP) foi estabelecida.	1
Sessão NNTP fechado	Indica que uma sessão NNTP foi fechada.	1
Reconfigurar sessão NNTP	Indica que uma sessão NNTP foi reconfigurada.	3
Sessão NNTP finalizada	Indica que uma sessão NNTP foi finalizada.	3

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão NNTP negado	Indica que uma sessão NNTP foi negado.	3
Sessão NNTP em andamento	Indica que uma sessão NNTP está em andamento.	1
Sessão NFS emm aberto	Indica que uma sessão NFS (Network File System) foi estabelecida.	1
Sessão NFS fechada	Indica que uma sessão NFS foi fechada.	1
Sessão NFS reconfigurada	Indica que uma sessão NFS foi reconfigurada.	3
Sessão NFS finalizada	Indica que uma sessão NFS foi finalizada.	3
Sessão NFS negada	Indica que uma sessão do NFS foi negada.	3
Sessão NFS em andamento	Indica que uma sessão de NFS está em andamento.	1
Sessão NPC em aberto	Indica que uma sessão o Network Control Program (NCP) foi estabelecida.	1
Sessão NPC fechada	Indica que uma sessão do NCP foi fechada.	1
Sessão NCP reconfigurada	Indica que uma sessão do NCP foi reconfigurada.	3
Sessão NPC finalizada	Indica que uma sessão do NCP foi finalizada.	3
Sessão NCP negada	Indica que uma sessão do NCP foi negada.	3
Sessão NCP em andamento	Indica que uma sessão do NCP está em andamento.	1
Sessão NetBIOS em aberto	Indica que uma sessão NetBIOS foi estabelecida.	1
Sessão NetBIOS fechada	Indica que uma sessão NetBIOS foi fechada.	1
Sessão NetBIOS Reconfigurada	Indica que uma sessão NetBIOS foi reconfigurada.	3
Sessão NetBIOS finalizada	Indica que uma sessão NetBIOS foi finalizada.	3
Sessão NetBIOS negada	Indica que uma sessão NetBIOS foi negada.	3
Sessão NetBIOS Em Andamento	Indica que uma sessão NetBIOS está em andamento.	1
Sessão MODBUS em aberto	Indica que uma sessão MODBUS foi estabelecida.	1
Sessão MODBUS fechado	Indica que uma sessão MODBUS foi fechada.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão MODBUS reconfigurada	Indica que uma sessão MODBUS foi redefinida.	3
Sessão MODBUS finalizada	Indica que uma sessão MODBUS foi finalizada.	3
MODBUS Sessão negada	Indica que uma sessão MODBUS foi negada.	3
Sessão MODBUS em andamento	Indica que uma sessão MODBUS está em andamento.	1
Sessão LPD em aberto	Indica que uma sessão Line Printer Daemon (LPD) foi estabelecida.	1
Sessão LPD fechada	Indica que uma sessão LPD foi fechada.	1
Sessão LPD resetada	Indica que uma sessão LPD foi reconfigurada.	3
Sessão LPD finalizada	Indica que uma sessão LPD foi finalizada.	3
Sessão LPD negada	Indica que uma sessão LPD foi negada.	3
Sessão LPD em andamento	Indica que uma sessão LPD está em andamento.	1
Lotus Notes Sessão Aberta	Indica que uma sessão Lotus Notes foi estabelecida.	1
Lotus Notes Sessão encerrada	Indica que uma sessão Lotus Notes foi fechada.	1
Lotus Notes Sessão reconfigurada	Indica que uma sessão Lotus Notes foi reconfigurada.	3
Lotus Notes Sessão Terminada	Indica que uma sessão Lotus Notes foi encerrada.	3
Lotus Notes Sessão Negada	Indica que uma sessão Lotus Notes foi negada.	3
Lotus Notes Sessão negada	Indica que uma sessão Lotus Notes está em andamento.	1
Sessão Aberta Kerberos	Indica que uma sessão Kerberos foi estabelecida.	1
Sessão Kerberos fechada	Indica que uma sessão Kerberos foi fechada.	1
Sessão Keberos reconfigurada	Indica que uma sessão do Kerberos foi reconfigurado.	3
Sessão Kerberos finalizada	Indica que uma sessão Kerberos foi finalizada.	3
Sessão Kerberos negada	Indica que uma sessão Kerberos foi negada.	3
Sessão Kerberos em andamento	Indica que uma sessão do Kerberos está em andamento.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão IRC Aberta	Indica que uma sessão Internet Relay Chat (IRC) foi estabelecida.	1
Sessão IRC fechada	Indica que uma sessão IRC foi fechado.	1
Reconfigurar sessão IRC	Indica que uma sessão IRC foi reconfigurada	3
Sessão IRC finalizada	Indica que uma sessão IRC foi finalizada.	3
Sessão IRC negada	Indica que uma sessão IRC foi negada.	3
Sessão IRC em andamento	Indica que uma sessão IRC está em andamento.	1
Sessão IEC 104 aberta	Indica que uma sessão IEC 104 foi estabelecida.	1
Sessão IEC 104 fechada	Indica que uma sessão IEC 104 foi fechado.	1
Reconfigurar sessão IEC 104	Indica que uma sessão IEC 104 foi reconfigurada.	3
Sessão IEC 104 finalizada	Indica que uma sessão IEC 104 foi finalizado.	3
Sessão IEC 104 negada	Indica que uma sessão IEC 104 foi negada.	3
Sessão IEC 104 em andamento	Indica que uma sessão IEC 104 está em andamento.	1
Sessão Ident em aberto	Indica que uma sessão de protocolo de identidade de cliente (Ident) foi estabelecida.	1
Sessão Ident fechada	Indica que uma sessão Ident foi fechada.	1
Reconfigurar sessão Ident	Indica que uma sessão Ident foi reconfigurada	3
Sessão Ident finalizada	Indica que uma sessão Ident foi finalizada.	3
Sessão Ident negada	Indica que uma sessão Ident foi negada.	3
Sessão Ident em andamento.	Indica que uma sessão Ident está em andamento.	1
Sessão ICCP aberta	Indica que uma sessão Inter-Centro de Controle de Comunicações Protocol (ICCP) foi estabelecida.	1
Sessão ICCP fechada	Indica que uma sessão ICCP foi fechada.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Reconfigurar Sessão ICCP	Indica que uma sessão ICCP foi reconfigurada.	3
Sessão ICCP finalizada	Indica que uma sessão ICCP foi finalizada.	3
Sessão ICCP negada	Indica que uma sessão ICCP foi negada.	3
Sessão ICCP em andamento	Indica que uma sessão ICCP está em andamento.	1
GroupWiseSessão Aberta	Indica que uma sessão GroupWise foi estabelecida.	1
GroupWiseSessão fechada	Indica que uma sessão GroupWise foi encerrada.	1
GroupWiseSessão reconfigurada	Indica que uma sessão GroupWisefoi redefinida.	3
GroupWiseSessão finalizada	Indica que uma sessão GroupWisefoi encerrada.	3
GroupWiseSessão negada	Indica que uma sessão foi GroupWise negada.	3
GroupWiseSessão em andamento	Indica que uma sessão GroupWise está em andamento.	1
Sessão Gopher aberta	Indica que uma sessão Gopher foi estabelecida.	1
Sessão Gopher fechada	Indica que uma sessão Gopher foi fechada.	1
Reconfigurar sessão Gopher	Indica que uma sessão Gopher foi redefinido.	3
Sessão Gopher finalizada	Indica que uma sessão Gopher foi finalizada.	3
Sessão Gopher negada	Indica que uma sessão Gopher foi negada.	3
Sessão Gopher em andamento	Indica que uma sessão Gopher está em andamento.	1
Sessão GIOP em aberto	Indica que uma sessão GIOP (General Inter-ORB Protocol) foi estabelecida.	1
Sessão GIOP encerrada	Indica que uma sessão GIOP foi encerrada.	1
Sessão GIOP reconfigurada	Indica que uma sessão GIOP foi reconfigurada	3
Sessão GIOP finalizada	Indica que uma sessão GIOP foi finalizado.	3
Sessão GIOP negada	Indica que uma sessão GIOP foi negada.	3
Sessão GIOP em andamento	Indica que uma sessão GIOP está em andamento.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão finger aberta	Indica que um Dedo sessão foi estabelecida.	1
Sessão Finger fechado	Indica que uma sessão Finger foi fechada.	1
Reconfigurar Sessão Finger	Indica que uma sessão Finger foi reconfigurada.	3
Sessão finger encerrada	Indica que uma sessão finger foi finalizada.	3
Sessão Finger negada	Indica que uma sessão finger foi negado.	3
Sessão finger em andamento	Indica que a sessão finger está em andamento.	1
Sessão Echo Aberta	Indica que uma sessão echo foi estabelecida.	1
Sessão Echo fechada	Indica que uma sessão Echo foi fechada.	1
Sessão Echo negada	Indica que uma sessão echo foi negada.	3
Sessão Eco em andamento	Indica que uma sessão de eco está em andamento.	1
Sessão Net remota aberta	Indica que uma sessão .NET remoto foi reconfigurada.	1
Sessão NET remota aberta	Indica que uma sessão NET remota foi fechada.	1
Sessão .NET remota fechada	Indica que uma sessão .NET remota foi reconfigurada.	3
Sessão.NET Remota encerrada.	Indica que uma sessão .NET remoto foi encerrada.	3
Sessão remota .NET negada	Indica que uma sessão .NET remota foi negada.	3
Sessão .NET remota em andamento	Indica que uma sessão .NET remota está em andamento.	1
DNP3 Sessão Aberta	Indica que uma sessão Network Distribuído Proctologic (DNP3) foi estabelecida.	1
Sessão DNP3 encerrada	Indica que uma sessão DNP3 foi encerrada.	1
Sessão DNP3 reconfigurada	Indica que uma sessão DNP3 foi reconfigurada.	3
DNP3 Sessão finalizada	Indica que uma sessão DNP3 foi finalizado.	3
Sessão DNP3 Negada	Indica que uma sessão DNP3 foi negada.	3
Sessão DNP3 Em Andamento	Indica que uma sessão DNP3 está em andamento.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão descartar aberta	Indica que uma sessão Descartar foi estabelecida.	1
Sessão Descartar fechada	Indica que uma sessão Descartar foi fechada.	1
Reconfigurar sessão descartar	Indica que uma sessão descartar foi redefinida.	3
Sessaão descartar finalizada	Indica que uma sessão descartar foi finalizada.	3
Sessão Descartar negada	Indica que uma sessão Descartar foi negado.	3
Sessão Descartar em andamento	Indica que uma sessão Descartar está em andamento.	1
Sessão DHCP aberta	Indica que um Protocolo de Configuração de Host Dinâmico (DHCP) foi estabelecido.	1
Sessão DHCP encerrada	Indica que uma sessão DHCP foi fechada.	1
Sessão DHCP negada.	Indica que uma sessão DHCP foi negada.	3
Sessão DHCP em andamento	Indica que uma sessão do DHCP está em andamento.	1
DHCP OK	Indica que um lease DHCP foi obtido com êxito	1
Falha DHCP	Indica que um lease DHCP não pode ser obtido.	3
Sessão Aberta CVS	Indica que um Concurrent Versions System (CVS) sessão foi estabelecida.	1
Sessão CVS fechada	Indica que uma sessão do CVS foi fechado.	1
Sessão Reconfigurar CVS	Indica que uma sessão foi redefinido CVS.	3
Sessão Terminada CVS	Indica que uma sessão CVS era finalizada.	3
Sessão Negado CVS	Indica que uma sessão do CVS foi negado.	3
Sessão CVS em andamento	Indica que uma sessão do CVS está em andamento.	1
Sessão Aberta CUPS	Indica que uma sessão comum UNIX Printing System (CUPS) foi estabelecida.	1
Sessão CUPS encerradca	Indica que uma sessão CUPS foi fechado.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Reconfigurar sessão CUPS	Indica que uma sessão CUPS foi redefinido.	3
Sessão CUPS finalizada	Indica que uma sessão CUPS foi finalizada.	3
Sessão CUPS negada	Indica que uma sessão CUPS foi negada.	3
Sessão CUPS em andamento	Indica que uma sessão CUPS está em andamento.	1
Sessão Chargen inicidada	Indica que a sessão Gerador de Caracteres (Chargen) foi iniciado.	1
Sessão Chargen fechada	Indica que uma sessão Chargen foi fechado.	1
Reconfigurar Chargen Sessão	Indica que uma sessão foi redefinido Chargen.	3
Sessão crhargem Terminada	Indica que uma sessão Chargen foi finalizada.	3
Sessão Negado Chargen	Indica que uma sessão Chargen foi negado.	3
Sessão Chargen	Indica que uma sessão Chargen está em andamento.	1
Diversa VPN	Indica que uma sessão de VPN mista foi detectada	1
Sessão Iniciada DAP	Indica que uma sessão DAP foi estabelecida.	1
Sessão Encerrada DAP	Indica que uma sessão DAP foi encerrada.	1
Sessão DAP Negado	Indica que uma sessão DAP foi negado.	3
Status da Sessão do DAP	Indica que um pedido de status da sessão DAP foi feita.	1
Sessão DAP em Andamento	Indica que uma sessão DAP está em andamento.	1
Falha de Autenticação DAP	Indica que um DAP autenticação falhou.	4
Autenticação Bem-sucedido DAP	Indica que a autenticação bem-sucedida. DAP	1
Sessão Iniciada TOR	Indica que uma sessão TOR foi estabelecida.	1
Sessão TOR fechada	Indica que uma sessão TOR foi fechado.	1
Reconfigurar Sessão TOR	Indica que uma sessão TOR foi redefinido.	3
Sessão Terminada TOR	Indica que uma sessão TOR foi finalizado.	3

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão TOR negada.	Indica que uma sessão TOR foi negado.	3
Sessão TOR Em Andamento	Indica que uma sessão TOR está em andamento.	1
Jogo de Sessão Iniciada	Indica que uma sessão jogo foi iniciado.	1
Jogo de Sessão fechada	Indica que uma sessão jogo foi fechado.	1
Sessão Reconfigurar Jogo	Indica que um jogo de sessão foi redefinido.	3
Sessão Terminada Jogo	Indica que uma sessão game foi finalizado.	3
Jogo Sessão Negado	Indica que um jogo de sessão foi negado.	3
Em Andamento Sessão Jogo	Indica que uma sessão jogo está em andamento.	1
Tentativa de Login de Administrador	Indica que uma tentativa de efetuar login como um usuário administrativo foi detectado.	2
Tentativa de Login do Usuário	Indica que uma tentativa de efetuar login como um usuário não administrativo foi detectado.	2
Servidor do Cliente	Indica atividade cliente / servidor.	1
Entrega de Conteúdo	Indica atividade de entrega de conteúdo.	1
Transferência de Dados	Indica uma transferência de dados.	3
Armazenamento de Dados	Indica atividade de data warehousing.	3
Serviços de Diretório	Indica fluxo de atividade.	2
Arquivo Imprimir	Indica atividade de impressão do arquivo.	1
Transferência de Arquivos	Indica transferência de arquivos.	2
Jogos	Indica atividade de jogo.	4
Saúde	Indica atividade de saúde.	1
Sistema Interna	Indica atividade do sistema interno.	1
protocolo da Internet	Indica atividade de protocolo Internet	1
Preexistente	Indica atividade de saúde.	1
Enviar Correio	Indica atividade de correio.	1

Tabela 112. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Div.	Indica atividade mista.	2
Multimídia	Indica atividade multimídia.	2
Gerenciamento de Rede	Indica atividade de gerenciamento de rede.	
P2P	Indica-to-Peer (P2P) a atividade.	4
Acesso Remoto	Indica atividade de Acesso Remoto.	3
Protocolos Routing	Indica atividade de roteamento de protocolo.	1
Protocolos de Segurança	Indica atividade de protocolo de segurança.	2
Fluxo	Indica fluxo de atividade.	2
Protocolo desconhecido	Indica atividade incomum protocolo.	3
VoIP	Indica atividade VoIP.	1
Web	Indica atividade da web.	1
ICMP	Indica atividade ICMP	1

Auditoria

A categoria auditoria contêm eventos que estão relacionados a atividade de auditoria, tais como emails ou atividades FTP.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de auditoria.

Tabela 113. categorias de baixo nível e níveis de severidade para a categoria de auditoria

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento de Auditoria Geral	Indica que um evento de auditoria general foi iniciado.	1
O de execução	Indica que uma tarefa de auditoria interna foi executado.	1
Cópia em massa	Indica que uma cópia em massa foi detectada.	1
Dados do Dump	Indica que um dump de dados foi detectado.	1
Importar Dados	Indica que uma importação de dados foi detectada.	1
Seleção de Dados	Indica que um processo de seleção de dados foi detectado.	1

Tabela 113. categorias de baixo nível e níveis de severidade para a categoria de auditoria (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Truncamento de Dados	Indica que o processo truncamento de dados foi detectado.	1
Atualização de Dados	Indica que o processo de atualização de dados foi detectado.	1
Execução do procedimento / disparador	Indica que o procedimento ou disparo de execução do banco de dados foi detectado.	1
Alteração de Esquema	Indica que o esquema para uma execução de procedimento ou de disparo foi alterada.	1

Risco

A categoria de risco contém eventos que estão relacionados a IBM Security QRadar Risk Manager.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de risco.

Tabela 114. categorias de baixo nível e níveis de severidade para a categoria de auditoria

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Exposição de Política	Indica que uma exposição política foi detectada.	5
Violação de Conformidade	Indica que uma violação de conformidade foi detectado.	5
Exposição de vulnerabilidades	Indica que a rede ou dispositivo tiveram uma vulnerabilidade exposta.	9
Vulnerabilidade de Acesso Remoto	Indica que a rede ou dispositivo têm uma vulnerabilidade de acesso remoto.	9
Vulnerabilidade de Acesso Local	Indica que a rede ou dispositivo têm vulnerabilidade de acesso local.	7
Asbra o acesso wireless	Indica que a rede ou dispositivo abriram o acesso wireless.	5
Criptografia fraca	Indica que o host ou dispositivo tem a criptografia fraca.	5

Tabela 114. categorias de baixo nível e níveis de severidade para a categoria de auditoria (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Transferência de dados não criptografada	Indica que um host ou dispositivo é transmissão de dados que não está criptografada.	3
Armazenamento de dados não criptografado	Indica que o armazém de dados não está criptografada.	3
Incompatibilidade de Regra-Configurada	Indica que uma regra não está configurada corretamente.	3
Incompatibilidade de Dispositivo-Configurado	Indica que um dispositivo na rede não está configurado corretamente.	3
Os Hosts-Configurados	Indica que um host de rede não está sendo configurado corretamente.	3
Possível perda de dados	Indica que a possibilidade de perda de dados foi detectado.	5
Autenticação fraca	Indica que um host ou dispositivo está suscetível a fraude.	5
Sem senha	Indica que não existe senha.	7
Fraude	Indica que um host ou dispositivo está suscetível a fraude.	7
Possívesis destinos DoS	Indica um host ou dispositivo é um destino possível DoS.	3
Possíveis fraquezas DoS	Indica um host ou dispositivo tiver um ponto fraco DoS possível.	3
Perda de Confidencialidade	Indica que uma perda de confidencialidade foi detectado.	5
Política monitor de pontuação de risco de pontuação.	Indica que uma acumulação pontuação de risco da política de monitor foi detectado.	1

Gerenciador de risco de auditoria

A categoria de risco contém eventos que estão relacionados a IBM Security QRadar Risk Manager eventos de auditoria.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de gravidade associado para a categoria de auditoria Risk Manager.

Tabela 115. categorias de baixo nível e níveis de gravidade para a categoria de auditoria Risk Manager

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Política de Monitor	Indica que um monitor de política foi modificada.	3
Topologia	Indica que uma topologia foi modificado.	3
Simulações	Indica que uma topologia foi modificado.	3
Administração	Indica que as alterações administrativas foram feitas.	3

Controle

A categoria de controle contém eventos que estão relacionados ao seu hardware do sistema.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associado para a categoria de controle.

Tabela 116. categorias de baixo nível e níveis de severidade para a categoria de controle

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Leitura de Dispositivo	Indica que um dispositivo foi lido.	1
dispositivo de comunicação	Indica comunicação com um dispositivo.	1
Dispositivo de auditoria	Indica que um dispositivo de auditoria ocorreu.	1
Evento do Dispositivo	Indica que um evento de dispositivo.	1
Dispositivo Ping	Indica uma ação de ping para um dispositivo.	1
Configuração de Dispositivo	Indica que um dispositivo foi lido.	1
Rota de dispositivo	Indica que uma ação rotear dispositivo ocorreu.	1
Importação de dispositivo	Indica que uma importação de dispositivo ocorreu.	1
Informações sobre o Dispositivo	Indica que uma ação de informações sobre o dispositivo.	1
Aviso de Dispositivo	Indica que um aviso foi gerado em um dispositivo.	1
Erro do Dispositivo	Indica que um erro foi gerado em um dispositivo.	1
Retransmissão de evento	Indica um evento de retransmissão.	1

Tabela 116. categorias de baixo nível e níveis de severidade para a categoria de controle (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento NIC	Indica um potencial Interface (NIC) vulnerabilidade.	1
Evento UIQ	Indica um evento em um dispositivo móvel.	1
Eventos IMU	Indica um evento em um unidade de gerenciamento integrado (Unidade de Gerenciamento IMU).	1
Evento Faturamento	Indica um evento faturamento.	1
Evento DBMS	Indica um evento no Sistema de Gerenciamento de Banco de Dados (DBMS).	1
Importar evento	Indica que uma importação.	1
Local Importar	Indica que um local de importação.	1
Importação da Rota	Indica que uma importação de rota.	1
Exportar Evento	Indica que uma exportação ocorreu.	1
Sinal Remote	Indica um sinal remoto.	1
Status do Gateway	Indica o status do gateway.	1
Evento da Tarefa	Indica que uma tarefa ocorreu.	1
Evento de Segurança	Indica que um evento de segurança ocorreu.	1
Dispositivo de Detecção de violação	Indica que o sistema detectou uma ação de violação.	1
Evento de Tempo	Indica que um evento de tempo.	1
Comportamento suspeito	Indica que ocorreu um comportamento suspeito.	1
Interrupções de Energia	Indica que uma interrupção de disponibilidade de energia ocorreu.	1
Recuperação de Energia	Indica que a energia foi restaurada.	1
Pulsações	Indica que um ping de pulsação ocorreu.	1
Conexão Remota de Eventos	Indica uma conexão remota com o sistema.	1

Gerenciadores de perfis ativos

A categoria gerenciador de perfil ativo contêm eventos que estão relacionados aos gerenciadores de perfis ativos.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados ao recurso categoria do gerenciador de perfis.

Tabela 117. Categorias de baixo nível e níveis de severidade para a categoria do gerenciador de perfis

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ativo Criado	Indica que um recurso foi criado.	1
Ativo Atualizado	Indica que um ativo foi atualizado.	1
Ativo Observado	Indica que um ativo foi observado.	1
Ativo Movido	Indica que um ativo foi movido.	1
Ativo Excluído	Indica que um recurso foi excluído.	1
Ativo do host de acesso limpo	Indica que um ativo foi limpo.	1
Nome Ativo Criado	Indica que um nome de host foi criado.	1
Nome do Ativo Atualizado	Indica que um nome do host foi atualizado.	1
Nome Ativo Observado	Indica que um nome de host foi observado.	1
Nome do Ativo Movido	Indica que um nome de host foi movido.	1
Ativo do Host Excluído	Indica que um nome de host foi excluído.	1
Porta de ativos limpa	Indica que uma porta foi limpa.	1
Ativo de porta criada	Indica que uma porta foi criada.	1
Ativo de porta atualizada	Indica que uma porta foi atualizada.	1
Ativo de porta observada	Indica que uma porta foi observada.	1
Ativo porta movida	Indica que uma porta foi movida.	1
Ativo porta excluída	Indica que uma porta foi excluída.	1
Ativo de instância de vulnerabilidade limpa	Indica que uma instância da vulnerabilidade foi limpa.	1
Ativo de instância de vulnerabilidade criado	Indica que uma instância da vulnerabilidade foi criada.	1

Tabela 117. Categorias de baixo nível e níveis de severidade para a categoria do gerenciador de perfis (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ativo de instância de vulnerabilidade atualizado	Indica que um ativo de instância de vulnerabilidade afoi atualizado	1
Ativo de instância de vulnerabilidade observado	Indica que um ativo de instância de vulnerabilidade foi observado.	1
Ativo de instância de vulnerabilidade movido	Indica que um ativo de instância de vulnerabilidade foi movido	1
Ativo de instância de vulnerabilidade excluída	Indica que uma instância da vulnerabilidade foi excluída.	1
Ativo OS limpos	Indica que um sistema operacional foi limpo.	1
Ativo OS Criado	Indica que um sistema operacional foi criado.	1
Ativo propriedade atualizado	Indica que um sistema operacional foi atualizado.	1
Ativo OS observado	Indica que um sistema operacional foi observado.	1
Ativo OS movido	Indica que um sistema operacional foi movido.	1
Ativo OS excluído	Indica que um sistema operacional foi excluído.	1
Ativo de Propriedade Limpas	Indica que uma propriedade foi limpa.	1
Ativo de propriedade criado	Indica que uma propriedade foi criada.	1
Ativo de propriedades atualizado	Indica que uma propriedade foi atualizado.	1
Ativo de propriedade observado	Indica que uma propriedade foi observado.	1
Ativo de propriedade movido	Indica que uma propriedade foi movida.	1
Ativo de propriedade excluído	Indica que uma propriedade foi movida.	1
Endereço IP ativo limpo	Indica que um endereço IP foi limpo.	1
Endereço IP Ativo Criado	Indica que um endereço IP foi criado.	1
Endereço IP Ativo Atualizado	Indica que um endereço IP foi atualizado.	1
Endereço IP Ativo Observado	Indica que um endereço IP foi observado.	1
Endereço IP Ativo Movido	Indica que um endereço IP foi movido.	1

Tabela 117. Categorias de baixo nível e níveis de severidade para a categoria do gerenciador de perfis (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Endereço IP Ativo Excluído	Indica que um endereço IP foi excluído.	1
Ativo de Propriedade Limpas	Indica que uma interface foi limpa.	1
Ativo de interface criado	Indica que uma interface foi criada.	1
Ativo de interface atualizado	Indica que uma interface foi atualizado.	1
Ativo de interface Observado	Indica que uma interface foi observado.	1
Ativode interface Movido	Indica que uma interface foi movido.	1
Ativo de Interface Mesclados	Indica que uma interface foi mesclada.	1
Ativo de Interface Excluído	Indica que uma interface foi excluída.	1
Usuário do ativo limpo	Indica que um usuário foi limpo.	1
Usuário do ativo observado	Indica que um usuário foi observado.	1
Usuário de ativo movido	Indica que um usuário foi movido.	1
Usuário do Ativo Excluído	Indica que um usuário foi excluído.	1
Ativo de política digitalizada limpo	Indica que um ativo de política digitalizada foi limpa.	1
Ativo de política digitalizada observado	Indica que um ativo de política digitalizado foi observado.	1
Ativo de política digitalizada movido	Indica que um ativo de política digitalizado foi limpo.	1
Política de ativos digitalizados excluídos	Indica que uma política de ativos digitalizados foi excluída.	1
Aplicações de ativos Windows limpas	Indica que um aplicativo Windows foi limpo.	1
Ativo Aplicativo Windows Observado	Indica que um aplicativoWindows foi observado.	1
Aplicativo ativo em Windows movido	Indica que um aplicativo Windows foi movido.	1
Ativo aplicativo Windows excluído.	Indica que um aplicativoWindows foi excluído.	1

Tabela 117. Categorias de baixo nível e níveis de severidade para a categoria do gerenciador de perfis (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ativos de serviços digitalizados limpos	Indica que ativos de serviços digitalizados foram limpos.	1
Ativos de serviços digitalizados observados	Indica que um serviço digitalizadoo foi movido.	1
Ativos de serviços digitalizados movido	Indica que um ativo de serviços digitalizados foi movido.	1
Ativos de serviços digitalizados excluídos	Indica que Ativos de serviços digitalizados foram excluídos.	1
Caminho de ativos Windows limpos.	Indica que uma correção Windows foi limpa.	1
Ativo Windows Patch Observado	Indica que um Windows correção foi observado.	1
Caminho de ativo Windows movido	Indica que ua correção Windows foi movido.	1
Patch de Ativo Windows Excluído.	Indica que uma correção Windows excluída.	1
Ativo de caminho UNIXLimpas	Indica que uma correção foi limpo UNIX.	1
Ativo UNIX Patch Observado	Indica que uma correção UNIX foi observada.	1
Asset UNIX Patch Moved	Indica que um UNIX correção foi movido.	1
Ativo de correção UNIX excluído	Indica que uma correção UNIX foi excluído.	1
Ativo correção de varredura limpo	Indica que o ativo correção de varredura foi limpo.	1
Ativo correção de varredura criado	Indica que o ativo correção de varredura foi observado.	1
Ativo correção de varredura movido	Indica que uma varredura de correção foi movida.	1
Ativo correção de varredura excluído	Indica que uma varredura de correção foi excluída.	1
Ativo correção de varredura limpo	Indica que um ativo de correção de varredura foi limpo.	1
Ativo correção de varredura criado	Indica que um ativo de correção de varredura foi limpo.	1
Ativo correção de varredura movido	Indica que uma varredura de correção foi movida.	1
Varredura de Porta ativa Excluída	Indica que uma varredura de correção foi excluída.	1
O Application Client Limpas	Indica que um aplicativo cliente foi limpo.	1

Tabela 117. Categorias de baixo nível e níveis de severidade para a categoria do gerenciador de perfis (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
O Aplicativo Cliente Observado	Indica que um aplicativo cliente foi observado.	1
Ativo Movido Application Client	Indica que um aplicativo cliente foi movido.	1
O Aplicativo Cliente Excluído	Indica que um aplicativo cliente foi excluído.	1
Ativo Observado de Varredura de Correção	Indica que uma varredura de correção foi observado.	1
Ativo Criado de Varredura de Porta	Indica que uma varredura de correção foi observado.	1

Capítulo 24. Portas Usadas pelo QRadar

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

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

Portas e Iptables

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

Comunicação do SSH na Porta 22

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

Portas QRadar

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

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

Tabela 118. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes

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

Tabela 118. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

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

Tabela 118. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

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

Tabela 118. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

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

Tabela 118. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Direção	Requisito
762	Daemon de montagem Network File System (NFS) (mountd)	TCP/UDP	Conexões entre o QRadar Console e o servidor NFS	A montagem Daemon de Network File System (NFS), no qual o processo solicita a montagem de um arquivo de sistema em uma locação específica.
1514	Syslog-ng	TCP/UDP	Conexão entre o componente local do Coletor de eventos e componente local do Processador de eventos para o daemon syslog-ng para criação de log	porta de log interno para syslog-ng
2049	NFS	TCP	Conexões entre o QRadar Console e o servidor NFS	O protocolo do Sistema de Arquivos de Rede (NFS) para compartilhar arquivos ou dados entre componentes
2055	Dados do NetFlow	UDP	Do gerenciador de interfaces na fonte de fluxo (normalmente um roteador) ao QRadar QFlow Collector.	Datagrama NetFlow a partir de componentes, como roteadores
3389	Remote Desktop Protocol (RDP) e Ethernet sobre USB estão ativados	TCP/UDP		Se o sistema operacional Windows estiver configurado para suportar RDP e o Ethernet sobre USB, um usuário poderá iniciar uma sessão para o servidor por meio da rede de gerenciamento. Isso significa que a porta padrão para RDP, 3389, deve ser aberta.
3900	Porta de presença remota do Módulo de Gerenciamento Integrado	TCP/UDP		Utilize esta porta para interagir com o console do QRadar por meio do Módulo de Gerenciamento Integrado.
4333	Porta de redirecionamento	TCP		Esta porta é designada como uma porta de redirecionamento para pedidos de Protocolo de Resolução de Endereço (ARP) em QRadar resolução de ofensa.
5432	Postgres	TCP	Comunicação para o host gerenciado que é utilizado para acessar a instância do banco de dados local	Obrigatório para fornecimento hosts gerenciados na guia **Admin**

Tabela 118. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Direção	Requisito
6543	Pulsação de alta disponibilidade	TCP/UDP	Bidirecional entre o host secundário e o host primário em um cluster de HA	ping de pulsação a partir de um host secundário para um host principal em um cluster de HA para detectar falha de hardware ou de rede
7676, 7677, e quatro portas aleatoria-mente limitadas acima de 32000.	Conexões do sistema de mensagens (IMQ)	TCP	Fila de mensagens de comunicações entre os componentes do em um host gerenciado.	Fila de mensagens do broker para comunicações entre os componentes em um host gerenciado As portas 7676 e 7677 são portas TCP estáticas e quatro conexões extras são criadas em portas aleatórias.
7777 – 7782, 7790, 7791	Porta de servidor JMX	TCP	Comunicações internas, essas portas não estão disponíveis externamente	Monitoramento do servidor JMX (Mbean) para ECS, contexto de host, Tomcat, VIS, relatório, ariel e serviços de acumulador **Nota:** Essas portas são utilizadas pelo Suporte do QRadar.
7789	Distributed Replicated Block Device de alta disponibilidade	TCP/UDP	Bidirecional entre o host secundário e o host primário em um cluster de HA	O Distributed Replicated Block Device é usado para manter unidades sincronizadas entre os hosts primário e secundário em configurações de HA
7800	Apache Tomcat	TCP	A partir do Coletor de eventos para o QRadar Console	Tempo real (fluxo) para eventos
7801	Apache Tomcat	TCP	A partir do Coletor de eventos para o QRadar Console	Tempo real (fluxo) para fluxos
7803	Apache Tomcat	TCP	A partir do Coletor de eventos para o QRadar Console	Porta do mecanismo de detecção de anomalias
8000	Event Collection Service (ECS)	TCP	A partir do Coletor de eventos para o QRadar Console	Porta de atendimento para Event Collection Service (ECS) específico.
8001	Porta do daemon SNMP	UDP	Sistemas externos SNMP que solicitam informações de trap SNMP do QRadar Console	Porta de atendimento UDP para solicitações de dados SNMP externas.
8005	Apache Tomcat	TCP	Nenhum	Uma porta local que não é utilizada pelo QRadar
8009	Apache Tomcat	TCP	A partir do processo do daemon de HTTP (HTTPd) para o Tomcat	conector do Tomcat, onde o pedido é utilizado e um proxy para o serviço da Web

Tabela 118. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

Porta	Descrição	Protocolo	Direção	Requisito
8080	Apache Tomcat	TCP	A partir do processo do daemon de HTTP (HTTPd) para o Tomcat	conector do Tomcat, onde o pedido é utilizado e um proxy para o serviço da Web.
9995	Dados do NetFlow	UDP	A partir da interface de gerenciamento na fonte de fluxo (normalmente um roteador) para o Coletor de QFlow	Datagrama NetFlow a partir de componentes, como roteadores
10000	Interface de administração do sistema baseada na web do QRadar	TCP/UDP	sistemas de desktop do usuário para todos os hosts QRadar	Mudanças do servidor, tais como a senha raiz de hosts e acesso ao firewall
23111	Servidor da web SOAP	TCP		porta do servidor da Web SOAP para o serviço de coleta de eventos (ECS)
23333	Fibre Channel Emulex	TCP	Sistemas de desktop do usuário que se conectam aos dispositivos QRadar com uma placa Fibre Channel	serviço Fibre Channel Remote Management HBAnywhere Emulex (elxmgmt)
32004	Encaminhamento de evento normalizado	TCP	Bidirecional entre componentes do QRadar	Dados do evento normalizado que são comunicados a partir de uma origem externa ou entre QRadar Event Collectors
32005	Fluxo de dados	TCP	Bidirecional entre componentes do QRadar	Porta de comunicação do fluxo de dados entre QRadar Event Collectors quando em hosts gerenciados separados
32006	Consultas do Ariel	TCP	Bidirecional entre componentes do QRadar	Porta de comunicação entre o servidor proxy Ariel e o servidor de consulta do Ariel
32009	Dados de identificação	TCP	Bidirecional entre componentes do QRadar	Dados de identificação que são comunicados entre o serviço de informações de vulnerabilidade (VIS) passivo e o Event Collection Service (ECS)
32010	Porta de origem de recebimento do fluxo	TCP	Bidirecional entre componentes do QRadar	Porta de atendimento do fluxo para coletar dados do QRadar QFlow Collectors
32011	Porta de atendimento do Ariel	TCP	Bidirecional entre componentes do QRadar	A porta de atendimento do Ariel para procuras de banco de dados, informações de progresso e outros comandos associados

Tabela 118. Portas de Atendimento que são Utilizadas pelo QRadar, Serviços e Componentes (continuação)

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

Procurando Portas em Uso por QRadar

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

Procedimento

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

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

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

   Exemplos:

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

Visualizando Associações de Porta do IMQ

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

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

Procedimento

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

   ```
   telnet localhost 7676
   ```

3. Se nenhuma informação for exibida, pressione a tecla Enter para fechar a conexão.

Capítulo 25. Servidores públicos do QRadar

Para poder fornecer as informações de segurança mais atuais, o IBM Security QRadar requer acesso a vários servidores públicos e feeds RSS.

Servidores públicos

Tabela 119. Servidores públicos que o QRadar deve acessar. Esta tabela lista descrições para os endereços IP ou nomes de host acessados pelo QRadar.

Endereço IP ou nome do host	Descrição
194.153.113.31	Scanner DMZ do IBM Security QRadar Vulnerability Manager
194.153.113.32	Scanner DMZ do QRadar Vulnerability Manager
qmmunity.q1labs.com	Servidor de atualização automática do QRadar
www.iss.net	Item do painel do Centro de Informações de Ameaças do X-Force
update.xforce-security.com	Servidor de atualização do Feed de Ameaças do X-Force
license.xforce-security.com	Servidor de licenciamento do Feed de Ameaças do X-Force

Feeds RSS para produtos QRadar

Tabela 120. Feeds RSS. A lista a seguir descreve os requisitos para os feeds RSS utilizados pelo QRadar. Copie as URLs em um editor de texto e remova as quebras de página antes de colá-las em um navegador.

Título	URL	Requisitos
Inteligência de Segurança	http://feeds.feedburner.com/SecurityIntelligence	QRadar e uma conexão de Internet
Vulnerabilidades/Ameaças da Inteligência de Segurança	http://securityintelligence.com/topics/vulnerabilities-threats/feed	QRadar e uma conexão de Internet
Minhas Notificações IBM	http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid= feeder.create_feed&feeder.feedtype=RSS&feeder.uid=270006EH0R&feeder.subscrid= S14b5f284d32&feeder.subdefkey=swgother&feeder.maxfeed=25	QRadar e uma conexão de Internet
Notícias de Segurança	http://*IP_address_of_QVM_processor* :8844/rss/research/news.rss	Implementação do processador do IBM Security QRadar Vulnerability Manager

Tabela 120. Feeds RSS (continuação). A lista a seguir descreve os requisitos para os feeds RSS utilizados pelo QRadar. Copie as URLs em um editor de texto e remova as quebras de página antes de colá-las em um navegador.

Título	**URL**	**Requisitos**
Conselhos sobre Segurança	http://*IP_address_of_QVM_processor* :8844/rss/research/advisories.rss	Implementação do processador do QRadar Vulnerability Manager
Vulnerabilidades Mais Recentes Publicadas	http://*IP_address_of_QVM_processor* :8844/rss/research/vulnerabilities.rss	Implementação do processador do QRadar Vulnerability Manager
Varreduras Concluídas	http://*IP_address_of_QVM_processor* :8844/rss/scanresults/completedScans.rss	Implementação do processador do QRadar Vulnerability Manager
Varreduras em Andamento	http://*IP_address_of_QVM_processor* :8844/rss/scanresults/runningScans.rss	Implementação do processador do QRadar Vulnerability Manager

Avisos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a 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).

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.

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

Considerações sobre 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, ajustar as interações com o usuário final ou para outros propósitos. Em muitas casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoalmente identificáveis. Se esta Oferta de Software usar cookies para coletar informações pessoais identificáveis, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

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 de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de privacidade da IBM em http://www.ibm.com/privacy e a Declaração de privacidade online da IBM em http://www.ibm.com/privacy/details, a seção intitulada “Cookies, web beacons e

outras tecnologias" e a "Declaração de privacidade de software como serviço e de produtos de software IBM" em http://www.ibm.com/software/info/product-privacy.

Glossário

Este glossário fornece termos e definições para software e produtos [nome do produto].

As referências cruzadas a seguir são usadas neste glossário:

- *Consulte* o encaminha de um termo não preferencial para um termo preferencial ou de forma de abreviação para uma forma integral.
- *Consulte também* o encaminha para um termo relacionado ou contrastante.

Para outros termos e definições adicionais, veja o website IBM Terminology (abre em uma nova janela).

A

acumulador
Um registro no qual um operando de uma operação pode ser armazenada e, subsequentemente, substituído pelo resultado dessa operação.

agregação de link
O agrupamento de placas da interface da rede física, tal como cabos ou portas, em uma única interface de rede lógica. A agregação de link é usada para aumentar a largura da banda e a disponibilidade de rede.

Alta disponibilidade (HA)
Pertencente a um sistema em cluster, que é reconfigurado quando nó ou falhas daemon ocorrem, para que as cargas de trabalho possam ser redistribuídos para os nós restantes no cluster.

anomalia
Um desvio do comportamento esperado da rede.

ARP Veja Protocolo de Resolução de Endereço.

ARP (Address Resolution Protocol)
Um protocolo que mapeia dinamicamente um endereço de IP para um adaptador de rede, mapeia em uma rede local.

arquivo-chave
Em segurança de computador, um arquivo que contém chaves públicas, chaves privadas, raízes confiáveis e certificados.

arquivo de armazenamento confiável
Um arquivo de banco de dados de chave que contém as chaves públicas para uma entidade confiável.

assinatura de aplicativo
Um conjunto exclusivo de características que são derivados pela análise de carga útil do pacote e, em seguida, utilizado para identificar um aplicativo específico.

ativo Um objeto gerenciável que é implementado ou que se pretende que seja implementado em um ambiente operacional.

B

burst Um aumento agudo e repentino na taxa dos eventos ou fluxos recebidos de forma que o limite licenciado da taxa de fluxo ou evento é excedido.

C

camada de rede
Na arquitetura de OSI, a camada que fornece serviços para estabelecer um caminho entre os sistemas abertos com uma qualidade de serviço previsíveis.

captura de conteúdo
Um processo que captura um valor configurável de carga útil e em seguida, armazena os dados em um log do fluxo.

CIDR Consulte Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
Um método para incluir a classe C de endereços IP (Internet Protocol). Os endereços são oferecidos aos Provedores de Serviço Internet (ISPs) para utilização

de seus clientes. Endereços CIDR reduzem o tamanho das tabelas de roteamento e tornam disponíveis mais endereços IP nas organizações.

cliente
Um programa ou computador de software que atende os serviços a partir de um servidor.

Cluster HA
Uma configuração de alta disponibilidade que consiste em um servidor principal e um servidor secundário.

compartilhamento administrativo
Um recurso de rede que fica oculto dos usuários sem privilégios administrativos. Os compartilhamentos administrativos fornecem aos administradores acesso a todos os recursos em um sistema de rede.

comportamento
Os efeitos observados em uma operação ou evento, incluindo os resultados.

conjunto de referência
Uma lista de elementos únicos que são derivados de eventos ou fluxos em uma rede. Por exemplo, uma lista de endereços IP de uma lista de nomes de usuários.

console
Uma estção de exibição, da qual um operador pode controlar e observar um sistema de produção.

contexto do host
Um serviço que monitora os componentes para assegurar que cada componente está operando conforme o esperado.

conversão de endereço de rede (NAT)
Em um firewall, a conversão de segurança de Internet Protocol (IP) endereça para endereços registrados externos. Isto permite comunicações com redes externas, mas mascara os endereços IP usados dentro do firewall.

credencial
Um conjunto de informações que é concedida a um usuário ou certos processos de direitos de acesso.

credibilidade
Uma classificação numérica entre 0-10 que é utilizada para determinar a integridade de um evento ou uma ofensa. Credibilidade aumenta à medida que várias fontes relatam o mesmo evento ou ofensa.

criptografia
Na segurança do computador, o processo de transformação de dados em uma forma ininteligível, de tal maneira que os dados originais, quer não pode ser obtido ou só pode ser obtida por meio de um processo de decriptografia.

CVSS Veja Common Vulnerability System.

D

dados de carga útil
os dados do aplicativo contidos em um fluxo de IP, excluindo cabeçalho e informações administrativas.

destino de encaminhamento
Um ou mais sistemas fornecedores que recebem dados brutos e normalizados a partir de fontes de log e fontes de fluxo.

destino externo
Um dispositivo que está fora do local primário que recebe fluxo de evento ou dados de um coletor de eventos.

Device Support Module (DSM)
Um arquivo de configuração que analisa eventos recebidos de múltiplas fontes de log e os converte para um formato de taxonomia padrão, que pode ser exibida como saída.

DHCP Consulte Dynamic Host Configuration Protocol.

dispositivo de varredura externo
Uma máquina que é conectada à rede para reunir informações de vulnerabilidade sobre ativos na rede.

DNS Consulte Domain Name System.

DSM Consulte Módulo de Suporte de Dispositivo.

Dynamic Host Configuration Protocol (DHCP)
Um protocolo de comunicação utilizado para gerenciar centralmente as informações de configuração. Por exemplo, o DHCP automaticamente designa endereços IP para computadores em uma rede.

E

endereço IP virtual de cluster
Um endereço IP que é compartilhado entre o host primário ou secundário e o cluster de HA.

extensão de origem de log
Um arquivo XML que inclui todos os padrões de expressão regular necessários para identificar e categorizar eventos da carga útil do evento.

F

falso positivo
Um resultado de teste classificado como positivo (indicando que o site está vulnerável ao ataque), que o usuário decide que é na realidade negativo (não uma vulnerabilidade).

Fluxo Uma única de transmissão de dados transmitidos através de um link durante uma conversação.

fluxo de log
Uma coleção de grvação de fluxo.

fluxo duplicado
Várias instâncias do mesmo fluxo de transmissão recebidos a partir de diferentes origens de dados.

folha Em uma árvore, uma entrada ou nó que não possui frutos.

fontes de fluxo
A orígem na qual o fluxo é capturado. Uma fonte de fluxo é classificada como interna, quando o fluxo vem de um hardware instalado em um gerenciador de host ou é classificado como externo, quando o fluxo é enviado para um coletor de fuxo.

FQDN
Consulte nome completo do domínio.

FQNN
Consulte nome completo da rede.

funcionário público
Um componente interno que analisa o tráfego de rede e os eventos de segurança em relação às regras customizadas definidas.

G

Gateway
Um dispositivo ou programa usado para conectar redes ou sistemas com diferentes arquiteturas de rede.

H

HA Consulte alta disponibilidade.

Hash-Com Message Authentication Code (HMAC)
O código de criptografia que usa criptografia função hash e chave secreta.

hierarquia de rede
Um tipo de contêiner que constitui uma coleta hierárquica de objetos da rede.

HMAC
Consulte Código de autenticação Hash-Based Message .

host de HA primário
O computador principal que é conectada ao cluster de HA.

host de HA secundário
O computador espera que o está conectado ao cluster de HA. O host de HA secundário assume a responsabilidade do host de HA primário se o host de HA primário falhar.

I

ICMP Consulte Internet Control Message Protocol.

Identifica
Uma coleta de atributos de uma origem de dados que representa uma pessoa, organização, lugar ou item.

IDS Consulte sistema de detecção de intrusão.

Interconexão de sistemas abertos (OSI)
A interconexão de sistemas abertos em concordância com padrões do International Organization for Standardization (ISO) para a troca de informações.

interface ligada
Consulte agregação de link.

Internet Control Message Protocol (ICMP)
Um protocolo de Internet que é usado por um getway para comunicar-se com um

host de origem, por exemplo, para reportar um erro em um datagrama.

intervalo de relatório
Um intervalo de tempo configurável no final do qual o processador de evento deve enviar todos os eventos capturados e fluxo de dados para o console.

intervalo de união
O intervalo no qual os eventos são empacotados. o pacote configurável de eventos ocorre em intervalos de 10s. e começa com o primeiro evento que não corresponde a nenhum evento de união atualmente. No intervalo de união, os três primeiros eventos correspondentes são empacotados e enviados para o processador de eventos.

IP Consulte Protocolo da Internet.

IP multicast
Transmissão de um datagrama protocolo de internet (IP), para configurar sistemas que formam um grupo multicast único.

IPS Consulte sistema de prevenção de intrusão.

ISP Consulte Provedor de serviços da Internet.

L

LDAP Consulte protocolo LDAP.

L2L Consulte Local para Local.

Local para Local (L2L)
Pertencente ao tráfego interno de uma rede local para outra rede local.

Local para Remoto (R2L)
O tráfego externo a partir de uma rede remota a uma rede local.

L2R Consulte Local para Remoto.

M

magnitude
Uma medida da importância relativa de uma determinada falha crítica. Magnitude é um valor calculado a partir de peso a relevância, gravidade e credibilidade.

mapa de referência
Um registro de dados de mapeamento direto de uma chave para um valor, por exemplo, um nome de usuário para um ID global.

mapa de referência de conjuntos
Um registro de dados de uma chave mapeada para muitos valores. Por exemplo, o mapeamento de uma lista de usuários privilegiados para um host.

mapa de referência de mapas
Um registro de dados de duas chaves mapeadas para muitos valores. Por exemplo, o mapeamento do total de bytes de um aplicativo para um IP de origem.

Mapear QID
Uma taxonomia que identifica cada evento único e mapeia os eventos de categoria baixo e alto nível, para determinar como um evento deve ser correlacionado e organizado.

máscara de sub-rede
Para sub-rede da Internet, uma máscara de 32 bits usada para identificar os bits do endereço da sub-rede na parte do host de um endereço IP.

N

NAT Consulte conversão de endereço de rede.

NetFlow
Um protocolo de rede Cisco que monitora dados do fluxo do tráfego de rede. Dados NetFlow incluem informações do cliente e informações de servidores, cujas portas são usadas, e o número de bytes e pacotes que fluem através de roteadores conectados a uma rede. Os dados são enviados para os coletores NetFlow onde dados são analisados.

Nome completo da rede (FQNN)
Em uma hierarquia da rede, o nome de um objeto que inclui todos os departamentos. Um exemplo de um nome completo de rede é CompanyA.Department.Marketing.

Nome completo do domínio (FQDN)
Em comunicações da Internet, o nome de um sistema de host que inclui todos os subnomes do nome de domínio. Um exemplo de um nome de domínio completo é rchland.vnet.ibm.com.

NRA Consulte número de sistema autônomo.

número do sistema ASN (Autonomous)
Em TCP/IP, um número que designa um sistema autônomo pela mesma central de autoridade que designa um endereço de IP. O sistema autônomo faz com que seja possível para algoritimos de roteamentos automatizados, a distinção desistemas autônomos.

O

objeto rede
Um componente de uma hierarquia de rede.

ofensa Uma mensagem enviada ou um evento gerado em resposta a uma condição monitorada. Por exemplo, uma ofensa fornecerá informações sobre se uma política tiver sido infringida ou a rede está sofrendo um ataque.

O objeto folha de banco dados
Um objeto terminal ou um nó em uma hierarquia de banco de dados.

ordem de análise
Uma definição de origem de log na qual o usuário pode definir a ordem de importância para origens de log que compartilham um endereço IP ou um nome de host comum.

origem do log
O equipamento de segurança ou o equipamento de rede a partir da qual uma origem de log de eventos.

origem externa
Um dispositivo que está fora do local primário que envia dados normalizados para um coletor de eventos.

o servidor whois
Um servidor que é utilizado para recuperar as informações sobre uma Internet recursos registrados, como nomes de domínio e alocações de endereço IP.

OSI Consulte interconexão de sistemas abertos.

OSVDB
Consulte Abrir Origem Vulnerabilidade de Banco de Dados.

P

Para Local (Remote L2R)
Relativo ao tráfego interno de uma rede local para outra rede remota.

para Remoto (Remote R2R)
O tráfego externo a partir de uma rede remota para outra rede remota.

peso de rede
O valor numérico aplicado para cada rede que significa a importância da rede. O peso da rede é definido pelo usuário.

ponto de dados
Um valor calculado de uma métrica em um momento.

protocolo
Um conjunto de regras que controlam a comunicação e a transferência de dados entre dois ou mais dispositivos ou sistemas em uma rede de comunicação.

Protocolo da Internet(IP)
Um protocolo que encaminha dados através de uma rede ou redes interconectadas. Este protocolo atua como um intermediário entre as camadas de protocolo superiores e a rede física. Consulte também Transmission Control Protocol.

Protocolo de Controle de Transmissões (TCP)
Um protocolo de comunicação utilizado na Internet e em todas as redes que seguem os padrões da Internet Engineering Task Force (IETF) para protocolo de interligação de redes. O TCP oferece um protocolo confiável de host a host em redes de comunicação através da comutação de pacotes e em sistemas interconectados dessas redes. Consulte também Internet Protocol.

protocolo LDAP
Um protocolo que usa TCP/IP para fornecer acesso aos diretórios que suportam um modelo X.500 que não incorra nos requisitos de recursos X.500 Directory Access Protocol (DAP)mais complexos. Por exemplo, LDAP pode ser usado para localizar pessoas, organizações, e outros recursos em um diretório intranet, ou internet.

Provedor de serviços da Internet (ISP)
Uma organização que fornece acesso à Internet.

R

recon Consulte reconhecimento.

reconhecimento (recon)
Um método pelo qual as informações pertencentes à identidade dos recursos da rede são reunidas. Varredura da rede e outras técnicas são usadas para compilar uma lista de eventos de recursos da rede que são então designados a um nível de severidade.

Rede Local
Consulte rede local.

Rede local (LAN)
Uma rede que conecta vários dispositivos em uma área limitada (tal como uma única construção ou campus) e que pode ser conectada a uma rede maior.

Redirecionamento do ARP
Um método ARP para notificar o host se existe um problema em uma rede.

regra Um conjunto de instruções condicionais que permitem que os sistemas de computador identifiquem relacionamentos e executem respostas automatizadas adequadamente.

regra de roteamento
Uma condição que quando seus critérios são satisfeitos por dados do evento, uma coleta de condições e roteamento subsequente são executadas.

relatório
Em um gerenciamento de consulta, os dados formatados que resultam da execução de uma consulta e da aplicação de um formulário a ela.

relevância
Uma medida de impacto relativo de um evento, categoria ou ofensa na rede.

R2L Consulte Local para Remoto.

R2R Consulte Para Remoto Remoto.

S

scanner
Um programa de segurança automatizado que procura por vulnerabilidades do software dentro de aplicativos da web.

severidade
Uma medida da ameaça relativo que uma origem apresenta em um destino.

sistema ativo
Em um cluster de alta disponibilidade (HA), o sistema que possui todos os seus serviços em execução.

Sistema de detecção de intrusão (intrusion detection system) (IDS)
Software que detecta tentativas de ataque ou ataques bem sucedidos nos recursos monitorados que são parte de uma rede ou de um host de sistema.

sistema de espera
Um sistema que automaticamente se torna ativo quando o sistema ativo falhar. Se a replicação de disco estiver ativado, replica dados do sistema ativo.

Sistema de Nomes de Domínio (DNS)
O sistema de banco de dados distribuído que mapeia nomes de domínio para endereços IP.

Sistema de Pontuação de Vulnerabilidade Comum - Common Vulnerability Scoring System (CVSS)
Um sistema de pontuação cuja severidade de vulnerabilidade é medida.

Sistema de prevenção de intrusão (IPS)
Um sistema que tenta negar a atividade potencialmente dolosa. Os mecanismos de negação podem envolver filtragem, rastreamento ou configuração de taxa limite.

SNMP
Consulte Simple Network Management Protocol.

SNMP (Simple Network Management Protocol)
Um conjunto de protocolos para sistemas de monitoramento e os dispositivos em redes complexas. As informações sobre os dispositivos gerenciados são definidas e armazenadas em uma Management Information Base (MIB).

SOAP Um protocolo leve, baseado em XML para troca de informações em um ambiente distribuído, descentralizado. SOAP pode ser utilizado para consultar e retornar informações e chamar os serviços através da Internet.

sub-procura
Uma função que permite que uma

consulta de procura para ser executada dentro de um conjunto de resultados de procura concluídas.

sub-rede
Consulte sub-rede.

sub-rede (sub-rede)
Uma rede que é dividida em subgrupos independentes menores, que ainda estão interconectados.

superflow
Um único fluxo que é composto de vários fluxos com propriedades semelhantes para aumentar a capacidade de processamento reduzindo as restrições de armazenamento.

T

tabela de referência
Uma tabela em que o registro de dados mapeia chaves que têm um tipo designado para outras chaves que são, em seguida, mapeadas para um único valor.

TCP Consulte Protocolo de Controle de Transmissões.

Tempo de atualização
Um dispositivo interno que é disparado manualmente ou automaticamente em intervalos de tempo que atualiza os dados da atividade de rede atual.

terminal
O endereço de uma API ou um serviço em um ambiente. Uma API expõe um terminal e ao mesmo tempo chama os terminais de outros serviços.

V

varredura em tempo real
Uma varredura de vulnerabilidade que gera dados do relatório a partir dos resultados da varredura com base no nome da sessão.

violação
Um ato que ignora ou contrária à política corporativa.

visualização do sistema
Uma representação visual de ambos primário e os hosts gerenciados que compõem um sistema.

vulnerabilidade
Uma exposição de segurança em um sistema operacional, software do sistema ou componente de software de aplicativo.

Vulnerabilidade de Banco de Dados de Origem Aberta (OSVDB)
Criado pela comunidade de segurança de rede para a segurança da comunidade de rede, um banco de dados aberto que fornece informações técnicas en uma rede de vulnerabilidade de segurança.

Índice Remissivo

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V