

IBM Security QRadar Log Manager
Versão 7.2.1

Guia dos Usuários



Nota

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 151.

Índice

Sobre o Guia do Usuário do QRadar Log Manager	vii
Capítulo 1. O que há de novo para usuários no QRadar Log Manager V7.2.2	1
Capítulo 2. Sobre o QRadar Log Manager	3
Navegadores da web suportados	3
Ativar o modo de documento e modo de navegação no Internet Explorer	3
Acessar o IBM Security QRadar	4
Guias da interface com o usuário	4
Guia Pannel	4
Guia Atividade de log	4
Guia ativos	4
guia relatórios	5
Guia IBM Security QRadar Vulnerability Manager	5
guia Admin.	5
Procedimentos comuns do QRadar	6
Visualizando mensagens	6
Classificando resultados	8
Atualizando e pausando a interface com o usuário	9
Investigando endereços IP	9
Investigar nomes de usuário	11
Tempo do sistema	11
Atualizando preferências do usuário	11
Acessar ajuda online	12
Redimensionar colunas	12
Configurar tamanho da página	13
Capítulo 3. Gerenciamento de painel	15
Atividade de log	15
Relatórios mais recentes	17
Resumo do sistema	17
Itens de gerenciamento de vulnerabilidade	17
Notificação do sistema	18
Incluindo itens do painel	19
Usando o painel para investigar a atividade de log	19
Configurando gráficos	20
Removendo itens do painel	21
Removendo um item do painel	21
Renomeando um painel	21
Excluindo um painel	22
Gerenciando notificações do sistema	22
Incluindo itens baseados em painel para a lista Incluir Itens	22
Capítulo 4. Investigação de atividade de log	25
Visão geral da guia Atividade de log	25
Barra de ferramentas da guia Atividade de log	25
Síntaxe de filtro rápido	29
Opções de menu ativado pelo botão direito	30
Barra de status	30
Monitorando a atividade de log	30
Visualizando eventos de fluxo	31
Visualizando eventos normalizados	31
Visualizando eventos brutos	34
Visualizando eventos agrupados	36

Detalhes do evento	41
Barra de ferramentas de detalhes do evento	44
Modificando mapeamento de eventos	45
Gerenciando dados de PCAP	46
Exibindo a coluna de dados do PCAP	46
Visualizando informações do PCAP	47
Fazendo download do arquivo PCAP para seu sistema de desktop	48
Exportando eventos	49
Capítulo 5. Gerenciamento de gráfico	51
Visão geral do gráfico de série temporal	51
Legendas do gráfico	53
Configurando gráficos	53
Capítulo 6. Procuras de dados	57
Procurando itens que correspondam com seus critérios	57
Salvando critérios de procura	63
Excluindo critérios de procura	64
Usando uma subprocura para refinar resultados da procura	65
Gerenciando resultados da procura	66
Salvando resultados da procura	66
Visualizando resultados da procura gerenciada	66
Cancelando uma procura	68
Excluindo uma procura	69
Gerenciando grupos de procura	69
Visualizando grupos de procura	69
Criando um novo grupo de procura	70
Editando um grupo de procura	70
Copiando uma procura salva em outro grupo	71
Removendo um grupo ou uma procura salva de um grupo	71
Capítulo 7. Propriedades de evento customizado	73
Permissões requeridas	73
Tipos de propriedades customizadas	73
Criando uma propriedade customizada baseada em regex	74
Criando uma propriedade customizada baseada em cálculo	76
Modificando uma propriedade customizada	77
Copiando uma propriedade customizada	79
Excluindo uma propriedade customizada	79
Capítulo 8. Gerenciamento de regras.	81
Considerações sobre permissão de regra	81
Visão geral de regras	81
Regra de evento	81
Condições da regra	81
Respostas da regra	82
Visualizando regras	83
Criando uma regra customizada	84
Criando uma regra de detecção de anomalia	85
Tarefas de gerenciamento de regra	86
Ativando e desativando regras	87
Editando uma regra	87
Copiando uma regra	87
Excluindo uma regra	88
Gerenciamento de grupo de regras	88
Visualizando um grupo de regra	88
Criando um grupo	89
Designando um item a um grupo	89
Editando um grupo	89
Copiando um item para outro grupo	90

Excluindo um item de um grupo	90
Excluindo um grupo	90
Editando blocos de construção	90
Parâmetros de página Regra.	91
Barra de ferramentas da página Regras	92
Parâmetros da página Resposta de regra.	94
Capítulo 9. Perfis de ativos	99
Sobre as vulnerabilidades.	99
Visão geral da guia Ativos	99
Lista da guia Ativo	100
Barra de ferramentas da guia Ativos.	101
Opções de menu ativado pelo botão direito	103
Visualizando um perfil de ativos	104
Incluindo ou editando um perfil de ativo	106
Procurando perfis de ativos.	110
Salvando critérios de procura de ativos.	111
Grupos de procura de ativos	112
Visualizando grupos de procura	112
Criando um novo grupo de procura	113
Editando um grupo de procura	113
Copiando uma procura salva em outro grupo	113
Removendo um grupo ou uma procura salva de um grupo	114
Tarefas de gerenciamento de perfil do ativo	114
Excluindo ativos	114
Importando perfis de ativos	114
Exportando ativos.	115
Pesquisar vulnerabilidades de ativos	116
Parâmetros da página Perfil de ativo	118
Área de janela de resumo de ativo	118
Área de janela de resumo da interface de rede	121
Área de janela de vulnerabilidade	121
Área de janela de serviços	123
Área de janela de Serviços do Windows	124
Área de janela de pacotes	124
Área de janela de correções do Windows	125
Área de janela de propriedades	125
Área de janela de políticas de risco	125
Área de janela de produtos.	126
Capítulo 10. Gerenciamento de relatório.	127
Visão geral da guia Relatórios	128
Considerações sobre fuso horário.	128
Permissões da guia Relatório	128
Parâmetros da guia Relatório	128
Ordem de classificação na guia Relatório	129
Barra de ferramentas da guia Relatório.	129
Barra de status	131
Layout de relatório	131
Tipos de gráfico	131
Tipos de diagrama.	132
Criando relatórios customizados	132
Tarefas de gerenciamento de relatório	135
Editando um relatório	136
Visualizando relatórios gerados	136
Excluindo conteúdo gerado.	137
Gerando um relatório manualmente.	137
Duplicando um relatório	137
Compartilhando um relatório	138
Relatórios de marca	138

Grupos de relatórios	139
Criando um grupo de relatórios	139
Editando um grupo	140
Designar um relatório a um grupo	140
Copiando um relatório para outro grupo	140
Removendo um relatório	141
Contêiner do gráfico	141
Parâmetros de contêiner do gráfico Vulnerabilidades do ativo	141
Parâmetros do contêiner do gráfico Eventos/logs	143
Avisos	151
Marcas registradas.	153
Considerações de política de privacidade	153
Glossário	155
A	155
B	155
C	155
D	156
E	156
F	156
G	157
H	157
I	157
L	157
M	158
N	158
O	158
P	159
R	159
S	160
T	160
V	160
Índice Remissivo	161

Sobre o Guia do Usuário do QRadar Log Manager

O Guia do Usuário do IBM® Security QRadar Log Manager fornece informações sobre como gerenciar o IBM Security QRadar SIEM incluindo as guias Painel, Atividade de log e Relatórios.

Público-alvo

Este guia é destinado a todos os usuários do QRadar SIEM responsáveis pela investigação e o gerenciamento da segurança de rede. Este guia presume que você tenha o acesso ao QRadar SIEM e um conhecimento da sua rede corporativa e das tecnologias de rede.

Documentação técnica

Para obter informações sobre como acessar mais documentações técnicas, notas técnicas e notas sobre a libertação, consulte a Acessando a Nota Técnica de Documentação do IBM Security (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

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 por meio da prevenção, detecção e resposta ao acesso incorreto 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. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que, necessariamente, envolverá procedimentos operacionais adicionais e poderá precisar de outros sistemas, produtos ou serviços para se tornar mais efetiva. A IBM NÃO GARANTE QUE QUAISQUER SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU QUE DEIXARÃO SUA EMPRESA ESTEJA IMUNE DE CONDUTAS MALICIOSAS OU ILEGAIS DE TERCEIROS.


Capítulo 1. O que há de novo para usuários no QRadar Log Manager V7.2.2

IBM Security QRadar Log Manager V7.2.2 introduz as atualizações das preferências do usuário para a seleção de idioma, seleção de diferentes códigos de idioma para valores numéricos, visualização das mensagens do sistema e interface com dados fornecidos de usuário.

Os usuários podem configurar suas preferências de idioma

O QRadar está disponível nos idiomas a seguir: inglês, chinês simplificado, chinês tradicional, japonês, coreano, francês, alemão, italiano, espanhol, e português (Brasil). Os usuários podem selecionar seu idioma preferencial ao escolher a configuração do **Código de Idioma** na lista de **Preferências**.  Saiba mais...

Suporte de valores numéricos em diferentes códigos de idioma para eventos customizados

O QRadar possui agora a capacidade de suportar valores numéricos usando diferentes códigos de idioma para eventos customizados.  Saiba mais...

As novas funções de usuário podem visualizar as notificações do sistema

Os usuários podem ver as notificações do sistema no Painel.

As novas funções de usuário podem ter interface com seus dados

Os usuários podem ter interface com as coleções de dados que suportam.

Capítulo 2. Sobre o QRadar Log Manager

O IBM Security QRadar Log Manager é uma plataforma de gerenciamento de segurança de rede que fornece o reconhecimento situacional e o suporte de conformidade através da correlação, análise e relatórios de eventos de segurança.

Navegar no aplicativo baseado na web

Ao usar o QRadar Log Manager, use as opções de navegação disponíveis na interface com o usuário em vez do botão **Voltar** do navegador da web.

Navegadores da web suportados

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

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

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

Tabela 1. Navegadores da web suportados para produtos QRadar

Navegador da web	Versão suportada
Mozilla Firefox	17,0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer de 32 bits, com o modo de documento e modo de navegação ativados	8.0 9.0
Google Chrome	A versão atual a partir da data da liberação dos produtos IBM Security QRadar V7.2.2

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

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

Procedimento

1. Em seu navegador da web Internet Explorer, pressione F12 para abrir a janela Ferramentas de Desenvolvedor.
2. Clique em **Modo de Navegador** e selecione a versão do seu navegador da web.
3. Clique em **Modo de Documento**.
 - Para o Internet Explorer V9.0, selecione **Internet Explorer 9**
 - Para o Internet Explorer V8.0, selecione **Internet Explorer 7.0 Standards**

Acessar o IBM Security QRadar

O IBM Security QRadar é um aplicativo baseado na web. O QRadar usa as informações de login padrão da URL, nome de usuário e senha.

Use as informações na tabela a seguir ao efetuar login em seu console do IBM Security QRadar.

Tabela 2. Informações de login padrão do QRadar

Informações de login	Padrão
URL	https://<Endereço IP>, em que <Endereço IP> é o endereço IP do console do QRadar. Para efetuar login para o QRadar em um IPv6 ou em um ambiente misto, agrupe os endereços IP em colchetes: https://[<IP Address>]
Nome de usuário	admin
Senha	A senha que é designada ao QRadar durante o processo de instalação.
Chave de licença	Uma chave de licença padrão fornece acesso ao sistema por 5 semanas.

Guias da interface com o usuário

A funcionalidade é dividida em guias. A guia **Painel** é exibida quando você efetua login.

É possível facilmente navegar nas guias para localizar os dados ou funcionalidade requeridos.

Guia Painel

A guia **Painel** é a guia padrão que será exibida ao efetuar login.

A guia **Painel** é a guia padrão exibida ao efetuar login no IBM Security QRadar Log Manager. Ele fornece um ambiente de área de trabalho que fornece um resumo e informações detalhadas sobre os eventos que ocorrem em sua rede.

Guia Atividade de log

A guia **Atividade de log** permitirá que você investigue os logs de evento enviados para o QRadar em tempo real, execute procuras poderosas e visualize a atividade de log usando gráficos de séries temporais configuráveis.

A guia **Atividade de log** permitirá que seja executada uma investigação detalhada dos dados do evento.

Para obter mais informações, consulte Investigação da atividade de log.

Guia ativos

O QRadar descobre automaticamente ativos, servidores e hosts operando em sua rede.

Perfis de ativo fornecem informações sobre cada ativo conhecido em sua rede, incluindo informações de identidade, se disponível, e quais serviços estão em execução em cada ativo. Esses dados de perfil são usados para finalidades de correlação para ajudar a reduzir positivos falsos.

Por exemplo, um ataque tenta usar um serviço específico que está sendo executado em um ativo específico. Nesta situação, o QRadar pode determinar se o ativo está vulnerável a este ataque correlacionando o ataque ao perfil de ativo. Usando a guia **Ativos**, é possível visualizar os ativos aprendidos ou procurar ativos específicos para visualizar seus perfis.

Para obter mais informações, consulte Gerenciamento de ativos.

guia relatórios

A guia **Relatórios** permitirá que você crie, distribua e gerencie relatórios para quaisquer dados dentro de QRadar.

O recurso Relatórios permitirá a criação de relatórios customizados para uso operacional e executivo. Para criar um relatório, você pode combinar as informações (como, segurança ou rede) em um único relatório. É possível também usar modelos de relatório pré-instalados que são incluídos com QRadar.

A guia **Relatórios** também permitirá que você marque seus relatórios com logotipos customizados. Esta customização é útil para distribuir relatórios para diferentes públicos.

Para obter mais informações sobre relatórios, consulte Gerenciamento de relatórios.

Guia IBM Security QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager é um componente do QRadar que você pode comprar separadamente. Você usa uma chave de licença para ativar o Gerenciador de Vulnerabilidade do QRadar.

Gerenciador de Vulnerabilidade do QRadar é uma plataforma de varredura de rede que fornece reconhecimento das vulnerabilidades que existem nos aplicativos, sistemas ou dispositivos em sua rede. Depois que as varreduras identificarem vulnerabilidades, você poderá procurar e revisar dados de vulnerabilidade, corrigir vulnerabilidades e executar novamente varreduras para avaliar o novo nível de risco.

Quando o IBM Security QRadar Vulnerability Manager estiver ativado, você poderá executar tarefas de avaliação de vulnerabilidades na guia Vulnerabilidades. Na guia Ativos, você pode executar varreduras do IBM Security QRadar Vulnerability Manager em ativos selecionados.

Para obter mais informações, consulte o Guia do Usuário do *IBM Security QRadar Vulnerability Manager*.

guia Admin

Os administradores usam a guia Administração para configurar e gerenciar os usuários, sistemas, redes, plug-ins e componentes. Os usuários com privilégios administrativos podem acessar a guia **Administração**.

As ferramentas de administração que os administradores podem acessar na guia **Administração** estão descritas na Tabela 1.

Tabela 3. Ferramentas de gerenciamento de administração disponíveis em QRadar

Ferramenta de administração	Descrição
Configuração do Sistema	Configura o sistema e as opções de gerenciamento do usuário.
Origens de Dados	Configura fontes de log.
Configuração de Redes e Serviços Remotos	Configurar redes remotas e grupos de serviços.
Plug-ins	Acesso os componentes de plug-in, como o plug-in IBM Security QRadar Risk Manager. Essa opção será exibida somente se houver plug-ins que estejam instalados em seu Console.
Editor de Implementação	Gerencie os componentes individuais da implementação do QRadar.

Todas as atualizações de configuração feitas na guia **Administração** são salvas em uma área de preparação. Quando todas as alterações estiverem concluídas, será possível implementar as atualizações de configuração no host gerenciado em sua implementação.

Procedimentos comuns do QRadar

Vários controles na interface com o usuário do QRadar são comuns para a maioria das guias da interface com o usuário.

As informações sobre esses procedimentos comuns estão descritas nas seções a seguir.

Visualizando mensagens

O menu **Mensagens**, no canto superior direito da interface com o usuário, fornece acesso a uma janela na qual você pode ler e gerenciar suas notificações do sistema.

Antes de Iniciar

Para as notificações do sistema serem exibidas na janela **Mensagens**, o administrador deve criar uma regra baseada em cada tipo de mensagem de notificação e selecionar a caixa de seleção **Notificação** no **Assistente de regras customizadas**.

Sobre Esta Tarefa

O menu **Mensagens** indica quantas notificações não lidas do sistema que você tem em seu sistema. Este indicador incrementa o número até que você feche as notificações do sistema. Para cada notificação do sistema, a janela **Mensagens** fornece um resumo e o registro de data para quando a notificação do sistema foi criada. Você pode passar o ponteiro do mouse sobre uma notificação para visualizar mais detalhes. Usando as funções na janela **Mensagens**, você pode gerenciar as notificações do sistema.

As notificações do sistema também estão disponíveis na guia **Painel** e em uma janela pop-up opcional que pode ser exibida no canto inferior esquerdo da interface com o usuário. As ações que você executa na janela **Mensagens** são propagadas para a guia **Painel** e a janela pop-up. Por exemplo, se você fechar uma notificação do sistema na janela **Mensagens**, a notificação do sistema será removida de todas as exibições das notificações do sistema.

Para obter mais informações sobre notificações do sistema do Painel, consulte Item de notificações do sistema.

A janela **Mensagens** fornece as seguintes funções:

Tabela 4. Funções disponíveis na janela Mensagens

Função	Descrição
Todos	Clique em Todos para visualizar todas as notificações do sistema. Esta opção é o padrão, portanto, você apenas clicará em Todos se selecionar outra opção e desejar exibir todas as notificações do sistema novamente.
Funcionamento	Clique em Funcionamento para visualizar apenas as notificações do sistema que tenham um nível de gravidade de funcionamento.
Erros	Clique em Erros para visualizar apenas as notificações do sistema que tenham um nível de gravidade de erro.
Avisos	Clique em Avisos para visualizar apenas as notificações do sistema que possuem um nível de gravidade de aviso.
Informações	Clique em Informações para visualizar apenas as notificações do sistema que tenham um nível de gravidade de informação.
Descartar todos	Clique em Descartar todos para fechar todas as notificações do sistema de seu sistema. Se você filtrou a lista de notificações do sistema usando o Funcionamento , Erros , Avisos ou Ícones de informações , o texto no ícone Visualizar tudo será alterado para uma das opções a seguir: <ul style="list-style-type: none"> • Descartar todos os erros • Descartar todo o funcionamento • Descartar todos os avisos • Descartar todos os avisos • Descartar todas as informações

Tabela 4. Funções disponíveis na janela Mensagens (continuação)

Função	Descrição
Visualizar tudo	Clique em Visualizar tudo para visualizar os eventos de notificação do sistema na guia Atividade de Log . Se você filtrou a lista de notificações do sistema usando o Funcionamento, Erros, Avisos ou Ícones de informações , o texto no ícone Visualizar tudo será alterado para uma das opções a seguir: <ul style="list-style-type: none"> • Visualizar todos os erros • Visualizar todo o funcionamento • Visualizar todos os avisos • Visualizar todas as informações
Descartar	Clique no ícone ao lado de Descartar ao lado de uma notificação do sistema para fechar a notificação do sistema de seu sistema.

Procedimento

1. Efetuar login no QRadar.
2. No canto superior direito da interface com o usuário, clicar em **Mensagens**.
3. Na janela **Mensagens**, visualizar os detalhes de notificação do sistema.
4. Opcional. Para refinar a lista de notificações do sistema, clique em uma das opções a seguir:
 - **Erros**
 - **Avisos**
 - **Informações**
5. Opcional. Para fechar as notificações do sistema, escolha uma das opções a seguir:

Opção	Descrição
Descartar todos	Clique para fechar todas as notificações do sistema.
Descartar	Clique no ícone Descartar próximo à notificação do sistema que você deseja fechar.

6. Opcional. Para visualizar os detalhes de notificação do sistema, passe o ponteiro do mouse sobre a notificação do sistema.

Classificando resultados

É possível classificar os resultados em tabelas clicando em um título da coluna. Uma seta na parte superior da coluna indica a direção da classificação.

Procedimento

1. Efetue login no QRadar.
2. Clique no cabeçalho da coluna uma vez para classificar a tabela em ordem decrescente; duas vezes para classificar a tabela em ordem crescente.

Atualizando e pausando a interface com o usuário

Você pode atualizar, pausar e executar manualmente os dados exibidos nas guias.

Sobre Esta Tarefa

A guia **Atividade de log** será atualizada automaticamente a cada 60 segundos se você estiver visualizando a guia no modo de Último Intervalo (atualização automática).

O cronômetro, que está no canto superior direito da interface, indica a quantidade de tempo até que a guia seja atualizada automaticamente.

Ao visualizar a guia **Atividade de log** no modo de Tempo Real (fluxo) ou Último Minuto (atualização automática), você poderá usar o ícone **Pausar** para pausar a exibição atual.

Você também pode pausar a exibição atual na guia **Painel**. Clicando em qualquer lugar dentro de um item de painel irá pausar a guia automaticamente. O cronômetro pisca em vermelho para indicar que a exibição atual está pausada.

Procedimento

1. Efetue login no QRadar.
2. Clique na guia que você deseja visualizar.
3. Escolha uma das opções a seguir:

Opção	Descrição
Atualizar	Clique em Atualizar , no canto direito da guia, para atualizar a guia.
Pausar	Clique para pausar a exibição na guia.
Executar	Clique para reiniciar o cronômetro depois que ele estiver pausada.

Investigando endereços IP

Você pode usar diversos métodos para investigar as informações sobre os endereços IP nas guias Painel, Atividade de log e Atividade de rede.

Sobre Esta Tarefa

Você pode localizar mais informações sobre um endereço IP por qualquer um dos métodos listados na tabela a seguir.

Tabela 5. Informações de endereços IP

Opção	Descrição
Informações > Consulta de DNS	Procura por entradas de DNS baseadas no endereço IP.
Informações > Consulta de WHOIS	Procura pelo proprietário registrado de um endereço IP remoto. O servidor WHOIS padrão é whois.arin.net.

Tabela 5. Informações de endereços IP (continuação)

Opção	Descrição
Informações > Varredura de porta	Executa uma varredura do Mapeador de Rede (NMAP) do endereço IP selecionado. Essa opção estará disponível apenas se o NMAP estiver instalado em seu sistema. Para obter mais informações sobre a instalação do NMAP, consulte a documentação do seu fornecedor.
Informações > Perfil de ativo	Exibe as informações do perfil de ativos. Essa opção será exibida se o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter mais informações, consulte <i>Guia do Usuário do IBM Security QRadar Vulnerability Manager</i> . Essa opção de menu estará disponível se o QRadar adquiriu os dados de perfil ativamente através de uma varredura.
Informações > Procurar eventos	Procura por eventos associados a esse endereço IP.
Informações > Procurar conexões	Procura por conexões associadas a esse endereço IP. Essa opção só estará disponível se você comprou o IBM Security QRadar Risk Manager e conectou o QRadar e o dispositivo do IBM Security QRadar Risk Manager. Para obter mais informações, consulte o <i>Guia do Usuário do IBM Security QRadar Risk Manager</i> .
Informações > Consulta de porta do computador	
Informações > Visualizar topologia	Exibe a guia que descreve a topologia de camada 3 da sua rede. Essa opção estará disponível se você comprou o IBM Security QRadar Risk Manager e conectou o QRadar e o dispositivo do IBM Security QRadar Risk Manager. dispositivo.
Execução de informações > Varredura QVM	Selecione a opção Executar Varredura QVM para varrer o IBM Security QRadar Vulnerability Manager nesse endereço IP. Essa opção é exibida somente quando o IBM Security QRadar Vulnerability Manager foi comprado e licenciado. Para obter mais informações, consulte <i>Guia do Usuário do IBM Security QRadar Vulnerability Manager</i> .

Para obter informações sobre a guia Riscos ou o IBM Security QRadar Risk Manager, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.

Procedimento

1. Efetue login no QRadar.
2. Clique na guia que você deseja visualizar.
3. Mova o ponteiro do mouse sobre um endereço IP para visualizar o local do endereço IP.

4. Clique com o botão direito do mouse no endereço IP ou no nome do ativo e selecione uma das opções a seguir:

Investigar nomes de usuário

É possível clicar com o botão direito em um nome de usuário para acessar mais opções de menu. Use essas opções para visualizar mais informações sobre o nome de usuário ou endereço IP.

É possível investigar os nomes de usuários quando o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

Ao clicar com o botão direito em um nome de usuário, será possível escolher as seguintes opções de menu.

Tabela 6. Opções de menu para investigação nome de usuário

Opção	Descrição
Visualizar ativos	Exibe os ativos atuais que estão associados ao nome de usuário selecionado. Para obter mais informações sobre a visualização de ativos, consulte Gerenciamento de ativos.
Visualizar Histórico de Usuário	Exibe todos os ativos que estão associados ao nome de usuário selecionado nas 24 horas anteriores.
Visualizar eventos	Exibe os eventos que são associados ao nome de usuário selecionado. Para obter mais informações sobre a janela Lista de eventos, consulte Monitoramento de atividade de log.

Para obter mais informações sobre como customizar o menu ativado pelo botão direito, consulte o *Guia de Administração* do seu produto.

Tempo do sistema

O canto direito da interface com o usuário QRadar exibe o tempo do sistema, que é o tempo no console.

O tempo do console sincroniza os sistemas QRadar na implementação do QRadar. O tempo do console é usado para determinar quais eventos de tempo foram recebidos de outros dispositivos para correlação de sincronização de tempo correta.

Em uma implementação distribuída, o console pode estar em um fuso horário diferente de seu computador de área de trabalho.

Quando você aplica filtros e procuras baseadas em tempo na guia **Atividade do log**, você deve usar o tempo do sistema do console para especificar um intervalo de tempo.

Atualizando preferências do usuário

É possível configurar as preferências do usuário, como código de idioma, na principal interface com o usuário do QRadar.

Procedimento

1. Para acessar as informações sobre o usuário, clique em **Preferências**.
2. Atualizar as preferências.

Opção	Descrição
Nome de usuário	Exibe seu nome de usuário. Não é possível editar este campo.
Senha	A senha deve atender aos seguintes critérios: <ul style="list-style-type: none">• Mínimo de 6 caracteres• Máximo de 255 caracteres• Conter pelo menos um caractere especial• Contém um caractere maiúsculo
Password (Confirm)	Confirmação de senha,
Email Address	O endereço de email deve atender aos seguintes requisitos: <ul style="list-style-type: none">• Mínimo de 10 caracteres• Máximo de 255 caracteres
Código de idioma	O QRadar está disponível nos idiomas a seguir: inglês, chinês simplificado, chinês tradicional, japonês, coreano, francês, alemão, italiano, espanhol, russo e português (Brasil). Se um código de idioma não estiver listado, a interface com o usuário não está traduzida no idioma associado. Entretanto, outras convenções culturais associadas, como tipo de caractere, ordenação, formato de data e hora, unidade de moeda são suportadas.
Enable Popup Notifications	Selecione esta caixa de seleção se você deseja ativar as notificações do sistema pop-up a serem exibidas em sua interface com o usuário.

Acessar ajuda online

É possível acessar a Ajuda online do QRadar por meio da interface com o usuário principal do QRadar.

Para acessar a Ajuda Online, clique em **Ajuda > Conteúdo de ajuda**.

Redimensionar colunas

É possível redimensionar as colunas em várias guias no QRadar.

Coloque o ponteiro do mouse sobre a linha que separa as colunas e arraste a borda da coluna para o novo local. Você também pode redimensionar colunas dando um clique duplo na linha que separa as colunas para redimensionar automaticamente a coluna à largura do maior campo.

Nota: O redimensionamento de coluna não funciona nos navegadores da web Microsoft Internet Explorer, Versão 7.0 quando as guias estão exibindo os registros no modo de fluxo.

Configurar tamanho da página

Os usuários com privilégios administrativos podem configurar o número máximo de resultados que são exibidos nas tabelas em várias guias no QRadar.

Capítulo 3. Gerenciamento de painel

A guia **Painel** é a visualização padrão ao efetuar login.

Ele fornece um ambiente de área de trabalho no qual é possível exibir visualizações dos dados que são coletados.

Os painéis permitem que seus itens de painel sejam organizados em visualizações funcionais, que permite que você concentre em áreas específicas de sua rede.

Use a guia Painel para monitorar o comportamento do evento de segurança.

É possível customizar seu painel. O conteúdo que é exibido na guia **Painel** é específico do usuário. As alterações que são feitas em uma sessão afetam somente o seu sistema.

Para customizar sua guia **Painel**, é possível executar as seguintes tarefas:

- Incluir e remover itens do painel de seus painéis.
- Mover e posicionar itens para atender seus requisitos. Ao posicionar itens, cada item será automaticamente redimensionado proporcionalmente ao painel.
- Incluir itens do painel customizado que são baseados em algum dado.

Por exemplo, é possível incluir um item do painel que fornece um gráfico de série temporal ou um gráfico de barras que representa as 10 principais atividades de rede.

Para criar itens customizados, é possível criar as procuras salvas na guia **Atividade de log** e escolher como deseja os resultados que são representados em seu painel. Cada gráfico de painel exibe os dados atualizados em tempo real. Os gráficos de série temporal no painel são atualizados a cada 5 minutos.

Atividade de log

Os itens do painel **Atividade de log** permitirão monitorar e investigar eventos em tempo real.

Nota: Eventos ocultos ou encerrados não são incluídos nos valores que são exibidos na guia **Painel**.

Tabela 7. Itens de atividade de log

Item do painel	Descrição
Procuras de Eventos	<p>É possível exibir um item do painel customizado que é baseado em critérios de procura salvos a partir da guia Atividade de log. Itens de procura de eventos são listados no menu Incluir item > Atividade de log > Procuras de eventos. O nome do item de procura de eventos corresponde ao nome dos critérios de procura salvos nos quais o item é baseado.</p> <p>O QRadar inclui critérios de procura salvos que são pré-configurados para exibir itens de procura de evento em seu menu de guia Painel. É possível incluir mais itens de painel de procura de evento em sua guia do menu Painel. Para obter mais informações, consulte Incluindo itens de painel baseados em procura na lista Incluir itens.</p> <p>Em um item de painel Atividade de log, os resultados da procura exibem os últimos dados em tempo real em um gráfico. Os tipos de gráfico suportados são série temporal, tabela, de pizza e de barras. O tipo de gráfico padrão é de barras. Esses gráficos são configuráveis.</p> <p>Os gráficos de série temporal são interativos. É possível ampliar e verificar por meio de uma linha do tempo para investigar a atividade de log.</p>
Eventos por Gravidade	<p>O item de painel Eventos por severidade exibe o número de eventos ativos que são agrupados por severidade. Este item permitirá que você veja o número de eventos que são recebidos pelo nível de severidade designado. A severidade indica a quantidade de ameaça que uma origem de ofensa representa em relação a quão preparado está o destino para o ataque. O intervalo de severidade é 0 (baixo) a 10 (alto). Os tipos de gráficos suportados são tabela, de pizza e de barras.</p>

Tabela 7. Itens de atividade de log (continuação)

Item do painel	Descrição
Principais Fontes de Log	<p>O item de painel Principais origens de log exibe as 5 principais origens de log que enviaram eventos para o Gerenciador de log do QRadar nos últimos 5 minutos.</p> <p>O número de eventos que são enviados da origem de log especificada é indicado no gráfico de pizza. Este item permitirá visualizar alterações potenciais no comportamento, por exemplo, se uma origem de log de firewall que não esteja geralmente na lista dos 10 principais agora contribuir com uma grande porcentagem da contagem de mensagens geral, será necessário investigar esta ocorrência. Os tipos de gráficos suportados são tabela, de pizza e de barras.</p>

Relatórios mais recentes

O item de painel **Relatórios mais recentes** exibe os principais relatórios gerados recentemente.

A exibição fornece o título do relatório, a hora e a data em que o relatório foi gerado e o formato do relatório.

Resumo do sistema

O item de painel **Resumo do sistema** fornece um resumo de alto nível de atividade dentro das últimas 24 horas.

Dentro do item de resumo, você pode visualizar as seguintes informações:

- **Eventos atuais por segundo** – Exibe a taxa de eventos por segundo.
- **Novos eventos (últimas 24 horas)** – Exibe o número total de novos eventos que são recebidos nas últimas 24 horas.

Itens de gerenciamento de vulnerabilidade

Os itens do painel de Gerenciamento de Vulnerabilidade são exibidos apenas quando IBM Security QRadar Vulnerability Manager é adquirido e licenciado.

Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

É possível exibir um item do painel customizado baseado em critérios de procura salvos a partir da guia **Vulnerabilidades**. Itens de procura são listados no menu **Incluir item > Gerenciamento de vulnerabilidade > Procuras de vulnerabilidade**. O nome do item de procura corresponde ao nome dos critérios de procura salva que o item é baseado.

O QRadar inclui os critérios de procura salva padrão que são pré-configurados para exibir itens de procura no seu menu da **guia Painel**. É possível incluir mais itens de painel de procura em seu menu da **guia Painel**.

Os tipos de gráficos suportados são tabela, de pizza e de barras. O tipo de gráfico padrão é de barras. Esses gráficos são configuráveis.

Notificação do sistema

O item de painel da Notificação dos Sistemas exibe notificações de eventos que são recebidas pelo sistema.

Para notificações mostrarem no item do painel **Notificação do Sistema**, o Administrador deve criar uma regra que é baseada em cada tipo de mensagem de notificação e selecionar a caixa de seleção **Notificar** no Assistente de Regras Customizadas.

Para obter mais informações sobre como configurar notificações de eventos e criar regras de eventos, consulte o *Guia de Administração do IBM Security QRadar Log Manager*.

No item do painel **Notificações do Sistema**, você pode visualizar as seguintes informações:

- **Sinalizador** – Exibe um símbolo para indicar o nível de gravidade da notificação. Aponte para o símbolo para visualizar mais detalhes sobre o nível de gravidade.
 - Ícone **Saúde**
 - Ícone **Informações** (?)
 - Ícone **Erros** (X)
 - Ícone **Aviso** (!)
- **Criado** – Exibe a quantidade de tempo decorrido desde que a notificação foi criada.
- **Descrição** – Exibe informações sobre a notificação.
- **Ícone descartar** (x) – Permitirá que você feche uma notificação do sistema.

Você pode passar o mouse sobre uma notificação para visualizar mais detalhes:

- **IP do host** – Exibe o endereço IP do host que originou a notificação.
- **Gravidade** – Exibe o nível de gravidade do incidente que criou esta notificação.
- **Categoria de baixo nível** – Exibe a categoria de nível inferior que está associada ao incidente que gerou esta notificação. Por exemplo: Interrupção de Serviço.
- **Carga útil** – Exibe o conteúdo de carga útil que está associado ao incidente que gerou esta notificação.
- **Criado** – Exibe a quantidade de tempo decorrido desde que a notificação foi criada.

Quando você inclui o item do painel **Notificações do sistema**, as notificações do sistema também podem exibir como notificações pop-up na interface com o usuário QRadar. Estas notificações pop-up são exibidas no canto inferior direito da interface com o usuário, independente da guia selecionada.

Notificações pop-ups estão disponíveis apenas para usuários com permissões administrativas e são ativadas por padrão. Para desativar notificações pop-up, selecione **Preferências do usuário** e desmarque a caixa de seleção **Ativar notificações pop-up**.

Na janela pop-up Notificações do sistema, o número de notificações na fila é destacado. Por exemplo, se (1 – 12) for exibido no cabeçalho, a notificação atual será 1 de 12 notificações a serem exibidas.

A janela pop-up notificação do sistema fornece as seguintes opções:

- **Ícone avançar (>)** – Exibe a próxima mensagem de notificação. Por exemplo, se a mensagem de notificação atual for 3 de 6, clique no ícone para visualizar 4 de 6.
- **Ícone fechar (X)** – Fecha essa janela pop-up de notificação.
- **(detalhes)** - Exibe mais informações sobre essa notificação do sistema.

Incluindo itens do painel

Você pode incluir vários itens do painel para sua guia de Painel.

Procedimento

1. Clique na guia **Painel**.
2. Na barra de ferramentas, clique em **Incluir item**.
3. Selecione o item que você deseja incluir. Consulte itens do painel Disponível.

Usando o painel para investigar a atividade de log

Itens de painel baseados em procura fornecem um link para a guia **Atividade de log**, permitindo que você investigue a atividade de log mais a fundo.

Sobre Esta Tarefa

Para investigar os fluxos um item de painel de **Atividade de log**:

1. Clique no link **Visualizar na atividade de log**. A guia **Atividade de log** é exibida, exibindo resultados e dois gráficos que correspondem aos parâmetros de seu item de painel.

Os tipos de gráficos que são exibidos na guia de **Atividade de log** dependem de qual gráfico está configurado no item de painel:

Tipo de gráfico	Descrição
Barra, Pizza e Tabela	A guia de Atividade de log exibe um gráfico de barras, gráfico de pizza e tabela de detalhes.
Séries temporais	A guia Atividade de log exibe gráficos de acordo com os seguintes critérios: <ol style="list-style-type: none">1. Se o seu intervalo de tempo for menor ou igual a 1 hora, um gráfico de série temporal, um gráfico de barras e uma tabela de detalhes do evento serão exibidos.2. Se o seu intervalo de tempo for mais de 1 hora, um gráfico de série temporal será exibido e você será solicitado a clicar em Atualizar Detalhes. Esta ação inicia a procura que preenche os detalhes do evento e gera o gráfico de barras. Quando a procura é concluída, o gráfico de barras e a tabela de detalhes do evento são exibidos.

Configurando gráficos

Você pode configurar itens do painel de **Atividade de log**, **Rede de atividade** e **Conexões** (se aplicável) para especificar o tipo de gráfico e quantos objetos de dados que você deseja visualizar.

Sobre Esta Tarefa

Tabela 8. Configurando gráficos. Opções de parâmetros.

opção	descrição
Value to Graph	Na caixa de listagem, selecione o tipo de objeto que você deseja para o gráfico no gráfico. As opções incluem todos os eventos normalizados e customizados ou parâmetros de fluxo incluídos em seus parâmetros de procura.
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico que você deseja visualizar. As opções incluem: <ol style="list-style-type: none">1. Gráfico de barras – Exibe dados em um gráfico de barras. Essa opção está disponível somente para eventos agrupados.2. Gráfico de pizza – Exibe dados em um gráfico de pizza. Essa opção está disponível somente para eventos agrupados.3. Tabela - Exibe dados em uma tabela. Essa opção está disponível somente para eventos agrupados.4. Séries Temporais – Exibe um gráfico de linha interativa que representa os registros que são correspondidos por um intervalo de tempo especificado.
Display Top	Na caixa de listagem, selecione o número de objetos que você deseja visualizar no gráfico. As opções incluem 5 e 10 . O padrão é 10 .
Capture Time Series Data	Selecione essa caixa de seleção para ativar a captura de série temporal. Ao selecionar essa caixa de seleção, o recurso do gráfico começa a acumular dados para gráficos de série temporal. Por padrão, essa opção está desativada.
Time Range	Na caixa de listagem, selecione o intervalo de tempo que você deseja visualizar.

As configurações de gráfico customizado são retidas, para que sejam exibidos como configurado cada vez que você acessar a guia **Painel**.

O Gerenciador de Log do QRadar coleta os dados de modo que, quando você executar uma procura salva de série temporal, haverá um cache de dados do evento ou fluxo disponível para exibir os dados para o período de tempo anterior. Parâmetros acumulados são indicados por um asterisco (*) na caixa de listagem **Valor para gráfico**. Se você selecionar um valor para o gráfico que não estiver acumulado (sem asterisco), dados de série temporal não ficarão disponíveis.

Procedimento

1. Clique na guia de **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel que contém o item que você deseja customizar.
3. No cabeçalho do item de painel que você deseja configurar, clique no ícone **Configurações**.
4. Configure os parâmetros de gráfico que estão descritos na Tabela 1.

Removendo itens do painel

Você pode remover itens de um painel e incluir o item novamente a qualquer momento.

Sobre Esta Tarefa

Ao remover um item do painel, o item não será removido completamente.

Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel do qual você deseja remover um item.
3. No cabeçalho de item do painel, clique no ícone vermelho [x] para remover o item do painel.

Removendo um item do painel

É possível remover um item de seu painel e exibi-lo em uma nova janela em seu sistema da área de trabalho.

Sobre Esta Tarefa

Ao remover um item do painel, o item do painel original permanecerá na guia **Painel**, enquanto uma janela separada com um item do painel duplicado permanecerá aberta e se atualizará durante os intervalos planejados. Se você fechar o aplicativo do QRadar, a janela separada permanecerá aberta para monitoramento e continuará a atualizar até que você feche a janela manualmente ou encerre o sistema de computador.

Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel a partir do qual você deseja remover um item.
3. No cabeçalho de item do painel, clique no ícone verde para remover o item do painel e abri-o em uma janela separada.

Renomeando um painel

Você pode renomear um painel e atualizar a descrição.

Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel que você deseja editar.

3. Na barra de ferramentas, clique no ícone **Renomear painel**.
4. No campo **Nome**, digite um novo nome para o painel. O comprimento máximo é de 65 caracteres.
5. No campo **Descrição**, insira uma nova descrição do painel. O comprimento máximo é de 255 caracteres
6. Clique em **OK**.

Excluindo um painel

Você pode excluir um painel.

Sobre Esta Tarefa

Após excluir um painel, a guia **Painel** será atualizada e o primeiro painel listado na caixa de listagem **Mostrar painel** será exibido. O painel que você excluiu não será mais exibido na caixa de listagem **Mostrar painel**.

Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel que você deseja excluir.
3. Na barra de ferramentas, clique em **Excluir painel**.
4. Clique em **Sim**.

Gerenciando notificações do sistema

Você pode especificar o número de notificações que você deseja exibir em seu item do painel **Notificação do sistema** e fechar as notificações do sistema após lê-las.

Antes de Iniciar

Assegure-se de que o item do painel **Notificação do sistema** esteja incluído em seu painel.

Procedimento

1. No cabeçalho de item do painel **Notificação do sistema**, clique no ícone **Configurações**.
2. Na caixa de listagem **Exibir**, selecione o número de notificações do sistema que você deseja visualizar.
 - As opções são **5**, **10** (padrão), **20**, **50** e **Todos**.
 - Para visualizar todas as notificações do sistema efetuadas login nas últimas 24 horas, clique em **Todos**.
3. Para fechar uma notificação do sistema, clique no ícone **Excluir**.

Incluindo itens baseados em painel para a lista Incluir Itens

Você pode incluir itens de painel baseados em procura para seu menu **Incluir itens**.

Antes de Iniciar

Para incluir um item de painel de eventos ao menu **Incluir item** na guia **Painel**, você deve acessar a guia **Atividade de log** para criar critérios de procura que especifica que os resultados da procura podem ser exibidos na guia **Painel**. O

critério de procura também deve especificar que os resultados são agrupados em um parâmetro.

Sobre Esta Tarefa

Este procedimento se aplica a todos os itens de painel baseados em procura, incluindo itens de painel IBM Security QRadar Risk Manager. Os itens de painel do QRadar Risk Manager são exibidos somente quando o QRadar Risk Manager foi comprado e licenciado e você estabeleceu a conexão entre o Console e o dispositivo QRadar Risk Manager. Para obter informações adicionais consulte *Guia do Usuário do IBM Security QRadar Risk Manager*

Procedimento

1. Escolha:
 - Para incluir um item de painel de procura de evento, clique na guia **Atividade de log**.
2. Na caixa de listagem **Procurar**, escolha uma das seguintes opções:
 - Para criar uma procura, selecione **Novo procura**.
 - Para editar uma procura salva, selecione **Editar procura**.
3. Configure ou edite seus parâmetros de procura, conforme necessário.
 - Na área de janela Editar Procura, selecione a opção **Incluir em meu painel**.
 - Na área de janela Definição de Coluna, selecione uma coluna e clique no ícone **Incluir coluna** para mover a coluna para a lista **Grupo**.
4. Clique em **Filtrar**. Os resultados da procura são exibidos.
5. Clique em **Salvar critérios**. Consulte Salvando critérios de procura na guia Ofensa
6. Clique em **OK**.
7. Verifique se seus critérios de procura salva com êxito incluídos ao item de painel de procura de evento ou fluxo para a lista **Incluir itens**
8. Clique na guia **Painel**.
9. Para verificar um item de procura de eventos, selecione **Incluir item > Atividade de log > Procuras de eventos > Incluir item**

Capítulo 4. Investigação de atividade de log

É possível monitorar e investigar a atividade de log (eventos) em tempo real ou executar procuras avançadas.

Usando a guia **Atividade de log**, é possível monitorar e investigar a atividade de log (eventos) em tempo real ou executar procuras avançadas.

Visão geral da guia Atividade de log

Um evento é um registro a partir de uma fonte de log, como um dispositivo de firewall ou roteador, que descreve uma ação em uma rede ou host.

Deve-se ter permissão para visualizar a guia **Atividade de log**.

Barra de ferramentas da guia Atividade de log

É possível acessar várias opções na barra de ferramentas Atividade de log

Usando a barra de ferramentas, é possível acessar as seguintes opções:

Tabela 9. Opções da barra de ferramentas Atividade de log

Opção	Descrição
Procurar	Clique em Procurar para executar procuras avançadas em eventos. As opções incluem: <ul style="list-style-type: none">• Nova procura – Selecione esta opção para criar uma nova procura de evento.• Editar procura – Selecione esta opção para selecionar e editar uma procura de evento.• Gerenciar resultados da procura – Selecione esta opção para visualizar e gerenciar resultados da procura.
Procuras Rápidas	Nessa caixa de listagem, é possível executar procuras salvas anteriormente. As opções são exibidas na caixa de listagem Procuras rápidas apenas quando tiver salvado os critérios de procura que especificam a opção Incluir em minhas procuras rápidas .
Incluir filtro	Clique em Incluir filtro para incluir um filtro aos resultados da procura atual.
Salvar critérios	Clique em Salvar critérios para salvar os critérios de procura atuais.
Salvar resultados	Clique em Salvar resultados para salvar os resultados da procura atual. Essa opção será exibida somente após uma procura ser concluída. Esta opção está desativada no modo de fluxo.
Cancelar	Clique em Cancelar para cancelar uma procura em andamento. Esta opção está desativada no modo de fluxo.

Tabela 9. Opções da barra de ferramentas Atividade de log (continuação)

Opção	Descrição
Regras	<p>A opção Regras será visível somente se tiver permissão para visualizar as regras.</p> <p>Clique em Regras para configurar as regras de evento customizado. As opções incluem:</p> <ul style="list-style-type: none"> • Regras – Selecione esta opção para visualizar ou criar uma regra. Se tiver somente a permissão para visualizar as regras, a página de resumo do assistente de regras será exibida. Se tiver a permissão para manter as regras customizadas, o assistente de regras será exibido e será possível editar a regra. Para ativar as opções de regra de detecção de anomalias (Incluir limite de regra, Incluir regra comportamental e Incluir regra de anomalia), é necessário salvar os critérios de procura agregados, pois os critérios da procura salva especificam os parâmetros requeridos. <p>Nota: As opções de regra de detecção de anomalias são visíveis apenas se tiver a permissão Atividade de log > Manter regras customizadas.</p> <ul style="list-style-type: none"> • Incluir regra de limite – Selecione esta opção para criar uma regra de limite. Uma regra de limite testa o tráfego de evento para atividade que excede um limite configurado. Os limites podem ser baseados em quaisquer dados que são coletados pelo QRadar. Por exemplo, se criar uma regra de limite indicando que não mais de 220 clientes podem efetuar login no servidor entre às 8h e 17h, as regras gerarão um alerta quando o 221º cliente tentar efetuar login. <p>Ao selecionar a opção Incluir regra de limite, o assistente Regras será exibido e preenchido previamente com as opções apropriadas para criar uma regra de limite.</p>

Tabela 9. Opções da barra de ferramentas Atividade de log (continuação)

Opção	Descrição
Regras (continuação)	<ul style="list-style-type: none"> <li data-bbox="959 262 1453 850"> <p>• Incluir regra comportamental – Selecione esta opção para criar uma regra comportamental. Uma regra comportamental testa o tráfego de evento por atividade anormal, como a existência de tráfego novo ou desconhecido, que é o tráfego que para subitamente ou uma alteração de porcentagem na quantidade de tempo que um objeto está ativo. Por exemplo, é possível criar uma regra comportamental para comparar o volume médio de tráfego dos últimos 5 minutos com o volume médio de tráfego da última hora. Se houver uma alteração maior do que 40%, a regra gerará uma resposta.</p> <p>Ao selecionar a opção Incluir regra comportamental, o assistente de regras é exibido e preenchido previamente com as opções apropriadas para criar uma regra comportamental.</p> <li data-bbox="959 850 1453 1394"> <p>• Incluir regra de anomalia – Selecione esta opção para criar uma regra de anomalia. Uma regra de anomalia testa o tráfego de evento por atividade anormal, como a existência de tráfego novo ou desconhecido, que é o tráfego que para subitamente ou uma alteração de porcentagem na quantidade de tempo que um objeto está ativo. Por exemplo, se uma área de sua rede que nunca se comunica com a Ásia iniciar uma comunicação com os hosts nesse país, uma regra de anomalia gerará um alerta.</p> <p>Ao selecionar a opção Incluir regra de anomalia, o assistente de regras será exibido e preenchido previamente com as opções apropriadas para criar uma regra de anomalias.</p>

Tabela 9. Opções da barra de ferramentas Atividade de log (continuação)

Opção	Descrição
Ações	<p>Clique em Ações para executar as seguintes ações:</p> <ul style="list-style-type: none"> • Mostrar todos – Selecione esta opção para remover todos os filtros nos critérios de procura e exibir todos os eventos não filtrados. • Imprimir – Selecione esta opção para imprimir os eventos que são exibidos na página. • Exportar para XML > Colunas visíveis – Selecione esta opção para exportar somente as colunas que estão visíveis na guia Atividade de log. Essa é a opção recomendada. Consulte Exportando eventos. • Exportar para XML > Exportação integral (todas as colunas) – Selecione esta opção para exportar todos os parâmetros de eventos. Uma exportação integral pode demorar um longo período de tempo para ser concluída. Consulte Exportando eventos. • Exportar para CSV > Colunas Visíveis - Selecione essa opção para exportar apenas as colunas visíveis na guia Atividade de log. Essa é a opção recomendada. Consulte Exportando eventos. • Exportar para CSV > Exportação integral (todas as colunas) – Selecione esta opção para exportar todos os parâmetros de eventos. Uma exportação integral pode demorar um longo período de tempo para ser concluída. Consulte Exportando eventos. • Excluir – Selecione esta opção para excluir um resultado da procura. Consulte Gerenciando resultados da procura de fluxo e de evento. • Notificar – Selecione esta opção para especificar que deseja que seja enviada uma notificação por email na conclusão das procuras selecionadas. Essa opção está ativada apenas para procuras em andamento. <p>Nota: As opções Imprimir, Exportar para XML e Exportar para CSV estão desativadas no modo de fluxo e ao visualizar resultados parciais de procura.</p>

Tabela 9. Opções da barra de ferramentas Atividade de log (continuação)

Opção	Descrição
Filtro rápido	<p>Digite seus critérios de procura no campo Filtro rápido e clique no ícone Filtro rápido ou pressione Enter no teclado. Todos os eventos que correspondem aos seus critérios de procura são exibidos na lista de eventos. Uma procura de texto é executada na carga útil do evento para determinar quais correspondem aos critérios especificados.</p> <p>Nota: Ao clicar no campo Filtro rápido, uma dica de ferramenta será exibida, fornecendo informações sobre a sintaxe apropriada a ser usada para o critério de procura. Para obter mais informações de sintaxe, consulte Sintaxe de filtro rápido.</p>

Sintaxe de filtro rápido

O recurso Filtro rápido permitirá que pesquise as cargas úteis de eventos usando uma cadeia de procura de texto.

A funcionalidade Filtro Rápido está disponível nos seguintes locais na interface com o usuário:

- Barra de ferramentas **Atividade de log** - Na barra de ferramentas, um campo **Filtro rápido** permitirá que digite uma cadeia de procura de texto e clique no ícone **Filtro rápido** para aplicar seu filtro rápido na lista atualmente exibida de eventos.
- Caixa de diálogo **Incluir filtro**. Na caixa de diálogo **Incluir filtro**, que é acessada clicando no ícone **Incluir filtro** na guia **Atividade de log**, é possível selecionar **Quick Filter** como seu parâmetro de filtragem e digitar uma cadeia de procura de texto. Isso permitirá aplicar o filtro rápido na lista atualmente exibida de eventos. Para obter mais informações sobre a caixa de diálogo **Incluir filtro**, consulte Sintaxe de filtro rápido.
- Página Procura de evento - Na página de procura de eventos, é possível incluir um **Filtro rápido** na sua lista de filtros a serem incluídos em seus critérios de procura. Para obter mais informações sobre como configurar critérios de procura, consulte Procurando fluxos ou eventos.

Ao visualizar eventos em tempo real (fluxo) ou no último modo de intervalo, será possível digitar apenas palavras ou frases simples no campo **Filtro rápido**. Ao visualizar eventos usando um intervalo de tempo, use as seguintes diretrizes de sintaxe para digitar seus critérios de procura de texto:

- Os termos de procura podem incluir qualquer texto simples que espera encontrar na carga útil. Por exemplo, "Firewall"
- Incluir vários termos entre aspas duplas para indicar que deseja procurar a frase exata. Por exemplo, "Firewall deny"
- Os termos de procura podem incluir curingas de caracteres únicos e múltiplos. O termo de procura não pode começar com um curinga. Por exemplo, "F?rewall" ou "F??ew*"
- Os termos de procura são combinados em sequência a partir do primeiro caractere na palavra ou frase da carga útil. Por exemplo, o termo de procura "user" não corresponde à frase a seguir: "ruser", "myuser" ou "anyuser". O termo de procura "user*" não corresponde a nenhuma palavra que começa com "user", por exemplo, "user_1", "user_2".

- Agrupa termos usando expressões lógicas, como AND, OR e NOT. A sintaxe faz distinção entre maiúsculas e minúsculas e os operadores devem estar em letras maiúsculas para serem reconhecidos como expressões lógicas e não como termos de procura. Por exemplo: (%PIX* AND ("URL Acessada" OR "Negação udp src") AND 10.100.100.*) Ao criar critérios de procura que incluem a expressão lógica NOT, será necessário incluir pelo menos um outro tipo de expressão lógica, caso contrário, o filtro não retornará nenhum resultado. Por exemplo: (%PIX* AND ("URL Acessada" OR "Negação udp src") NOT 10.100.100.*)
- Os seguintes caracteres devem ser precedidos por uma barra invertida para indicar que o caractere é parte de seu termo de procura: - && | | ! () { } [] ^ " ~ * ? : \. Por exemplo: "%PIX\ -5\ -304001"

Opções de menu ativado pelo botão direito

Na guia **Atividade de log**, é possível clicar com o botão direito em um evento para acessar mais informações sobre o filtro de eventos.

As opções do menu ativado pelo botão direito são:

Tabela 10. Opções de menu ativado pelo botão direito

Opção	Descrição
Filtrar em	Selecione esta opção para filtrar no evento selecionado, dependendo do parâmetro selecionado no evento.
Mais opções:	Selecione esta opção para investigar um endereço IP ou um nome de usuário. Para obter mais informações sobre como investigar um endereço IP, consulte Investigando endereços IP. Para obter mais informações sobre como investigar um nome de usuário, consulte Investigando nomes de usuário. Nota: Esta opção não é exibida no modo de fluxo.

Barra de status

Durante o fluxo de eventos, a barra de status exibe o número médio dos resultados recebidos por segundo.

Este é o número de resultados que o Console recebeu com sucesso a partir dos processadores de eventos. Se o número for maior que 40 resultados por segundo, apenas 40 resultados serão exibidos. O restante é acumulado no buffer de resultado. Para visualizar mais informações de status, mova o ponteiro do mouse sobre a barra de status.

Quando os eventos não estão em fluxo, a barra de status exibe o número dos resultados da procura atualmente exibidos na guia e a quantidade de tempo necessária para processar os resultados da procura.

Monitorando a atividade de log

Por padrão, a guia **Atividade de log** exibe eventos no modo de fluxo, que permite visualizar os eventos em tempo real.

Para obter mais informações sobre o modo de fluxo, consulte Visualizando eventos de fluxo. É possível especificar um intervalo de tempo diferente para filtrar eventos usando a caixa de listagem **Visualização**.

Se os critérios de procura salvos forem configurados anteriormente como o padrão, os resultados dessa procura serão exibidos automaticamente ao acessar a guia **Atividade de log**. Para obter mais informações sobre como salvar os critérios de procura, consulte Salvando critérios de procura de fluxo e de evento.

Visualizando eventos de fluxo

O modo de fluxo permitirá que você visualize os dados do evento inseridos no seu sistema. Este modo fornece a você uma visualização em tempo real do seu evento de atividade atual, exibindo os últimos 50 eventos.

Sobre Esta Tarefa

Se você aplicar quaisquer filtros na guia **Atividade de Log** ou em seu critério de procura antes de ativar o modo de fluxo, os filtros serão mantidos em modo de fluxo. No entanto, o modo de fluxo não suporta procuras que incluem eventos agrupados. Se você ativar o modo de fluxo de eventos agrupados ou o critério de procura agrupado, a guia **Atividade de Log** exibirá os eventos normalizados. Consulte Visualizando eventos normalizados.

Quando você deseja selecionar um evento para visualizar detalhes ou executar uma ação, você deve pausar o fluxo antes de clicar duas vezes em um evento. Quando o fluxo é pausado, os últimos 1.000 eventos são exibidos.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Visualização**, selecione **Tempo real (fluxo)**. Para obter informações sobre as opções da barra de ferramentas, consulte a Tabela 4-1. Para obter mais informações sobre os parâmetros exibidos no modo de fluxo, consulte a Tabela 4-7.
3. Opcional. Pausar ou executar o fluxo de eventos. Escolha uma das opções a seguir:
 - Para selecionar um registro de eventos, clique no ícone **Pausar** para pausar o fluxo.
 - Para reiniciar o modo de fluxo, clique no ícone **Executar**.

Visualizando eventos normalizados

Os eventos são coletados em formato bruto, e então normalizados para exibição na guia **Atividade de Log**.

Sobre Esta Tarefa

A normalização envolve a análise de dados de evento brutos e a preparação dos dados para exibir informações legíveis sobre a guia. Quando os eventos são normalizados, o sistema normaliza os nomes também. Portanto, o nome exibido na guia **Atividade de Log** pode não corresponder ao nome exibido no evento.

Nota: Se você selecionou um prazo para exibição, um gráfico de série temporal será exibido. Para obter mais informações sobre como usar gráficos de série temporal, consulte visão geral do gráfico de série temporal.

A guia **Atividade de Log** exibe os seguintes parâmetros quando você visualiza os eventos normalizados:

Tabela 11. Guia de atividade de log – Parâmetro padrão (normalizado)

Parâmetro	Descrição
Filtros Atuais	A parte superior da tabela exibe os detalhes dos filtros aplicados aos resultados da procura. Para limpar esses valores de filtro, clique em Limpar filtro . Nota: Esse parâmetro só será exibido após você aplicar um filtro.
Visualização	Nesta caixa de listagem, você pode selecionar o intervalo de tempo que você deseja filtrar.
Current Statistics	Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo: Nota: Clique na seta ao lado de Estatísticas atuais para exibir ou ocultar as estatísticas. <ul style="list-style-type: none"> • Resultados totais – Especifica o número total de resultados que correspondeu ao seu critério de procura. • Arquivos de dados procurados – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado. • Arquivos de dados compactados procurados – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado. • Contagem de arquivo de índice – Especifica o número total de arquivos de índice procurado durante o período de tempo especificado. • Duração – Especifica a duração da procura. Nota: Estatísticas atuais são úteis para resolução de problemas. Quando contatar o Suporte ao Cliente para solucionar problemas de eventos, você poderá ser solicitado a fornecer informações da estatística atual.

Tabela 11. Guia de atividade de log – Parâmetro padrão (normalizado) (continuação)

Parâmetro	Descrição
Charts	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em Ocultar gráficos se deseja remover os gráficos de sua exibição. Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. Para obter mais informações sobre a configuração de gráficos, consulte Capacidade de gerenciamento do gráfico. Nota: Se você usar o Mozilla Firefox como seu navegador e uma extensão do navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para gráficos exibidos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.
Ícone ofensas	Clique neste ícone para visualizar detalhes da ofensa associada a este evento. Para obter mais informações, consulte Capacidade de gerenciamento do gráfico. Nota: Dependendo do seu produto, esse ícone pode não estar disponível. Você deve ter o IBM Security QRadar SIEM.
Start Time	Especifica a hora do primeiro evento, conforme reportado para QRadar pela origem de log.
Nome do evento	Especifica o nome normalizado do evento.
Origem de Log	Especifica a origem de log que originou o evento. Se houver várias fontes de log associadas a esse evento, este campo especificará o termo Várias e o número de fontes de log.
Contagem de eventos	Especifica o número total de eventos empacotados neste evento normalizado. Os eventos são empacotados quando vários eventos do mesmo tipo para o mesmo endereço IP de origem e destino são detectados dentro de um curto período.
Time	Especifica a data e hora em que o QRadar recebeu o evento.
Categoria de Baixo Nível	Especifica a categoria de baixo nível associada a este evento. Para obter mais informações sobre as categorias de eventos, consulte o <i>Guia de Administração do IBM Security QRadar Log Manager</i> .
IP de Origem	Especifica o endereço IP de origem do evento.
Porta de origem	Especifica a porta de origem do evento.

Tabela 11. Guia de atividade de log – Parâmetro padrão (normalizado) (continuação)

Parâmetro	Descrição
IP de destino	Especifica o endereço IP de destino do evento.
Porta de destino	Especifica a porta de destino do evento.
Nome de usuário	Especifica o nome de usuário associado a este evento. Os nomes de usuário estão frequentemente disponíveis em eventos de autenticação relacionada. Para todos os outros tipos de eventos onde o nome de usuário não estiver disponível, este campo especificará N/D.
Magnitude	Especifica a magnitude deste evento. Variáveis incluem credibilidade, relevância e gravidade. Passe o mouse sobre a barra de magnitude para exibir os valores e a magnitude calculada. Para obter mais informações sobre a credibilidade, relevância e gravidade, consulte o Glossário.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Exibir**, selecione **Padrão (normalizado)**.
3. Na caixa de listagem **Visualização**, selecione o prazo que você deseja exibir.
4. Clique no ícone **Pausar** para pausar o fluxo.
5. Clique duas vezes no evento que deseja exibir com mais detalhes. Para obter mais informações, consulte Detalhes do evento.

Visualizando eventos brutos

Você pode visualizar dados do evento bruto, que são os dados do evento não analisados do registro de origem.

Sobre Esta Tarefa

Quando você visualiza dados dos eventos brutos, a guia **Atividade de Log** fornece os seguintes parâmetros para cada evento.

Tabela 12. Parâmetros de evento bruto

Parâmetro	Descrição
Filtros Atuais	A parte superior da tabela exibe os detalhes dos filtros aplicados aos resultados da procura. Para limpar esses valores de filtro, clique em Limpar filtro . Nota: Esse parâmetro só será exibido após você aplicar um filtro.
Visualização	Nesta caixa de listagem, você pode selecionar o intervalo de tempo que você deseja filtrar.

Tabela 12. Parâmetros de evento bruto (continuação)

Parâmetro	Descrição
Current Statistics	<p>Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo:</p> <p>Nota: Clique na seta ao lado de Estatísticas atuais para exibir ou ocultar as estatísticas.</p> <ul style="list-style-type: none"> • Resultados totais – Especifica o número total de resultados que correspondeu ao seu critério de procura. • Arquivos de dados procurados – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado. • Arquivos de dados compactados procurados – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado. • Contagem de arquivo de índice – Especifica o número total de arquivos de índice procurado durante o período de tempo especificado. • Duração – Especifica a duração da procura. <p>Nota: As estatísticas Atuais são úteis para a resolução de problemas. Quando contatar o Suporte ao Cliente para solucionar problemas de eventos, você poderá ser solicitado a fornecer informações da estatística atual.</p>
Charts	<p>Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em Ocultar gráficos se deseja remover os gráficos de sua exibição. Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida.</p> <p>Nota: Se você usar o Mozilla Firefox como seu navegador e uma extensão do navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para gráficos exibidos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.</p>
Start Time	<p>Especifica a hora do primeiro evento, conforme reportado para QRadar pela origem de log.</p>

Tabela 12. Parâmetros de evento bruto (continuação)

Parâmetro	Descrição
Origem de Log	Especifica a origem de log que originou o evento. Se houver várias fontes de log associadas a esse evento, este campo especificará o termo Várias e o número de fontes de log.
Payload	Especifica as informações de carga útil do evento original no formato UTF-8.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Exibir**, selecione **Eventos brutos**.
3. Na caixa de listagem **Visualização**, selecione o prazo que você deseja exibir.
4. Clique duas vezes no evento que deseja exibir com mais detalhes. Consulte Detalhes do evento.

Visualizando eventos agrupados

Usando a guia **Atividade de Log**, você pode visualizar os eventos agrupados por várias opções. Na caixa de listagem **Exibir**, você pode selecionar o parâmetro que deseja para os eventos do grupo.

Sobre Esta Tarefa

A caixa de lista de Exibição não é exibida no modo de fluxo porque o modo de fluxo não suporta eventos agrupados. Se você inseriu o modo de fluxo usando o critério de procura não agrupada, esta opção será exibida.

A caixa de lista de Exibição fornece as opções a seguir:

Tabela 13. Opções de eventos agrupados

Opção de grupo	Descrição
Categoria de Baixo Nível	Exibe uma lista resumida dos eventos agrupados pela categoria de baixo nível do evento.
Nome do evento	Exibe uma lista resumida dos eventos agrupados pelo nome normalizado do evento.
IP de destino	Exibe uma lista resumida dos eventos agrupados pelo endereço IP de destino do evento.
Porta de destino	Exibe uma lista resumida dos eventos agrupados pelo endereço de porta de destino do evento.
IP de Origem	Exibe uma lista resumida dos eventos agrupados pelo endereço IP de origem do evento.
Regra customizada	Exibe uma lista resumida dos eventos agrupados pela regra customizada associada.

Tabela 13. Opções de eventos agrupados (continuação)

Opção de grupo	Descrição
Nome de usuário	Exibe uma lista resumida dos eventos agrupados pelo nome de usuário associado ao evento.
Origem de Log	Exibe uma lista resumida dos eventos agrupados pelas origens de log que enviaram o evento para QRadar.
Categoria de Alto Nível	Exibe uma lista resumida dos eventos agrupados pela categoria de alto nível do evento.
Rede	Exibe uma lista resumida dos eventos agrupados pela rede associada ao evento.
Porta de origem	Exibe uma lista resumida dos eventos agrupados pelo endereço de porta de origem do evento.

Depois de selecionar uma opção na caixa de listagem **Exibir**, o layout da coluna dos dados dependerá da opção do grupo escolhido. Cada linha na tabela de eventos representa um grupo de eventos. A guia **Atividade de Log** fornece as seguintes informações para cada grupo de eventos.

Tabela 14. Parâmetros de eventos agrupados

Parâmetro	Descrição
Grouping By	Especifica o parâmetro no qual a procura é agrupada.
Filtros Atuais	A parte superior da tabela exibe os detalhes do filtro aplicado aos resultados da procura. Para limpar esses valores de filtro, clique em Limpar filtro .
Visualização	Na caixa de listagem, selecione o intervalo de tempo que você deseja filtrar.

Tabela 14. Parâmetros de eventos agrupados (continuação)

Parâmetro	Descrição
Current Statistics	<p>Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo:</p> <p>Nota: Clique na seta ao lado de Estatísticas atuais para exibir ou ocultar as estatísticas.</p> <ul style="list-style-type: none"> • Resultados totais – Especifica o número total de resultados que correspondeu ao seu critério de procura. • Arquivos de dados procurados – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado. • Arquivos de dados compactados procurados – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado. • Contagem de arquivo de índice – Especifica o número total de arquivos de índice procurado durante o período de tempo especificado. • Duração – Especifica a duração da procura. <p>Nota: As estatísticas Atuais são úteis para a resolução de problemas. Quando você contata o Suporte ao Cliente para resolver eventos, você pode ser solicitado a fornecer informações de estatística atuais.</p>

Tabela 14. Parâmetros de eventos agrupados (continuação)

Parâmetro	Descrição
Charts	<p>Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em Ocultar gráficos se deseja remover o gráfico de sua exibição.</p> <p>Cada gráfico fornece uma legenda, que é uma referência visual para ajudá-lo a associar os objetos de gráfico aos parâmetros que eles representam. Usando o recurso legenda, é possível executar as seguintes ações:</p> <ul style="list-style-type: none"> • Mova o ponteiro do mouse sobre um item de legenda para visualizar mais informações sobre os parâmetros que ele representa. • Clique com o botão direito no item de legenda para investigar melhor o item. • Clique em um item de legenda para ocultar os itens no gráfico. Clique no item de legenda novamente para mostrar o item oculto. É possível também clicar no item do gráfico correspondente para ocultar e mostrar o item. • Clique em Legenda se deseja remover a legenda da exibição do gráfico. <p>Nota: Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida.</p> <p>Nota: Se você usar o Mozilla Firefox como seu navegador e uma extensão do navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para exibir gráficos, você deverá remover a extensão de navegador bloqueadora de anúncio. Para obter mais informações, consulte a documentação do navegador.</p>
Source IP (Unique Count)	Especifica o endereço IP de origem associado a esse evento. Se houver vários endereços IP associados a este evento, este campo especificará o termo Vários e o número de endereços IP.
Destination IP (Unique Count)	Especifica o endereço IP de destino associado a este evento. Se houver vários endereços IP associados a este evento, este campo especificará o termo Vários e o número de endereços IP.
Destination Port (Unique Count)	Especifica as portas de destino associadas a este evento. Se houver várias portas associadas a este evento, este campo especificará o termo Várias e o número de portas.
Nome do evento	Especifica o nome normalizado do evento.

Tabela 14. Parâmetros de eventos agrupados (continuação)

Parâmetro	Descrição
Log Source (Unique Count)	Especifica as origens de log que enviou o evento para QRadar. Se houver várias fontes de log associadas a esse evento, este campo especificará o termo Várias e o número de fontes de log.
High Level Category (Unique Count)	Especifica a categoria de alto nível deste evento. Se houver várias categorias associadas a este evento, este campo especificará o termo Várias e o número de categorias. Para obter mais informações sobre categorias, consulte o <i>Guia de Administração do IBM Security QRadar Log Manager</i> .
Low Level Category (Unique Count)	Especifica a categoria de nível inferior deste evento. Se houver várias categorias associadas a este evento, este campo especificará o termo Várias e o número de categorias.
Protocol (Unique Count)	Especifica o ID do protocolo associado a este evento. Se houver vários protocolos associados a este evento, este campo especificará o termo Vários e o número de IDs de protocolo.
Username (Unique Count)	Especifica o nome de usuário associado a este evento, se disponível. Se houver vários nomes de usuários associados a este evento, este campo especificará o termo Vários e o número de nomes de usuários.
Magnitude (Maximum)	Especifica a magnitude máxima calculada para eventos agrupados. As variáveis usadas para calcular a magnitude incluem credibilidade, relevância e gravidade. Para obter mais informações sobre a credibilidade, relevância e gravidade, consulte o Glossário.
Event Count (Sum)	Especifica o número total de eventos empacotados neste evento normalizado. Os eventos são empacotados quando vários eventos do mesmo tipo, para o mesmo endereço IP de origem e destino, são vistos dentro de um curto período.
Count	Especifica o número total de eventos normalizados com este grupo de eventos.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Visualização**, selecione o prazo que você deseja exibir.
3. Na caixa de lista de Exibição, escolha em qual parâmetro você deseja agrupar eventos. Consulte a Tabela 2. Os grupos de eventos são listados. Para obter mais informações sobre os detalhes do grupo de eventos. Consulte a Tabela 1.

4. Para visualizar a página Lista de eventos para um grupo, clique duas vezes no grupo de eventos que você deseja investigar. A página Lista de eventos não retém as configurações de gráfico que você pode ter definido na guia **Atividade de Log**. Para obter mais informações sobre os parâmetros da página Lista de Eventos, consulte a Tabela 1.
5. Para visualizar os detalhes de um evento, clique duas no evento que você deseja investigar. Para obter mais informações sobre detalhes do evento, consulte a Tabela 2.

Detalhes do evento

É possível visualizar uma lista de eventos em vários modos, incluindo no modo de fluxo ou em grupos de eventos. No modo escolhido para visualizar eventos, é possível localizar e visualizar os detalhes de um único evento.

A página de detalhes do evento fornece as seguintes informações:

Tabela 15. Detalhes do evento

Parâmetro	Descrição
Nome do evento	Especifica o nome normalizado do evento.
Categoria de Baixo Nível	Especifica a categoria de nível inferior deste evento.
Descrição do Evento	Especifica uma descrição do evento, se disponível.
Magnitude	Especifica a magnitude deste evento. Para obter mais informações sobre magnitude, consulte o Glossário
Relevância	Especifica a relevância deste evento. Para obter mais informações sobre a relevância, consulte o Glossário.
Gravidade	Especifica a severidade deste evento. Para obter mais informações sobre severidade, consulte o Glossário.
Credibilidade	Especifica a credibilidade deste evento. Para obter mais informações sobre credibilidade, consulte o Glossário.
Nome de usuário	Especifica o nome de usuário associado a este evento, se disponível.
Start Time	Especifica a hora que o evento foi recebido da fonte de log.
Horário de Armazenamento	Especifica a hora em que o evento foi armazenado no banco de dados doQRadar.
Horário da Fonte de Log	Especifica a hora do sistema, conforme relatada pela fonte de log na carga útil do evento.
Informações de destino e de origem	
IP de Origem	Especifica o endereço IP de origem do evento.

Tabela 15. Detalhes do evento (continuação)

Parâmetro	Descrição
IP de destino	Especifica o endereço IP de destino do evento.
Nome do Ativo-fonte	Especifica o nome de ativo definido pelo usuário da origem de eventos. Para obter mais informações sobre ativos, consulte Gerenciamento de ativos.
Nome do Ativo de Destino	Especifica o nome de ativo definido pelo usuário do destino do evento. Para obter mais informações sobre ativos, consulte Gerenciamento de ativos
Porta de origem	Especifica a porta de origem deste evento.
Porta de destino	Especifica a porta de destino deste evento.
IP de Origem NAT Anterior	Para um firewall ou outro dispositivo capaz de Conversão de Endereço de Rede (NAT), este parâmetro especifica o endereço IP de origem antes dos valores NAT serem aplicados. O NAT converte um endereço IP em uma rede para um endereço IP diferente em outra rede.
IP de Destino NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará o endereço IP de destino antes dos valores de NAT serem aplicados.
Porta de Origem NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de origem antes dos valores de NAT serem aplicados.
Porta de Destino NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de destino antes dos valores de NAT serem aplicados.
IP de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará o endereço IP de origem após os valores de NAT serem aplicados.
IP de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará o endereço IP de destino após os valores de NAT serem aplicados.
Porta de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de origem após os valores de NAT serem aplicados.
Porta de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de destino após os valores de NAT serem aplicados.
Porta de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de origem após os valores de NAT serem aplicados.

Tabela 15. Detalhes do evento (continuação)

Parâmetro	Descrição
Porta de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de destino após os valores de NAT serem aplicados.
Origem de IPv6	Especifica o endereço IPv6 de origem do evento.
Destino de IPv6	Especifica o endereço IPv6 de destino do evento.
MAC de Origem	Especifica o endereço MAC de origem do evento.
MAC de Destino	Especifica o endereço MAC de destino do evento.
Informações úteis	
Payload	Especifica o conteúdo da carga útil do evento. Este campo oferece 3 guias para visualizar a carga útil: <ul style="list-style-type: none"> • Formato de Transformação Universal (UTF) – Clique em UTF. • Hexadecimal - Clique em HEX. • Base64 – Clique em Base64.
Informações adicionais	
Protocolo	Especifica o protocolo associado a esse evento.
QID	Especifica o QID desse evento. Cada evento tem um QID exclusivo. Para obter mais informações sobre o mapeamento de um QID, consulte Modificando o mapeamento de eventos.
Origem de Log	Especifica a fonte de log que enviou o evento para QRadar. Se houver várias fontes de log associadas a esse evento, este campo especificará o termo Várias e o número de fontes de log.
Contagem de eventos	Especifica o número total de eventos empacotados neste evento normalizado. Os eventos são empacotados quando vários eventos do mesmo tipo, para o mesmo endereço IP de origem e destino, são vistos dentro de um curto período.
Custom Rules	Especifica as regras customizadas que correspondem a esse evento. .
Regras Customizadas Parcialmente Correspondidas	Especifica as regras customizadas que correspondem parcialmente esse evento.
Annotations	Especifica a anotação desse evento. As anotações são descrições de texto que as regras podem incluir automaticamente para eventos como parte da resposta da regra.

Tabela 15. Detalhes do evento (continuação)

Parâmetro	Descrição
Informações de identificação	– O QRadar coleta informações de identificação, se disponível, a partir de mensagens da fonte de log. Informações de identidade fornecem detalhes adicionais sobre ativos em sua rede. Fontes de log geram informações de identificação somente se a mensagem de log enviada para QRadar contiver um endereço IP e pelo menos um dos seguintes itens: nome de usuário ou endereço MAC. Nem todas as fontes de log geram informações de identificação. Para obter mais informações sobre identidade e ativos, consulte Gerenciamento de ativos.
Nome de Usuário de Identidade	Especifica o nome de usuário do ativo que está associado a esse evento.
IP de Identidade	Especifica o endereço IP do ativo que está associado a esse evento.
Nome BIOS de Rede de Identidade	Especifica o nome do Sistema Base de Entrada/Saída (NetBios) do ativo que está associado a esse evento.
Campo Identity Extended	Especifica mais informações sobre o ativo que está associado a esse evento. O conteúdo deste campo é o texto definido pelo usuário e depende dos dispositivos em sua rede que estão disponíveis para fornecer informações de identificação. Exemplos incluem: localização física de dispositivos, políticas relevantes, comutador de rede e nomes de portas.
Has Identity (Flag)	Especifica True se o QRadar tiver identificado as informações coletadas para o ativo que está associado a este evento. Para obter mais informações sobre quais dispositivos enviam informações de identificação, consulte o <i>Guia de Configuração do IBM Security QRadar DSM</i> .
Nome do Host de Identidade	Especifica o nome do host do ativo que está associado a esse evento.
MAC de Identidade	Especifica o endereço MAC do ativo que está associado a esse evento.
Nome do Grupo de Identidades	Especifica o nome do grupo do ativo que está associado a esse evento.

Barra de ferramentas de detalhes do evento

A barra de ferramentas de detalhes fornece várias funções para visualizar detalhes de eventos.

A barra de ferramentas **detalhes do evento** fornece as seguintes funções:

Tabela 16. Barra de ferramentas de detalhes do evento

Retornar para lista de eventos	Clique em Retornar para Lista de eventos para retornar para a lista de eventos.

Tabela 16. Barra de ferramentas de detalhes do evento (continuação)

Mapear Evento	Clique em Mapear evento para editar o mapeamento de eventos. Para obter mais informações, consulte Modificando de mapeamento de eventos.
Positivo Falso	Clique em Positivo falso para ajustar o QRadar para evitar que eventos positivos falsos sejam gerados em ofensas.
Extrair Propriedade	Clique em Extrair propriedade para criar uma propriedade de evento customizada do evento selecionado.
Anterior	Clique em Anterior para visualizar o evento anterior na lista de eventos.
Avançar	Clique em Avançar para visualizar o próximo evento na lista de eventos.
Dados do PCAP	<p>Nota: Essa opção será exibida somente se o QRadar Console estiver configurado para se integrar com o Juniper JunOS Platform DSM. Para obter mais informações sobre o gerenciamento de dados PCAP, consulte Gerenciando dados PCAP.</p> <ul style="list-style-type: none"> • Visualizar informações de PCAP – Selecione esta opção para visualizar as informações de PCAP. Para obter mais informações, consulte Exibindo informações de PCAP. • Fazer download do arquivo PCAP – Selecione esta opção para fazer download do arquivo PCAP para seu sistema de área de trabalho. Para obter mais informações, consulte Fazendo download do arquivo PCAP em seu sistema de área de trabalho.
Imprimir	Clique em Imprimir para imprimir os detalhes do evento.

Modificando mapeamento de eventos

Você pode mapear manualmente um evento normalizado ou bruto para uma categoria de nível superior e inferior (ou QID).

Antes de Iniciar

Esta ação manual é usada para mapear eventos de origem de log desconhecidos para eventos conhecidos do QRadar para que eles possam ser categorizados e processados apropriadamente.

Sobre Esta Tarefa

Para fins de normalização, o QRadar mapeia automaticamente eventos de origens de log para categorias de nível superior e inferior.

Para obter mais informações sobre as categorias de eventos, consulte o *Guia de Administração do IBM Security QRadar Log Manager*.

Se os eventos forem recebidos de origens de log que o sistema não pode categorizar, os eventos serão categorizados como desconhecidos. Esses eventos ocorrem por vários motivos, incluindo:

- **Eventos definido pelo usuário** – algumas origens de log, como Snort, permite criar eventos definidos pelo usuário.
- **Eventos novos ou mais antigos** – as origens de log do fornecedor podem atualizar seu software com as liberações de manutenção para suportar novos eventos que o QRadar pode não suportar.

Nota: O ícone **Mapear evento** será desativado para os eventos quando a categoria de nível superior for a Auditoria de SIM ou o tipo de origem de log for Simple Object Access Protocol (SOAP).

Procedimento

1. Clique na guia **Atividade de Log**.
2. Opcional. Se você estiver visualizando os eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Dê um clique duplo no evento que você deseja mapear.
4. Clique em **Mapear evento**.
5. Se você souber o QID que deseja mapear para esse evento, insira o QID no campo **Inserir QID**.
6. Se você não souber o QID que deseja mapear para esse evento, será possível procurar um QID determinado:
 - a. Escolha uma das opções a seguir: Para procurar um QID pela categoria, selecione a categoria de nível superior na caixa de listagem Categoria de nível superior. Para procurar um QID pela categoria, selecione a categoria de nível inferior na caixa de listagem Categoria de nível inferior. Para procurar um QID pelo tipo de origem de log, selecione um tipo de origem de log na caixa de listagem Tipo de origem de log. Para procurar um QID pelo nome, insira um nome no campo QID/Nome.
 - b. Clique em **Procurar**.
 - c. Selecione o **QID** que você deseja associar a esse evento.
7. Clique em **OK**.

Gerenciando dados de PCAP

Se o Console do QRadar estiver configurado para se integrar ao Juniper JunOS Platform DSM, em seguida, a Captura de Pacotes (PCAP) poderá ser recebida, processada e os dados poderão ser armazenados a partir de uma origem de log do Juniper SRX-Series Services Gateway.

Para obter mais informações sobre o Juniper JunOS Platform DSM, consulte o *Guia de Configuração do IBM Security QRadar DSM*.

Exibindo a coluna de dados do PCAP

A coluna **Dados do PCAP** não é exibida na guia **Atividade de log** por padrão. Ao criar critérios de procura, você deverá selecionar a coluna **Dados do PCAP** na área de janela Definição de Coluna.

Antes de Iniciar

Antes que você possa exibir os dados do PCAP na guia **Atividade de log**, a origem de log do Gateway de Serviços das Séries SRX da Juniper deverá ser configurada com o protocolo de Combinação de Syslog do PCAP. Para obter mais informações sobre como configurar os protocolos de origem de log, consulte o *Guia de Gerenciamento do Log Sources*.

Sobre Esta Tarefa

Ao executar uma procura que inclua a coluna **Dados do PCAP**, um ícone será exibido na coluna **Dados do PCAP** dos resultados da procura, se os dados do PCAP estiverem disponíveis para um evento. Usando o ícone **PCAP**, você pode visualizar os dados do PCAP ou fazer o download do arquivo **PCAP** para seu sistema de desktop.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Procurar**, selecione **Nova Procura**.
3. Opcional. Para procurar eventos que possuam os dados do PCAP, configure os critérios de procura a seguir:
 - a. Na primeira caixa de listagem, selecione **Dados do PCAP**.
 - b. Na segunda caixa de listagem, selecione **Iguais**.
 - c. Na terceira caixa de listagem, selecione **Verdadeiro**.
 - d. Clique em **Incluir filtro**.
4. Configure suas definições de coluna para incluir a coluna **Dados do PCAP**:
 - a. Na lista **Colunas disponíveis** na área de janela Definição de Coluna, clique em **Dados do PCAP**.
 - b. Clique no ícone **Incluir coluna** no conjunto de ícones inferior para mover a coluna **Dados do PCAP** para a lista **Colunas**.
 - c. Opcional. Clique no ícone **Incluir coluna** no conjunto de ícones superior para mover a coluna **Dados do PCAP** para a lista **Agrupar por**.
5. Clique em **Filtrar**.
6. Opcional. Se você estiver visualizando os eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
7. Dê um clique duplo no evento que você deseja investigar.

O que Fazer Depois

Para obter mais informações sobre a visualização e download de dados do PCAP, consulte as seções a seguir:

- Visualizando informações do PCAP
- Fazendo download do arquivo PCAP para seu sistema de desktop

Visualizando informações do PCAP

No menu da barra de ferramentas **Dados do PCAP**, você pode visualizar uma versão legível dos dados no arquivo do PCAP ou fazer o download do arquivo PCAP para o sistema de sua área de trabalho.

Antes de Iniciar

Antes de poder visualizar informações do PCAP, você deve executar ou selecionar uma procura que exibe os **Dados** da coluna.

Sobre Esta Tarefa

Antes que os dados do PCAP possam ser exibidos, o arquivo PCAP deve ser recuperado para exibição na interface com o usuário. Se o processo de download tomar um longo período, a janela Informações para download do pacote do PCAP será exibida. Na maioria dos casos, o processo de download é rápido e esta janela não será exibida.

Depois que o arquivo for recuperado, uma janela pop-up fornecerá uma versão legível do arquivo PCAP. Você pode ler as informações exibidas na janela, ou fazer download das informações para o sistema de sua área de trabalho.

Procedimento

1. Para o evento que você deseja investigar, escolha uma das opções a seguir:
 - Selecione o evento e clique no ícone **PCAP**.
 - Clicar com o botão direito do mouse no ícone **PCAP** para o evento e selecionar **Mais opções > Visualizar informações do PCAP**.
 - Clique duas vezes no evento que você deseja investigar e, em seguida, selecione **Dados do PCAP > Visualizar informações do PCAP** na barra de ferramentas detalhes do evento.
2. Se você deseja fazer download das informações para o sistema de sua área de trabalho, escolha uma das opções a seguir:
 - Clique em **Download do arquivo PCAP** para fazer o download do arquivo PCAP original a ser usado em um aplicativo externo.
 - Clique em **Download do texto PCAP** para fazer o download das informações do PCAP em formato .TXT
3. Escolha uma das opções a seguir:
 - Se você deseja abrir o arquivo para visualização imediata, selecione a opção **Abrir com** e selecione um aplicativo na caixa de listagem.
 - Se você deseja salvar a lista, selecione a opção **Salvar arquivo**.
4. Clique em **OK**.

Fazendo download do arquivo PCAP para seu sistema de desktop

Você pode fazer download do arquivo PCAP para seu sistema de desktop para o armazenamento ou uso em outros aplicativos.

Antes de Iniciar

Antes que você possa visualizar informações de PCAP, você deverá executar ou selecionar uma procura que exiba a coluna **Dados do PCAP**. Consulte **Exibindo a coluna de dados do PCAP**.

Procedimento

1. Para o evento que você deseja investigar, escolha uma das opções a seguir:
 - Selecione o evento e clique no ícone **PCAP**.

- Clique com o botão direito do mouse no ícone do PCAP para o evento e selecione **Mais opções > Fazer download do arquivo PCAP**.
 - Dê um clique duplo no evento que você deseja investigar e, em seguida, selecione **Dados do PCAP > Fazer download arquivo PCAP** na barra de ferramentas de detalhes do evento.
2. Escolha uma das opções a seguir:
 - Se você deseja abrir o arquivo para visualização imediata, selecione a opção **Abrir com** e selecione um aplicativo na caixa de listagem.
 - Se você deseja salvar a lista, selecione a opção **Salvar arquivo**.
 3. Clique em **OK**.

Exportando eventos

Você pode exportar eventos no formato Linguagem de Marcação Extensível (XML) ou Valores Separados por Vírgulas (CSV).

Antes de Iniciar

A duração de tempo necessária para exportar seus dados depende do número de parâmetros especificados.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Opcional. Se você estiver visualizando os eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Na caixa de listagem **Ações**, selecione uma das opções a seguir:
 - **Exportar para XML > Colunas visíveis** – selecione essa opção para exportar somente as colunas visíveis na guia Atividade de log. Essa é a opção recomendada.
 - **Exportar para XML > Exportação integral (Todas as colunas)** – selecione essa opção para exportar todos os parâmetros de eventos. Uma exportação integral pode demorar um longo período de tempo para ser concluída.
 - **Exportar para CSV > Colunas visíveis** – selecione essa opção para exportar somente as colunas visíveis na guia **Atividade de log**. Essa é a opção recomendada.
 - **Exportar para CSV > Exportação integral (todas as colunas)** – Selecione esta opção para exportar todos os parâmetros de eventos. Uma exportação integral pode demorar um longo período de tempo para ser concluída.
4. Se você deseja continuar suas atividades enquanto a exportação estiver em andamento, clique em **Notificar quando estiver pronto**.

Resultados

Quando a exportação for concluída, você receberá uma notificação de que a exportação foi concluída. Se não foi selecionado o ícone **Notificar quando estiver pronto**, a janela de status será exibida.

Capítulo 5. Gerenciamento de gráfico

É possível usar as opções várias configuração do gráfico para visualizar seus dados.

Se for selecionado um prazo ou uma opção de agrupamento para visualizar seus dados, os gráficos serão exibidos acima da lista de eventos.

Os gráficos não serão exibidos quando estiverem no modo de fluxo.

É possível configurar um gráfico para selecionar com quais dados deseja criar gráficos. É possível configurar gráficos independentes um do outro para exibir seus resultados de procura de diferentes perspectivas.

Os tipos de gráfico incluem:

- Gráfico de barras - Exibe de dados em um gráfico de barras. Essa opção está disponível somente para eventos agrupados.
- Gráfico de pizza – Exibe os dados em um gráfico de pizza. Essa opção está disponível somente para eventos agrupados.
- Tabela – Exibe os dados em uma tabela. Essa opção está disponível somente para eventos agrupados.
- Série Temporal – Exibe um gráfico de linha interativo que representa os registros que são correspondidos por um intervalo de tempo especificado. Para obter informações sobre como configurar os critérios de procura de série temporal, consulte Visão geral do gráfico de série temporal.

Após configurar um gráfico, as configurações do gráfico serão retidas quando você:

- Alterar sua visualização usando a caixa de listagem **Exibir**.
- Aplicar um filtro.
- Salvar seus critérios de procura.

Suas configurações de gráfico não serão retidas quando você:

- Iniciar uma nova procura.
- Acessar uma procura rápida.
- Visualizar resultados agrupados em uma janela de ramificação.
- Salvar resultados da procura.

Nota: Se o navegador da web Mozilla Firefox for usado e uma extensão de navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para exibir gráficos, você deverá remover a extensão de navegador bloqueadora de anúncio. Para obter mais informações, consulte a documentação do navegador.

Visão geral do gráfico de série temporal

Gráficos de série temporal são representações gráficas de sua atividade com o tempo.

Picos e vales que são exibidos nos gráficos representam a atividade de volume alto e baixo. Gráficos de série temporal são úteis para tendência a curto e longo prazo de dados.

Usando gráficos de série temporal, você pode acessar, navegar e investigar atividade de log ou de rede a partir de várias visualizações e perspectivas.

Nota: Você deve ter as permissões de função apropriada para gerenciar e visualizar gráficos de série temporal.

Para exibir gráficos de série temporal, você deverá criar e salvar uma procura que inclui séries temporais e opções de agrupamento. Você pode salvar até 100 de procuras de série temporal.

Procuras salvas de séries temporais padrão são acessíveis na lista de procuras disponíveis na página de procura do evento.

É possível identificar facilmente procuras salvas de série temporal no menu **Procuras rápidas**, porque o nome da procura é anexada com o intervalo de tempo especificado nos critérios de procura.

Se os seus parâmetros de procura corresponderem a uma procura salva anteriormente para definição de coluna e opções de agrupamento, um gráfico de série temporal pode exibir automaticamente para os resultados da procura. Se um gráfico de série temporal não exibir automaticamente para seu critério de procuras não salvas, nenhum critério de procura salva anteriormente existirá para corresponder a seus parâmetros de procura. Se isso ocorrer, você deverá ativar a captura de dados da série temporal e salvar seus critérios de procura.

Você pode ampliar e varrer uma linha de tempo em um gráfico de série temporal para investigar a atividade. A tabela a seguir fornece funções que podem ser usadas para visualizar gráficos de série temporal.

Tabela 17. Funções de gráficos de série temporal

Função	Descrição
Visualizar dados em mais detalhes	<p>Usando o recurso de zoom, é possível investigar pequenos segmentos de tempo de tráfego de evento.</p> <ul style="list-style-type: none">• Mova o ponteiro do mouse sobre o seu gráfico e, em seguida, use a roda do mouse para ampliar o gráfico (rolar a roda de rolagem do mouse para cima).• Destaque a área do gráfico que deseja ampliar. Quando você liberar o botão do mouse, o gráfico exibirá um segmento de tempo menor. Agora você pode clicar e arrastar o gráfico para varrer o gráfico. <p>Quando você ampliar um gráfico de série temporal, o gráfico será atualizado para exibir um segmento de tempo menor.</p>

Tabela 17. Funções de gráficos de série temporal (continuação)

Função	Descrição
Visualizar um período de tempo maior de dados	Usando o recurso de zoom, é possível investigar segmentos de tempo maior ou retornar para o intervalo de tempo máximo. Você pode expandir um intervalo de tempo usando uma das seguintes opções: <ul style="list-style-type: none"> • Clique em Reconfiguração de Zoom no canto superior esquerdo do gráfico. • Mova o ponteiro do mouse sobre o gráfico e, em seguida, use a roda do mouse para expandir a visualização (role a roda de rolagem do mouse para baixo).
Varra o gráfico	Quando você tiver ampliado um gráfico de série temporal, você pode clicar e arrastar o gráfico para a esquerda ou para a direita para varrer a linha de tempo.

Legendas do gráfico

Cada gráfico fornece uma legenda, que é uma referência visual para ajudá-lo a associar os objetos de gráfico aos parâmetros que eles representam.

Usando o recurso legenda, é possível executar as seguintes ações:

- Mova o ponteiro do mouse sobre um item de legenda ou sobre bloco de cor da legenda para visualizar mais informações sobre os parâmetros que ele representa.
- Clique com o botão direito no item de legenda para investigar melhor o item.
- Clique em um item de legenda de um gráfico de barras ou de pizza para ocultar o item no gráfico. Clique no item de legenda novamente para mostrar o item oculto. É possível também clicar no item do gráfico correspondente para ocultar e mostrar o item.
- Clique em **Legenda** ou na seta ao lado, se desejar remover a legenda da exibição do gráfico.

Configurando gráficos

Você pode usar as opções de configurações para alterar o tipo de gráfico, o tipo de objeto que você deseja registrar em gráfico e o número de objetos representados no gráfico. Para os gráficos de séries temporais, você também pode selecionar um intervalo de tempo e ativar a captura de dados de séries temporais.

Antes de Iniciar

Os gráficos não são exibidos quando você visualiza os eventos no modo de Tempo Real (fluxo). Para exibir os gráficos, você deve acessar a guia **Atividade do log** e escolher uma das opções a seguir:

- Selecione as opções nas caixas de listagem **Visualizar** e **Exibir** e, em seguida, clique em **Salvar Critérios** na barra de ferramentas. Consulte Salvando evento e critérios de procura de fluxo.
- Na barra de ferramentas, selecione uma procura salva na lista **Procura rápida**.
- Execute uma procura agrupada e, em seguida, clique em **Salvar critérios** na barra de ferramentas.

Se você planeja configurar um gráfico de séries temporais, assegure-se de que os critérios de procura salvos estejam agrupados e especifiquem um intervalo de tempo.

Sobre Esta Tarefa

Os dados podem ser acumulados para que, ao executar uma procura de séries temporais, um cache de dados esteja disponível para exibir dados para o período de tempo anterior. Após ativar a captura de dados de séries temporais para um parâmetro selecionado, um asterisco (*) será exibido ao lado do parâmetro na caixa de listagem Value to Graph.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na área de janela Gráficos, clique no ícone **Configurar**.
3. Configure valores para os parâmetros a seguir:

Opção	Descrição
Parâmetro	Descrição
Value to Graph	Na caixa de listagem, selecione o tipo de objeto que você deseja que apareça no eixo Y do gráfico. As opções incluem todos os parâmetros de eventos normalizados e customizados incluídos em seus parâmetros de procura.
Display Top	Na caixa de listagem, selecione o número de objetos que você deseja visualizar no gráfico. O padrão é 10. A representação de gráfico com mais de 10 itens pode fazer com que os dados de gráfico fiquem ilegíveis.
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico que você deseja visualizar. Se o gráfico de barras, pizza ou tabela for baseado em critérios de procura salvos com um intervalo de tempo de mais de 1 hora, você deverá clicar em Atualizar detalhes para atualizar o gráfico e preencher os detalhes do evento
Capturar Dados de Série Temporal	Selecione essa caixa de seleção, se você desejar ativar a captura de dados de séries temporais. Ao selecionar essa caixa de seleção, o recurso de gráfico começará a acumular dados para os gráficos de séries temporais. Por padrão, essa opção está desativada. Essa opção está apenas disponível em gráficos Séries Temporais.
Time Range	Na caixa de listagem, selecione o intervalo de tempo que você deseja visualizar. Essa opção está apenas disponível em gráficos Séries Temporais.

4. Se você selecionou a opção de gráfico **Séries temporais** e ativou a opção **Capturar dados de séries temporais**, clique em **Salvar critérios** na barra de ferramentas.
5. Para visualizar a lista de eventos, se o intervalo de tempo for maior que 1 hora, clique em **Atualizar detalhes**.

Capítulo 6. Procuras de dados

Na guia **Atividade de log**, você pode procurar eventos usando critérios específicos.

Você pode criar uma procura ou carregar um conjunto de critérios de procura salvo anteriormente. Você pode selecionar, organizar e agrupar as colunas de dados a serem exibidas nos resultados da procura.

Após executar uma procura, você poderá salvar os critérios de procura e os resultados da procura.

Procurando itens que correspondam com seus critérios

Você pode procurar dados que correspondam com seus critérios de procura.

Sobre Esta Tarefa

Um vez que o banco de dados inteiro é procurado, as procuras podem levar um longo tempo, dependendo do tamanho do seu banco de dados.

Você pode usar o parâmetro de procura **Quick Filter** para procurar os itens que correspondam à sequência de texto na carga útil do evento.

Para obter mais informações sobre como usar o parâmetro Quick Filter, consulte a Sintaxe do Quick Filter (eventos).

A tabela a seguir descreve as opções de procura que você pode usar para procurar os dados do evento e fluxo:

Tabela 18. Opções de procura

Opções	Descrição
Grupo	Selecione um grupo de procura de evento para visualizar na lista Procuras salvas disponíveis .
Digitar Procura Salva ou Selecionar a partir da Lista	Insira o nome de uma procura salva ou uma palavra-chave para filtrar a lista Procuras salvas disponíveis .
Procuras Salvas Disponíveis	Essa lista exibe todas as procuras disponíveis, a menos que você use as opções Agrupar ou inserir procura salva ou Selecionar da lista para aplicar um filtro na lista. Você pode selecionar uma procura salva nessa lista para ser exibida ou editada.
Procurar	O ícone Procurar está disponível em várias áreas de janela na página de procura. Você poderá clicar em Procurar ao concluir a configuração da procura e desejar visualizar os resultados.
Incluir em Minhas Procuras Rápidas	Selecione essa caixa de seleção para incluir essa procura em seu menu Procura rápida .

Tabela 18. Opções de procura (continuação)

Opções	Descrição
Incluir em Meu Painel	Selecione essa caixa de seleção para incluir os dados da procura salva na guia Painel . Para obter mais informações sobre a guia Painel , consulte o Gerenciamento de painel. Nota: Esse parâmetro será exibido somente se a procura for agrupada.
Configurar como Padrão	Selecione essa caixa de seleção para configurar essa procura como a procura padrão.
Compartilhar com Todos	Selecione essa caixa de seleção para compartilhar essa procura com todos os outros usuários.
Tempo Real (fluxo)	Exibe os resultados no modo de fluxo. Para obter mais informações sobre o modo de fluxo, consulte Visualizando eventos de fluxo. Nota: Quando o Tempo Real (fluxo) estiver ativado, não será possível agrupar seus resultados da procura. Se você selecionar qualquer opção de agrupamento na área de janela Definição de Coluna, uma mensagem de erro será aberta.
Último Intervalo (atualização automática)	Exibe os resultados da procura no modo de atualização automática. No modo de atualização automática, a guia Atividade de log é atualizada em um intervalo de um minuto para exibir as informações mais recentes.
Recente	Selecione um intervalo de tempo predefinido para sua procura. Após selecionar essa opção, você deverá selecionar uma opção de intervalo de tempo na caixa de listagem.
Intervalo Específico	Selecione um intervalo de tempo customizado para sua procura. Após selecionar essa opção, você deverá selecionar a data e o intervalo de tempo nos calendários Horário de início e Horário de encerramento .

Tabela 18. Opções de procura (continuação)

Opções	Descrição
Acumulação de Dados	<p>Essa área de janela será exibida somente ao carregar uma procura salva.</p> <p>Ativando contagens exclusivas em dados acumulados compartilhados com muitas outras procuras salvas e relatórios podem diminuir o desempenho do sistema.</p> <p>Ao carregar uma procura salva, essa área de janela exibirá as opções a seguir:</p> <ul style="list-style-type: none"> • Se nenhum dado for acumulando para essa procura salva, a mensagem informativa a seguir será exibida: Dados não estão sendo acumulados para essa procura. • Se os dados estiverem acumulando para essa procura salva, as opções a seguir serão exibidas: <ul style="list-style-type: none"> – Colunas – quando você clicar ou passar o mouse sobre esse link, uma lista das colunas que estão acumulando os dados será aberta. – Ativar contagens exclusivas/Desativar contagens exclusivas – esse link permite que você ative ou desative os resultados da procura para exibir as contagens de eventos exclusivas em vez de contagens médias ao longo do tempo. Ao clicar no link Ativar contagens exclusivas, uma caixa de diálogo será aberta e indicará quais procuras salvas e relatórios compartilham os dados acumulados.
Filtros Atuais	Essa lista exibe os filtros aplicados a essa procura. As opções para incluir um filtro estão localizadas acima da lista Filtros atuais .
Salvar resultados quando a procura for concluída	Selecione essa caixa de seleção para salvar e nomear os resultados da procura.
Exibir	Selecione essa lista para especificar uma coluna predefinida configurada para exibir nos resultados da procura.
Digitar Coluna ou Selecionar a partir da Lista	<p>Você pode usar o campo para filtrar as colunas listadas na lista Colunas Disponíveis.</p> <p>Insira o nome da coluna que você deseja localizar ou insira uma palavra-chave para exibir uma lista de nomes de colunas. Por exemplo, insira Dispositivo para exibir uma lista de colunas que incluem o Dispositivo no nome da coluna.</p>

Tabela 18. Opções de procura (continuação)

Opções	Descrição
Colunas Disponíveis	Essa lista exhibe as colunas disponíveis. As colunas que estão atualmente em uso por essa procura salva estão destacadas e exibidas na lista Colunas .
Incluir e remover ícones da coluna (conjunto superior)	Use o conjunto superior de ícones para customizar a lista Agrupar por . <ul style="list-style-type: none"> • Incluir coluna – selecione uma ou mais colunas da lista Colunas disponíveis e clique no ícone Incluir coluna. • Remover coluna – selecione uma ou mais colunas da lista Agrupar por e clique no ícone Remover coluna.
Incluir e remover ícones da coluna (conjunto inferior)	Use o conjunto inferior de ícones para customizar a lista Colunas . <ul style="list-style-type: none"> • Incluir coluna – selecione uma ou mais colunas da lista Colunas Disponíveis e clique no ícone Incluir coluna. • Remover coluna – selecione uma ou mais colunas na lista Colunas e clique no ícone Remover coluna.
Agrupar por	Essa lista especifica as colunas nas quais a procura salva agrupa os resultados. Use as opções a seguir para customizar a lista adicional Agrupar Por : <ul style="list-style-type: none"> • Mover para cima – selecione uma coluna e a mova para cima através da lista de prioridade usando o ícone Mover para cima. • Mover para baixo – selecione uma coluna e a mova para baixo através da lista de prioridade usando o ícone Mover para baixo. <p>A lista de prioridade especifica em qual ordem os resultados serão agrupados. Os resultados da procura são agrupados pela primeira coluna na lista Agrupar por e, em seguida, agrupados pela próxima coluna na lista.</p>

Tabela 18. Opções de procura (continuação)

Opções	Descrição
Colunas	<p>Especifica as colunas escolhidas para a procura. Você pode selecionar mais colunas na lista Colunas disponíveis. Você pode customizar ainda mais a lista Colunas, usando as opções a seguir:</p> <ul style="list-style-type: none"> • Mover para cima – move a coluna selecionada para cima na lista de prioridades. • Mover para baixo – move a propriedade selecionada na lista de prioridades. <p>Se o tipo de coluna for numérico ou baseado em tempo e houver uma entrada na lista Agrupar por, então a coluna incluirá uma caixa de listagem. Use a caixa de listagem para escolher como deseja agrupar a coluna.</p> <p>Se o tipo de coluna for um grupo, a coluna incluirá uma caixa de listagem para selecionar quantos níveis você deseja incluir para o grupo.</p>
Ordenar Por	<p>Na primeira caixa de listagem, selecione a coluna pela qual você deseja classificar os resultados da procura. Em seguida, na segunda caixa de listagem, selecione a ordem que você deseja exibir para os resultados da procura. As opções incluem Decrescente e Crescente.</p>
Limite de Resultados	<p>Você pode especificar o número de linhas que um procura retorna na janela Editar procura. O campo Limite de resultados também aparece na janela Resultados.</p> <ul style="list-style-type: none"> • Para uma procura salva, o limite é armazenado na procura salva e reaplicado ao carregar a procura. • Ao classificar em uma coluna no resultado da procura que tem limite de linha, a classificação será feita dentro das linhas limitadas mostradas na grade de dados. • Para um agrupamento por procura com o gráfico de séries temporais ativado, o limite da linha somente se aplica à grade de dados. O suspenso Top N no gráfico de séries temporais ainda controla quantas séries temporais são desenhadas no gráfico.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Procurar**, selecione **Nova procura**.
3. Para selecionar uma procura salva anteriormente:

- a. Escolha uma das opções a seguir:na lista **Procuras Salvas Disponíveis**, selecione a procura salva que deseja carregar.No campo **InserirProcura Salva** ou **Selecionar da Lista**, insira o nome da procura que deseja carregar.
 - b. Clique em **Carregar**.
 - c. Na área de janela **Editar Procura**, selecione as opções que você deseja para essa procura. Consulte a Tabela 1.
4. Para criar uma procura, na área de janela **Intervalo de Tempo**, selecione as opções para o intervalo de tempo que você deseja capturar para essa procura.
5. Opcional. Na área de janela **Acumulação de Dados**, ative as contagens exclusivas:
 - a. Clique em **Ativar contagens exclusivas**.
 - b. Na janela **Aviso**, leia a mensagem de aviso e clique em **Continuar**. Para obter mais informações sobre a ativação de contagens exclusivas, consulte a Tabela 1.
6. Na área de janela **Parâmetros de Procura**, defina seus critérios de procura:
 - a. Na primeira caixa de listagem, selecione um parâmetro que você deseja procurar. Por exemplo, **Dispositivo**, **Porta de Origem** ou **Nome do Evento**.
 - b. Na segunda caixa de listagem, selecione o modificador que você deseja usar para a procura.
 - c. No campo de entrada, digite as informações específicas relacionadas ao seu parâmetro de procura.
 - d. Clique em **Incluir filtro**.
 - e. Repita as etapas de a até d para cada filtro que você deseja incluir nos critérios de procura.
7. Opcional. Para salvar automaticamente os resultados da procura quando a procura estiver concluída, selecione a caixa de seleção **Salvar resultados quando a procura for concluída** e, em seguida, insira um nome para a procura salva.
8. Na área de janela **Definição de Coluna**, defina as colunas e o layout da coluna que você deseja usar para visualizar os resultados:
 - a. Na caixa de listagem **Exibir**, selecione a coluna pré-configurada definida para associar a essa procura.
 - b. Clique na seta ao lado de **Definição de visualização avançada** para exibir os parâmetros de procura avançada.
 - c. Customizar as colunas a serem exibidas nos resultados da procura. Consulte a Tabela 1.
 - d. Opcional. No campo **Limite de resultados**, insira o número de linhas que você deseja que a procura retorne.
9. Clique em **Filtrar**.

Resultados

O status **Em progresso (<percentual>%Concluído)** será exibido no canto superior direito.

Ao visualizar os resultados da procura parcial, o mecanismo de procura funcionará em segundo plano para concluir a procura e atualizará os resultados parciais para atualizar sua visualização.

Quando a procura estiver concluída, o status **Concluído** será exibido no canto superior direito.

Salvando critérios de procura

Você pode salvar os critérios de procura configurados para que você possa reutilizar os critérios e usar os critérios de procura salvos em outros componentes, como relatórios. Os critérios de procura salvos não expiram.

Sobre Esta Tarefa

Se você especificar um intervalo de tempo para a sua procura, então o nome da procura será anexado ao intervalo de tempo especificado. Por exemplo, uma procura salva nomeada Explora por Origem com um intervalo de tempo de Últimos 5 minutos torna-se Explora por Origem – Últimos 5 minutos.

Se você alterar um conjunto de colunas em uma procura salva anteriormente e, em seguida, salvar os critérios de procura usando o mesmo nome, as acumulações anteriores para os gráficos de séries temporais serão perdidas.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Execute uma procura.
3. Clique em **Salvar critérios**.
4. Insira os valores para os parâmetros:

Opção	Descrição
Parâmetro	Descrição
Nome da Procura	Digite o nome exclusivo que deseja designar a esses critérios de procura.
Designar procura ao(s) grupo(s)	Selecione a caixa de seleção para o grupo que você deseja designar a essa procura salva. Se você não selecionar um grupo, essa procura salva será designada ao grupo Outros por padrão. Para obter mais informações, consulte Gerenciando grupos de procura.
Manage Groups	Clique em Gerenciar grupos para gerenciar grupos de procura. Para obter mais informações, consulte Gerenciando grupos de procura.

Opção	Descrição
Timespan options:	<p>Escolha uma das opções a seguir:</p> <ul style="list-style-type: none"> • Tempo real (fluxo) – selecione essa opção para filtrar os resultados da procura durante o modo de fluxo. • Último intervalo (atualização automática) – selecione essa opção para filtrar os resultados da procura durante o modo de atualização automática. As guias Atividade de log e Atividade de rede são atualizadas em intervalos de um minuto para exibir as informações mais recentes. • Recente – selecione essa opção e, nessa caixa de listagem, selecione o intervalo de tempo que você deseja filtrar. • Intervalo específico – selecione essa opção e, no calendário, selecione a data e hora do intervalo que você deseja filtrar.
Include in my Quick Searches	Selecione essa caixa de seleção para incluir essa procura na caixa de listagem Procura rápida na barra de ferramentas.
Include in my Dashboard	Selecione essa caixa de seleção para incluir os dados da procura salva na guia Painel . Para obter mais informações sobre a guia Painel , consulte o Gerenciamento de painel. Nota: Esse parâmetro será exibido somente se a procura for agrupada.
Set as Default	
Compartilhar com Todos	Selecione essa caixa de seleção para compartilhar esses requisitos de procura com todos os usuários.

5. Clique em **OK**.

Excluindo critérios de procura

Você pode excluir os critérios de procura.

Sobre Esta Tarefa

Ao excluir uma procura salva, objetos associados a ela poderão não funcionar. Os relatórios e as regras de detecção de anomalias são objetos do QRadar que usam os critérios de procura salvos. Após excluir uma procura salva, edite os objetos associados para assegurar-se de que eles continuarão a funcionar.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Procurar**, selecione **Nova procura** ou **Editar procura**.
3. Na área de janela **Procuras Salvas**, selecione uma procura salva na caixa de listagem **Procuras salvas disponíveis**.
4. Clique em **Excluir**.
 - Se os critérios de procura salvos não estiverem associados a outros objetos do QRadar, uma janela de confirmação será exibida.

- Se os critérios de procura salvos estiverem associados a outros objetos, a janela Excluir procura salva será exibida. A janela lista os objetos associados à procura salva que você deseja excluir. Observe os objetos associados.
5. Clique em **OK**.
 6. Escolha uma das opções a seguir:
 - Clique em **OK** para continuar.
 - Clique em **Cancelar** para fechar a janela Excluir procura salva.

O que Fazer Depois

Se os critérios de procura salvos forem associados a outros objetos do QRadar, acesse os objetos associados que você observou e edite-os para remover ou substituir a associação com a procura salva excluída.

Usando uma subprocura para refinar resultados da procura

É possível usar uma subprocura para procurar em um conjunto de resultados da procura concluído. A subprocura é usada para refinar os resultados da procura, sem procurar no banco de dados novamente.

Antes de Iniciar

Ao definir uma procura que você deseja usar como base para a subprocura, certifique-se de que a opção Tempo Real (fluxo) esteja desativada e a procura não esteja agrupada.

Sobre Esta Tarefa

Esse recurso não está disponível para pesquisas agrupadas, pesquisas em andamento ou em modo de fluxo.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Execute uma procura.
3. Quando a procura estiver concluída, inclua outro filtro:
 - a. Clique em **Incluir filtro**.
 - b. Na primeira caixa de listagem, selecione um parâmetro que você deseja procurar.
 - c. Na segunda caixa de listagem, selecione o modificador que você deseja usar para a procura. A lista de modificadores disponíveis depende do atributo selecionado na primeira lista.
 - d. No campo de entrada, insira as informações específicas relacionadas à sua procura.
 - e. Clique em **Incluir filtro**.

Resultados

A área de janela Filtro original especifica os filtros originais aplicados à procura base. A área de janela Filtro do Current especifica os filtros aplicados na subprocura. Você pode limpar os filtros de subprocura sem reiniciar a procura de base. Clique no link **Limpar filtro** ao lado do filtro que você deseja limpar. Se você limpar um filtro na área de janela Filtro Original, a procura de base será reativada.

Se você excluir os critérios de procura de base para os critérios de subprocura salvos, você ainda terá acesso para os critérios de subprocura salvos. Se você adicionar um filtro, a subprocura irá pesquisar o banco de dados inteiro, visto que a função de procura não mais baseia a procura em um conjunto de dados procurado anteriormente.

O que Fazer Depois

Salvar critérios de procura

Gerenciando resultados da procura

É possível iniciar várias procuras, e, em seguida, navegar para outras guias para executar outras tarefas enquanto suas procuras são concluídas em segundo plano.

É possível configurar uma procura para enviar uma notificação por email quando a procura for concluída.

A qualquer momento quando uma procura estiver em andamento, será possível retornar para a guia **Atividade de log** para visualizar os resultados da procura parciais ou completos.

Salvando resultados da procura

Você pode salvar os resultados da procura.

Sobre Esta Tarefa

Se você executar uma procura e não salvar os resultados da procura explicitamente, eles estarão disponíveis em Gerenciar intervalo de procura por 24 horas e, então, serão automaticamente excluídos.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Execute uma procura.
3. Clique em **Salvar resultados**.
4. Na janela Salvar resultado da procura, insira um nome exclusivo para os resultados da procura.
5. Clique em **OK**.

Visualizando resultados da procura gerenciada

Usando a página Gerenciar resultados da procura, você pode visualizar os resultados da procura parcial ou completa.

Sobre Esta Tarefa

Os resultados da procura retêm as configurações salvas do gráfico a partir do critério de procura associada, no entanto, se o resultado da procura for baseado em critério de procura excluída, os gráficos padrão (barra e setor) serão exibidos.

A página Gerenciar resultados da procura fornece os parâmetros a seguir

Tabela 19. Parâmetros da página gerenciar resultados da procura

Parâmetro	Descrição
Sinalizadores	Indica que uma notificação de email ficará pendente para quando a procura for concluída.
Usuário	Especifica o nome do usuário que iniciou a procura.
Nome	Especifica o nome da procura, se a procura foi salva. Para obter mais informações sobre como salvar uma procura, consulte Salvando resultados da procura.
Iniciado em	Especifica a data e hora em que a procura foi iniciada.
Terminado em	Especifica a data e hora em que a procura terminou.
Duração	Especifica a quantidade de tempo que a procura levou para ser concluída. Se a procura estiver em andamento, o parâmetro Duration especificará quanto tempo a procura levou no processamento da data de conclusão. Se a procura foi cancelada, o parâmetro Duration especificará o período de tempo que a procura levou no processamento antes de ter sido cancelada.
Expira em	Especifica a data e hora que um resultado da procura não salva irá expirar. O número de retenção da procura salva é configurado nas definições do sistema. Para obter mais informações sobre a configuração das definições do sistema, consulte o <i>Guia de Administração IBM Security QRadar Log Manager</i> .
Status	Especifica o status da procura. Os status são: <ul style="list-style-type: none"> • Enfileirado – Especifica que a procura está enfileirada para iniciar. • <percentual>%Concluído - Especifica o progresso da procura em termos de porcentagem concluída. Você pode clicar no link para visualizar os resultados parciais. • Classificação – Especifica que a procura concluiu a coleta de resultados e está atualmente preparando-os para visualização. • Cancelado – Especifica que a procura foi cancelada. Você pode clicar no link para visualizar os resultados coletados antes do cancelamento. • Concluído – Especifica que a procura foi concluída. Você pode clicar no link para visualizar os resultados. Consulte o Monitoramento da atividade de log
Tamanho	Especifica o tamanho do arquivo do conjunto de resultados da procura.

A barra de ferramentas da janela Gerenciar resultados da procura fornece as seguintes funções:

Tabela 20. Barra de ferramentas gerenciar resultados da procura

Função	Descrição
Nova procura	Clique em Nova procura para criar uma nova procura. Quando você clica neste ícone, a página de procura é exibida.
Salvar resultados	Clique em Salvar resultados para salvar os resultados da procura selecionada. Consulte salvando resultados da procura.
Cancelar	Clique em Cancelar para cancelar o resultado da procura selecionada em andamento ou enfileirada para iniciar. Consulte cancelando um procura.
Excluir	Clique em Excluir para excluir o resultado da procura selecionada. Consulte excluindo um resultado da procura.
Notificação	Clique em Notificação para ativar a notificação de email quando a procura selecionada for concluída.
Visualização	Nesta caixa de listagem, você pode selecionar quais resultados da procura que deseja listar na página Resultados da procura. As opções são: <ul style="list-style-type: none">• Resultados da procura salva• Todos os resultados da procura• Procuras canceladas/com erros• Procuras em andamento

Procedimento

1. Clique na guia **Atividade de Log**.
2. No menu **Procurar**, selecione **Gerenciar resultados da procura**.
3. Visualize a lista de resultados da procura.

Cancelando uma procura

Enquanto uma procura estiver na fila ou em andamento, você poderá cancelar a procura na página Gerenciar resultados da procura.

Sobre Esta Tarefa

Se a procura estiver em andamento quando for cancelada, os resultados acumulados até o cancelamento serão mantidos.

Procedimento

1. Clique na guia **Atividade de Log**.
2. A partir do menu **Procurar**, selecione **Gerenciar resultados da procura**.
3. Selecione o resultado da procura na fila ou em andamento que deseja cancelar.
4. Clique em **Cancelar**.

5. Clique em **Sim**.

Excluindo uma procura

Se um resultado da procura não for mais necessária, será possível excluir o resultado da procura da página Gerenciar resultados da procura.

Procedimento

1. Clique na guia **Atividade de Log**.
2. No menu **Procurar**, selecione **Gerenciar resultados da procura**.
3. Selecione o resultado de procura que você deseja excluir.
4. Clique em **Excluir**.
5. Clique em **Sim**.

Gerenciando grupos de procura

Usando a janela Procurar grupos, é possível criar e gerenciar grupos de procura de eventos, fluxo e ofensa.

Esses grupos permitem que você localize facilmente os critérios de procura salvos na guia **Atividade de log** e no assistente de relatório.

Visualizando grupos de procura

Um conjunto padrão de grupos e subgrupos estão disponíveis.

Sobre Esta Tarefa

Você pode visualizar grupos de procura na janela Grupos de procura de eventos.

Todas as procuras salvas não designadas a um grupo estão no grupo **Outros**.

A janela Grupos de procura de eventos exibe os seguintes parâmetros para cada grupo.

Tabela 21. Parâmetros da janela grupo de procura

Parâmetro	Descrição
Nome	Especifica o nome do grupo de procura.
Usuário	Especifica o nome do usuário que criou o grupo de procura.
Descrição	Especifica a descrição do grupo de procura.
Dados modificados	Especifica a data em que o grupo de procura foi modificado.

A barra de ferramentas da janela Grupo de procura de eventos fornece as seguintes funções.

Tabela 22. Funções da barra de ferramentas da janela Grupo de Procura

Função	Descrição
Novo grupo	Para criar um grupo de procura novo, você pode clicar em Novo grupo . Consulte Criando um grupo de procura novo.

Tabela 22. Funções da barra de ferramentas da janela Grupo de Procura (continuação)

Função	Descrição
Editar	Para editar um grupo de procura existente, você pode clicar em Editar . Consulte Editando um grupo de procura.
Copiar	Para copiar uma procura salva para outro grupo de procura, você pode clicar em Copiar . Consulte Copiando uma procura salva para outro grupo.
Remover	Para remover um grupo de procura ou uma procura salva de um grupo de procura, selecione o item que deseja remover, e, em seguida, clique em Remover . Consulte Removendo um grupo ou uma procura salva de um grupo.

Procedimento

1. Clique na guia **Atividade de Log**.
2. **Selecionar procura > Editar procura.**
3. Clique em **Gerenciar grupos**.
4. Visualize os grupos de procura.

Criando um novo grupo de procura

Você pode criar um novo grupo de procura.

Procedimento

1. Clique na guia **Atividade de Log**.
2. **Selecionar Procura Editar procura.**
3. Clique em **Gerenciar grupos**.
4. Selecione a pasta para o grupo no qual você deseja criar o novo grupo.
5. Clique em **Novo grupo**.
6. No campo **Nome**, digite um nome exclusivo para o novo grupo.
7. Opcional. No campo **Descrição**, digite uma descrição.
8. Clique em **OK**.

Editando um grupo de procura

Você pode editar os campos **Nome** e **Descrição** de um grupo de procura.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Selecione **Procurar > Editar procura**.
3. Clique em **Gerenciar grupos**.
4. Selecione o grupo que você deseja editar.
5. Clique em **Editar**.
6. Edite os parâmetros:
 - Digite um novo nome no campo **Nome**.
 - Insira uma nova descrição no campo **Descrição**.
7. Clique em **OK**.

Copiando uma procura salva em outro grupo

Você pode copiar uma procura salva para um ou mais grupos.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Selecione **Procurar > Editar procura**.
3. Clique em **Gerenciar grupos**.
4. Selecione a procura salva que deseja copiar.
5. Clique em **Copiar**.
6. Na janela Grupos de itens, marque a caixa de seleção para o grupo para o qual você deseja copiar a procura salva.
7. Clique em **Designar grupos**.

Removendo um grupo ou uma procura salva de um grupo

Você pode usar o ícone **Remover** para remover uma procura de um grupo ou remover um grupo de procura.

Sobre Esta Tarefa

Ao remover uma procura salva de um grupo, ela não será excluída do sistema. A procura salva é removida do grupo e movida automaticamente para o grupo **Outros**.

Não é possível remover os Grupos de Procura de Eventos do sistema.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Selecione **Procurar > Editar procura**.
3. Clique em **Gerenciar grupos**.
4. Escolha uma das opções a seguir:
 - Selecione a procura salva que você deseja remover do grupo.
 - Selecione o grupo que você deseja remover.
5. Clique em **Remover**.
6. Clique em **OK**.

Capítulo 7. Propriedades de evento customizado

Os eventos customizados e as propriedades de fluxo permitem procurar, visualizar e relatar as informações em logs que o QRadar SIEM geralmente não normaliza e exibe.

Você pode criar propriedades de evento customizado a partir de vários locais na guia **Atividade de log**:

- Detalhes do Evento – você pode selecionar um evento na guia **Atividade de log** para criar uma propriedade de evento customizado derivada de sua carga útil.
- Página Procurar - você pode criar e editar uma propriedade ou evento customizado na página Procurar. Ao criar uma nova propriedade customizada na página Procurar, a propriedade não será derivada de qualquer evento específico; portanto, a janela Definição de propriedade customizada não será preenchida previamente. Você pode copiar e colar as informações da carga útil a partir de outra origem.

Permissões requeridas

Para criar propriedades customizadas se tiver a permissão correta.

Você deve ter a permissão Propriedades do Evento Definidas pelo Usuário.

Se tiver permissões administrativas, também poderá criar e modificar propriedades customizadas na guia Administração.

Clique em **Admin > Origens de Dados > Propriedades de Evento Customizado**.

Verifique com seu administrador para assegurar-se de que você possui as permissões corretas.

Para obter informações adicionais, consulte o Guia de Administração do *IBM Security QRadar Log Manager*.

Tipos de propriedades customizadas

É possível criar um tipo de propriedade customizada.

Ao criar uma propriedade customizada, será possível optar por criar um Regex ou um tipo de propriedade calculado.

Usando as instruções de expressão regular (Regex), é possível extrair dados não normalizados das cargas úteis do evento.

Por exemplo, um relatório é criado para relatar todos os usuários que fazem suas mudanças de permissão em um servidor Oracle. Uma lista de usuários e o número de vezes que eles fizeram uma alteração na permissão da outra conta serão relatados. No entanto, normalmente a conta do usuário real ou a conta que foi alterada não pode ser exibida. É possível criar uma propriedade customizada para extrair essas informações dos logs e, em seguida, usar a propriedade em procuras e relatórios. O uso desse recurso requer conhecimento avançado de expressões regulares (regex).

Regex define o campo que você deseja que se torne a propriedade customizada. Após inserir uma instrução regex, será possível validá-la em relação à carga útil. Ao definir padrões regex customizados, siga para as regras regex conforme definidas pela linguagem de programação Java™.

Para obter mais informações, é possível consultar tutoriais regex disponíveis na web. Uma propriedade customizada pode ser associada a várias expressões regulares.

Quando um evento for analisado, cada padrão regex será testado no evento até que um padrão regex corresponda à carga útil. O primeiro padrão regex a corresponder à carga útil do evento determina os dados a serem extraídos.

Usando propriedades customizadas baseadas em cálculo, é possível executar cálculos propriedades de evento ou fluxo numérico existentes para produzir uma propriedade calculada

Por exemplo, é possível criar uma propriedade que exibe uma porcentagem dividindo uma propriedade numérica por outra propriedade numérica.

Criando uma propriedade customizada baseada em regex

É possível criar uma propriedade customizada baseada em regex para corresponder às cargas úteis de fluxo ou evento para uma expressão regular.

Sobre Esta Tarefa

Ao configurar uma propriedade customizada baseada em regex, a janela Propriedade de Evento Customizado fornece parâmetros. A tabela a seguir descreve alguns desses parâmetros.

Tabela 23. Janela de parâmetros (regex) de Propriedades de Evento Customizado

Parâmetro	Descrição
Campo de teste	Especifica a carga útil que foi extraída do evento ou fluxo não normalizado. Especifica a carga útil que foi extraída do evento não normalizado.
Nova Propriedade	O novo nome da propriedade não pode ser o nome de uma propriedade normalizada, como nome de usuário, IP de Origem ou IP de Destino.
Otimizar análise para regras, relatórios e procuras	Analisa e armazena a propriedade na primeira vez em que o evento ou fluxo for recebido. Ao selecionar a caixa de seleção, a propriedade não necessitará de mais análise para relatar, procurar ou testar a regra. Se limpar essa caixa de seleção, a propriedade será analisada todas as vezes em que um teste de relatório, de pesquisa ou de regra for aplicado.
Fonte de Log	Se várias fontes de log estiverem associadas a esse evento, esse campo especifica o termo Vários e o número de fontes de log.

Tabela 23. Janela de parâmetros (regex) de Propriedades de Evento Customizado (continuação)

Parâmetro	Descrição
RegEx	<p>A expressão regular que deseja usar para extrair os dados da carga útil. As expressões regulares fazem distinção entre maiúsculas e minúsculas.</p> <p>Os exemplos a seguir mostram expressões regulares de amostra:</p> <ul style="list-style-type: none"> • Email: <code>(.+@^[^\.]*\.[a-z]{2,})\$</code> • URL: <code>(http\:\/\/[a-zA-Z0-9\-\.\.]+\.[a-zA-Z]{2,3}(\S*)?\$)</code> • Nome de Domínio: <code>(http[s]?://(.?)["/?:])</code> • Número de Pontos Flutuantes: <code>([-+]?\d*\.\d*\$)</code> • Número Inteiro: <code>([-+]?\d*\$)</code> • Endereço IP: <code>(\b\d{1,3}\. \ \d{1,3}. \ \d{1,3}. \b \d{1,3})</code> <p>Os grupos de captura devem estar entre parênteses.</p>
Grupo de Captura	<p>Os grupos de captura tratam vários caracteres como uma unidade única. Em um grupo de captura, os caracteres são agrupados dentro de um conjunto de parênteses.</p>
Ativado	<p>Se você limpar a caixa de seleção, essa propriedade customizada não será exibida em filtros de procura ou listas de coluna e a propriedade não será analisada a partir das cargas úteis.</p>

Procedimento

1. Clique na guia **Atividade de Log**.
2. Se você estiver visualizando os eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Dê um clique duplo no evento ao qual você deseja basear a propriedade customizada
4. Clique em **Extrair propriedade**.
5. Na área de janela **Seleção do Tipo de Propriedade**, selecione a opção **Baseado em Regex**.
6. Configure os parâmetros de propriedade customizada.
7. Clique em **Testar** para testar a expressão regular com relação à carga útil.
8. Clique em **Salvar**.

Resultados

A propriedade customizada é exibida como uma opção na lista de colunas disponíveis na página de procura. Para incluir uma propriedade customizada em

uma lista de fluxos ou eventos, você deve selecionar a propriedade customizada na lista de colunas disponíveis ao criar uma pesquisa.

Criando uma propriedade customizada baseada em cálculo

É possível criar uma propriedade cliente baseada em cálculo para corresponder as cargas úteis do cliente em uma expressão comum.

Sobre Esta Tarefa

Ao configurar uma propriedade customizada baseada em cálculo, a janela Propriedade de Evento Customizado ou Propriedade de Fluxo Customizado fornece os parâmetros a seguir:

Tabela 24. Parâmetros de janela de definição de propriedade customizada (cálculo)

Parâmetro	Descrição
Definição de Propriedade	
Nome da Propriedade	Digite um nome exclusivo para essa propriedade customizada. O novo nome da propriedade não pode ser o nome de uma propriedade normalizada, como Nome do Usuário, IP de Origem ou de Destino.
Descrição	Digite uma descrição dessa propriedade customizada.
Definição de Cálculo da Propriedade	
Propriedade 1	Na caixa de listagem, selecione a primeira propriedade que você deseja usar em seu cálculo. As opções incluem todas as propriedades customizadas numéricas e normalizadas numéricas. Também é possível especificar um valor numérico específico. Na caixa de listagem Propriedade 1 , selecione a opção Definido pelo usuário . O parâmetro Numeric Property é exibido. Digite um valor numérico específico.
Operador	Na caixa de listagem, selecione o operador que você deseja aplicar para as propriedades selecionadas no cálculo. As opções incluem: <ul style="list-style-type: none">• Incluir• Subtrair• Multiplicar• Dividir

Tabela 24. Parâmetros de janela de definição de propriedade customizada (cálculo) (continuação)

Parâmetro	Descrição
Propriedade 2	<p>Na caixa de listagem, selecione a segunda propriedade que você deseja usar em seu cálculo. As opções incluem todas as propriedades customizadas numéricas e normalizadas numéricas.</p> <p>Também é possível especificar um valor numérico específico. Na caixa de listagem Propriedade 1, selecione a opção Definido pelo usuário. O parâmetro Numeric Property é exibido. Digite um valor numérico específico.</p>
Ativado	<p>Selecione esta caixa de seleção para ativar essa propriedade customizada.</p> <p>Se você desmarcar a caixa de seleção, essa propriedade customizada não será exibida em filtros de procura de eventos ou em listas de coluna e a propriedade de evento ou fluxo não será analisada a partir de cargas úteis.</p>

Procedimento

1. Escolha um dos seguintes: Clique na guia **Atividade de log**.
2. Opcional. Se você estiver visualizando eventos ou fluxos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Clique duas vezes no evento em que você deseja basear a propriedade customizada.
4. Clique em **Extrair propriedade**.
5. Na área de janela Seleção de Tipo de Propriedade, selecione a opção **Baseado em cálculo**.
6. Configure os parâmetros de propriedade customizada.
7. Clique em **Testar** para testar a expressão regular com relação à carga útil.
8. Clique em **Salvar**.

Resultados

A propriedade customizada agora é exibida como uma opção na lista de colunas disponíveis na página de procura. Para incluir uma propriedade customizada em uma lista de eventos ou fluxos, você deve selecionar a propriedade customizada da lista de colunas disponíveis ao criar uma procura.

Modificando uma propriedade customizada

Você pode modificar uma propriedade customizada.

Sobre Esta Tarefa

Você pode usar a janela Propriedades de evento customizado para modificar uma propriedade customizada.

As propriedades customizadas são descritas na tabela a seguir.

Tabela 25. Colunas da janela de propriedades customizadas

Coluna	Descrição
Nome da Propriedade	Especifica um nome exclusivo para essa propriedade customizada.
Tipo	Especifica o tipo para essa propriedade customizada.
Descrição da Propriedade	Especifica uma descrição para essa propriedade customizada.
Tipo de Fonte de Log	Especifica o nome do tipo de origem de log para o qual essa propriedade customizada se aplica. Essa coluna é exibida somente na janela Propriedades de evento Customizado.
Origem de Log	Especifica a origem de log para a qual essa propriedade customizada se aplica. Se houver várias fontes de log associadas a esse evento, este campo especificará o termo Várias e o número de fontes de log. Essa coluna é exibida somente na janela Propriedades de evento customizado.
Expressão	Especifica a expressão para essa propriedade customizada. A expressão depende do tipo de propriedade customizada: Para uma propriedade customizada baseada em regex, esse parâmetro especifica a expressão regular que você deseja usar para extrair os dados da carga útil. Para uma propriedade customizada baseada em cálculo, esse parâmetro especifica o cálculo que deseja usar para criar o valor da propriedade customizada.
Nome de usuário	Especifica o nome do usuário que criou essa propriedade customizada.
Ativado	Especifica se essa propriedade customizada está ativada. Esse campo especifica se é Verdadeiro ou Falso.
Data de Criação	Especifica a data que essa propriedade customizada foi criada.
Data da Modificação	Especifica a última vez que essa propriedade customizada foi modificada.

A barra de ferramentas Propriedade de Evento Customizado fornece as funções a seguir:

Tabela 26. Opções da barra de ferramentas da propriedade customizada

Opção	Descrição
Incluir	Clique em Incluir para incluir uma nova propriedade customizada.
Editar	Clique em Editar para editar a propriedade customizada selecionada.
Copiar	Clique em Copiar para copiar as propriedades customizadas selecionadas.
Excluir	Clique em Excluir para excluir as propriedades customizadas selecionadas.
Ativar/Desativar	Clique em Ativar/Desativar para ativar ou desativar as propriedades customizadas selecionadas para análise e visualização dos filtros de procura ou listas de colunas.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Procurar**, selecione **Editar procura**.
3. Clique em **Gerenciar propriedades customizadas**.
4. Selecione a propriedade customizada que você deseja editar e clique em **Editar**.
5. Editar os parâmetros necessários.
6. Opcional. Se você editou a expressão regular, clique em **Testar** para testar a expressão regular com relação à carga útil.
7. Clique em **Salvar**.

Copiando uma propriedade customizada

Para criar uma nova propriedade customizada baseada em uma propriedade customizada existente, você poderá copiar a propriedade customizada existente e, em seguida, modificar os parâmetros.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Procurar**, selecione **Editar procura**.
3. Clique em **Gerenciar propriedades customizadas**.
4. Selecione a propriedade customizada que você deseja copiar e clique em **Copiar**.
5. Editar os parâmetros necessários.
6. Opcional. Se você editou a expressão regular, clique em **Testar** para testar a expressão regular com relação à carga útil.
7. Clique em **Salvar**.

Excluindo uma propriedade customizada

Você pode excluir qualquer propriedade customizada, desde que a propriedade customizada não esteja associada à outra propriedade customizada.

Procedimento

1. Na caixa de listagem **Procurar**, selecione **Editar procura**.
2. Clique em **Gerenciar propriedades customizadas**.
3. Selecione a propriedade customizada que deseja excluir e clique em **Excluir**.
4. Clique em **Sim**.

Capítulo 8. Gerenciamento de regras

Na guia **Atividade de log**, você pode visualizar e manter as regras.

Este tópico se aplica a usuários que possuem as permissões de função do usuário **Visualizar regras customizadas** ou **Manter regras customizadas**.

Considerações sobre permissão de regra

É possível visualizar e gerenciar regras para as áreas da rede a que você tem acesso, se você tiver as permissões de função do usuário **Visualizar Regras Customizadas** e **Manter Regras Customizadas**.

Para criar regras de detecção de anomalias, você deve ter a permissão **Manter regra customizada** apropriada para a guia na qual deseja criar a regra. Por exemplo, para poder criar uma regra de detecção de anomalias na guia **Atividade de log**, deve-se ter **Atividade de log > Manter regra customizada**.

Para obter mais informações sobre as permissões de função de usuário, consulte o *Guia de Administração do IBM Security QRadar Log Manager*.

Visão geral de regras

As regras executam testes em eventos e se todas as condições de um teste forem atendidas, a regra irá gerar uma resposta.

Os testes em cada regra também podem referenciar outros blocos de construção e regras. Não será necessário criar regras em qualquer ordem específica porque o sistema verificará as dependências cada vez que uma nova regra for incluída, editada ou excluída. Se uma regra referenciada por outra regra for excluída ou desativada, um aviso será exibido e nenhuma ação será executada.

Para obter uma lista completa de regras padrão, consulte o *Guia de Administração do IBM Security QRadar SIEM*.

Regra de evento

Uma regra de evento executa testes em eventos conforme eles são processados em tempo real pelo Processador de eventos.

Você pode criar uma regra de evento para detectar um único evento, em determinadas propriedades ou sequências de eventos. Por exemplo, se desejar monitorar tentativas de login malsucedidas, acessos a vários hosts ou um evento de reconhecimento seguido por uma exploração em sua rede, você poderá criar uma regra de evento. É comum para regras de evento criar ofensas como uma resposta.

Condições da regra

Cada regra pode conter funções, blocos de construção ou testes.

Com as funções, é possível usar blocos de construção e outras regras para criar uma função de vários eventos. É possível conectar regras usando funções que suportam operadores booleanos, como OR e AND. Por exemplo, se desejar

conectar regras de evento, será possível usar quando um evento corresponder alguma ou todas as funções das regras a seguir.

Um bloco de construção é uma regra sem uma resposta e é usado como uma variável comum em várias regras ou para construir regras complexas ou lógicas que deseja usar em outras regras. É possível salvar um grupo de testes como blocos de construção para uso com outras funções. Blocos de construção permitirão que reutilize testes de uma regra específica em outras regras. Por exemplo, é possível salvar um bloco de construção que inclui os endereços IP de todos os servidores de correio em sua rede e, em seguida, usar esse bloco de construção para excluir os servidores de correio de outra regra. Os blocos de construção padrão são fornecidos como diretrizes, que devem ser revistas e editadas com base nas necessidades de sua rede.

É possível executar testes na propriedade de um evento, como endereço IP de origem ou severidade do evento.

Respostas da regra

Quando as condições da regra forem atendidas, uma regra poderá gerar uma ou mais respostas.

As regras podem gerar uma ou mais das seguintes respostas:

- Crie uma ofensa.
- Envie um email.
- Gere notificações do sistema no recurso do Painel.
- Incluir dados em conjuntos de referência.
- Inclua dados em coletas de dados de referência.
- Gere uma resposta para um sistema externo.
- Inclua dados em coletas de dados de referência que podem ser usados em testes de regras.

Tipos de coleção de dados de referência

Antes de poder configurar uma resposta da regra para enviar dados para uma coleta de dados de referência, você deve criar a coleta de dados de referência usando a interface da linha de comandos (CLI). O QRadar suporta os seguintes tipos de coleta de dados:

Conjunto de referência

Um conjunto de elementos, como uma lista de endereços IP ou nomes de usuário, que são derivados de eventos e fluxos que ocorrem em sua rede.

Mapa de referência

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

Mapa de referência de conjuntos

Os dados são armazenados em registros de que mapeiam uma tecla para vários valores. Por exemplo, para testar o acesso autorizado a uma patente, use uma propriedade de evento customizada para **Patent ID** como a chave e o parâmetro **Username** como o valor. Use um mapa de configurações para preencher uma lista de usuários autorizados.

Mapa de referência de mapas

Os dados são armazenados em registros que mapeiam uma chave para outra chave, que é, então, mapeada para um valor único. Por exemplo, para testar para violações de largura da banda da rede, você pode criar um mapa de mapas. Use o parâmetro **Source IP** como a primeira chave, o parâmetro **Application** como a segunda chave e o parâmetro **Total Bytes** como o valor.

Tabela de referência

Em uma tabela de referência, os dados são armazenados em uma tabela que mapeia uma chave para outra, que é, então, mapeada para valor único. A segunda chave tem um tipo designado. Esse mapeamento é semelhante a uma tabela de banco de dados em que cada coluna da tabela é associada a um tipo. Por exemplo, é possível criar uma tabela de referência que armazena o parâmetro **Username** como a primeira chave, e possui várias chaves secundárias que possuem um tipo designado pelo usuário como **Tipo IP** com o parâmetro **Source IP** ou **Source Port** como um valor. É possível configurar uma resposta da regra para incluir uma ou mais chaves definidas na tabela. É possível também incluir valores customizados à resposta da regra. O valor customizado deve ser válido para o tipo de chave secundária.

Nota: Para obter informações sobre conjuntos de referência e as coleções de dados de referência, consulte o *Guia de Administração* do seu produto.

Visualizando regras

Você pode visualizar os detalhes de uma regra, incluindo os testes, blocos de construção e respostas.

Antes de Iniciar

Dependendo das permissões da função de usuário, você poderá acessar a página regras na guia **Atividade de Log**. Para obter mais informações sobre as permissões da função de usuário, consulte o *Guia de Administração do IBM Security QRadar Log Manager*.

Sobre Esta Tarefa

A página Regras exibe uma lista de regras com seus parâmetros associados. Para localizar a regra a qual você deseja abrir e visualizar os detalhes, você pode usar a caixa de lista de Grupo ou o campo **Regras da procura** na barra de ferramentas.

Procedimento

1. Clique na guia **Atividade de Log** e, em seguida, selecione **Regras** na caixa de listagem **Regras** na barra de ferramentas.
2. Na caixa de listagem **Exibir**, selecione **Regras**.
3. Clique duas vezes na regra que você deseja visualizar.
4. Revise os detalhes da regra.

Resultados

Se você tiver a permissão **Visualizar regras customizadas**, mas não tem a permissão **Manter regras customizadas**, a página **Resumo da regra** será exibida e a regra não poderá ser editada. Se você tiver a permissão **Manter regras**

customizadas, a página **Editor de regra de teste de pilha** será exibida. Você pode revisar e editar detalhes da regra.

Criando uma regra customizada

Você pode criar novas regras para atender às necessidades de sua implementação.

Sobre Esta Tarefa

Para criar uma nova regra, você deverá ter a permissão **Ofensas > Manter regras customizadas**.

Você pode testar regras localmente ou globalmente. Um teste local significa que a regra é testada no processador de eventos local e não compartilhada com o sistema. Um teste global significa que a regra é compartilhada e testada por qualquer Processador de eventos no sistema. As regras globais enviam eventos e fluxos ao Processador de evento central que pode diminuir o desempenho no Processador de evento central.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Na lista **Ações**, selecione **Nova regra de evento**.
4. Leia o texto de introdução no assistente Regra. Clique em **Avançar**.
5. Clique em **Avançar** para visualizar a página Editor de Pilha de Teste de Regra.
6. No campo **Inserir o nome da regra aqui** na área de janela Regra, insira um nome exclusivo que você deseja designar a essa regra.
7. Na caixa de listagem, selecione **Local** ou **Global**.
8. Incluir um ou mais testes em uma regra:
 - a. Opcional. Para filtrar as opções na caixa de listagem **Grupo de teste**, insira o texto que você deseja filtrar no campo Tipo a ser filtrado.
 - b. Na caixa de listagem **Grupo de teste**, selecione o tipo de teste que você deseja incluir nessa regra.
 - c. Para cada teste que você deseja incluir na regra, selecione o sinal de mais (+) ao lado do teste.
 - d. Opcional. Para identificar um teste como teste excluído, clique em **e** no início do teste na área de janela Regra. O **e** é exibido como **e não**.
 - e. Clique nos parâmetros configuráveis sublinhados para customizar as variáveis do teste.
 - f. Na caixa de diálogo, selecione os valores para a variável **e**, em seguida, clique em **Enviar**.
9. Para exportar a regra configurada como um bloco de construção para o uso com outras regras:
 - a. Clique em **Exportar como blocos de construção**.
 - b. Insira um nome exclusivo para esse bloco de construção.
 - c. Clique em **Salvar**.
10. Na área de janela Grupos, marque as caixas de seleção dos grupos aos quais você deseja designar essa regra.
11. No campo **Notas**, insira uma nota que você deseja incluir para essa regra. Clique em **Avançar**.

12. Na página Respostas da regra, configure as respostas que você deseja que essa regra gere.
13. Clique em **Avançar**.
14. Revise a página Resumo de regra para assegurar-se de que as configurações estejam corretas. Faça as alterações, se necessário, e, em seguida, clique em **Concluir**.

Criando uma regra de detecção de anomalia

Use o assistente Regra de Detecção de Anomalias para criar regras que se aplicam aos critérios de intervalo de tempo, usando os testes de Data e Hora.

Antes de Iniciar

Para criar uma nova regra de detecção de anomalias, você deverá atender aos requisitos a seguir:

- Ter a permissão Manter Regras Customizadas.
- Executar uma procura agrupada.

As opções de detecção de anomalia serão exibidas após executar uma procura agrupada e salvar os critérios de procura.

Sobre Esta Tarefa

Você deve ter a permissão de função apropriada para poder criar uma regra de detecção de anomalia.

Para criar as regras de detecção de anomalias na guia **Atividade de log**, você deverá ter a permissão de função **Atividade de log Manter regras customizadas**.

Para criar as regras de detecção de anomalia na guia **Atividade de rede**, você deve ter a permissão de função **Rede Manter regras customizadas**.

As regras de detecção de anomalia usam todo o agrupamento e os critérios de filtros dos critérios de procura salvos nos quais a regra é baseada, mas não usam quaisquer intervalos de tempo dos critérios de procura.

Ao criar uma regra de detecção de anomalias, a regra será preenchida com uma pilha de teste padrão. Você pode editar os testes padrão ou incluir testes na pilha de teste. Pelo menos um teste Propriedade Acumulada deve ser incluído na pilha de teste.

Por padrão, a opção **Testar o valor [Selected Accumulated Property] de cada [group] separadamente** é selecionada na página Editor de Pilha de Teste de Regra.

Isso faz com que uma regra de detecção de anomalias teste a propriedade acumulada selecionada para cada grupo de eventos separadamente. Por exemplo, se o valor acumulado selecionado for **UniqueCount(sourceIP)**, a regra testará cada endereço IP de origem exclusivo para cada grupo de eventos.

Essa opção **Testar o valor [Selected Accumulated Property] de cada [group] separadamente** é dinâmica. O valor **[Selected Accumulated Property]** depende de qual opção foi selecionada no campo **Este teste de propriedade acumulada** da pilha de testes padrão. O valor **[group]** depende das opções de agrupamento especificadas nos critérios de procura salvos. Se diversas opções de agrupamento

forem incluídas, o texto poderá ficar truncado. Mova o ponteiro do mouse sobre o texto para visualizar todos os grupos.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Execute uma procura.
3. No menu **Regras**, selecione o tipo de regra que você deseja criar. As opções incluem:
 - Incluir regra de anomalia
 - Incluir Regra Limite
 - Incluir Regra comportamental
4. Leia o texto de introdução no assistente Regra. Clique em **Avançar**. A regra que você escolheu anteriormente está selecionada.
5. Clique em **Avançar** para visualizar a página Editor de Pilha de Teste de Regra.
6. No campo **digite o nome da regra aqui**, digite um nome exclusivo que você deseja designar a essa regra.
7. Para incluir um teste em uma regra:
 - a. Opcional. Para filtrar as opções na caixa de listagem Grupo de Teste, insira o texto que você deseja filtrar no campo Tipo a ser filtrado.
 - b. Na caixa de listagem Grupo de Teste, selecione o tipo de teste que deseja incluir nessa regra.
 - c. Para cada teste que você deseja incluir na regra, selecione o sinal + ao lado do teste.
 - d. Opcional. Para identificar um teste como teste excluído, clique em 'e' no início do teste na área de janela Regra. O e é exibido como e não.
 - e. Clique nos parâmetros configuráveis sublinhados para customizar as variáveis do teste.
 - f. Na caixa de diálogo, selecione os valores para a variável e, em seguida, clique em **Enviar**.
8. Opcional. Para testar o total de propriedades acumuladas selecionadas para cada grupo de eventos ou fluxo, limpe a caixa de seleção **Testar o valor [Selected Accumulated Property] de cada [group] separadamente**.
9. Na área de janela de grupos, marque as caixas de seleção dos grupos para os quais você deseja designar essa regra. Para obter mais informações, consulte Gerenciamento de grupo de regra.
10. No campo **Notas**, insira todas as notas que você deseja incluir nessa regra. Clique em **Avançar**.
11. Na página Respostas da regra, configure as respostas que você deseja que essa regra gere. "Parâmetros da página Resposta de regra" na página 94
12. Clique em **Avançar**.
13. Revise a regra configurada. Clique em **Concluir**.

Tarefas de gerenciamento de regra

Você pode gerenciar regras customizadas e de anomalia.

É possível ativar e desativar as regras, conforme necessário. É possível também editar, copiar ou excluir uma regra.

É possível criar regras de detecção de anomalias somente na guia **Atividade de log**.

Ativando e desativando regras

Ao ajustar seu sistema, você poderá ativar ou desativar as regras apropriadas para assegurar-se de que o sistema irá gerar ofensas significativas para seu ambiente.

Sobre Esta Tarefa

Você deve ter a permissão de função **Atividade de log > Manter regras customizadas** para poder ativar ou desativar uma regra.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Na caixa de listagem **Exibir** na página **Regras**, selecione **Regras**.
4. Selecione a regra que você deseja ativar ou desativar.
5. Na caixa de listagem **Ações**, selecione **Ativar/Desativar**.

Editando uma regra

Você pode editar uma regra para alterar o nome da regra, tipo de regra, testes ou respostas.

Sobre Esta Tarefa

Você deve ter a permissão de função **Atividade de log > Manter regras customizadas** para poder ativar ou desativar uma regra.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Na caixa de listagem **Exibir** na página **Regras**, selecione **Regras**.
4. Dê um clique duplo na regra que você deseja editar.
5. Na caixa de listagem **Ações**, selecione **Abrir**.
6. Opcional. Se você desejar alterar o tipo de regra, clique em **Voltar** e selecione um novo tipo de regra.
7. Na página Editor de pilha de testes de regra, editar os parâmetros.
8. Clique em **Avançar**.
9. Na página Resposta da regra, editar os parâmetros.
10. Clique em **Avançar**.
11. Revise a regra editada. Clique em **Concluir**.

Copiando uma regra

Você pode copiar uma regra existente, inserir um novo nome para a regra, e, em seguida, customizar os parâmetros na nova regra, conforme necessário.

Sobre Esta Tarefa

Você deve ter a permissão de função **Atividade de log > Manter regras customizadas** para poder ativar ou desativar uma regra.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Na caixa de listagem **Exibir**, selecione **Regras**.
4. Selecione a regra que você deseja duplicar.
5. Na caixa de listagem de **Ações**, selecione **Duplicar**.
6. No Inserir nome para o campo de regra copiada, digite um nome para a nova regra. Clique em **OK**.

Excluindo uma regra

Você pode excluir uma regra de seu sistema.

Sobre Esta Tarefa

Você deve ter a permissão de função **Atividade de log > Manter regras customizadas** para poder ativar ou desativar uma regra.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Na caixa de listagem **Exibir**, selecione **Regras**.
4. Selecione a regra que você deseja excluir.
5. Na caixa de listagem **Ações**, selecione **Excluir**.

Gerenciamento de grupo de regras

Se você for um administrador, estará apto a criar, editar e excluir grupos de regras. Categorizar suas regras ou blocos de construção em grupos permite que você visualize e rastreie suas regras de forma eficiente.

Por exemplo, você pode visualizar todas as regras que estão relacionadas à conformidade.

À medida que novas regras são criadas, é possível designar a regra para um grupo existente. Para obter informações sobre como designar um grupo usando o assistente de regra, consulte **Criando um regra customizada** ou **Criando uma regra de detecção de anomalia**.

Visualizando um grupo de regra

Na página **Regras**, você pode filtrar as regras ou blocos de construção para visualizar apenas as regras ou blocos de construção que pertencem a um grupo específico.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Na caixa de listagem **Exibir**, selecione se você deseja visualizar as regras ou blocos de construção.
4. Na caixa de listagem **Filtro**, selecione a categoria do grupo que você deseja visualizar.

Criando um grupo

A página Regras fornece os grupos de regras padrão, no entanto, você pode criar um novo grupo.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Clique em **Grupos**.
4. Na árvore de navegação, selecione o grupo no qual você deseja criar um novo grupo.
5. Clique em **Novo grupo**.
6. Insira valores para os seguintes parâmetros:
 - **Nome** – digite um nome exclusivo para ser designado ao novo grupo. O nome pode ter até 255 caracteres de comprimento.
 - **Descrição** – insira uma descrição que você deseja designar a esse grupo. A descrição pode ter até 255 caracteres de comprimento.
7. Clique em **OK**.
8. Opcional. Para alterar o local do novo grupo, clique no novo grupo e arraste a pasta para o novo local em sua árvore de navegação.

Designando um item a um grupo

É possível designar uma regra selecionada ou um bloco de construção a um grupo.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Selecione a regra ou bloco de construção que deseja designar a um grupo.
4. Na caixa de listagem **Ações**, selecione **Designar grupos**.
5. Selecione o grupo para o qual deseja designar a regra ou o bloco de construção.
6. Clique em **Designar grupos**.
7. Feche a janela **Escolher grupos**.

Editando um grupo

Você pode editar um grupo para alterar o nome ou a descrição.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Clique em **Grupos**.
4. Na árvore de navegação, selecione o grupo que você deseja editar.
5. Clique em **Editar**.
6. Atualize os valores para os parâmetros a seguir:
 - **Nome** – digite um nome exclusivo para ser designado ao novo grupo. O nome pode ter até 255 caracteres de comprimento.
 - **Descrição** – insira uma descrição que você deseja designar a esse grupo. A descrição pode ter até 255 caracteres de comprimento.
7. Clique em **OK**.

8. Opcional. Para alterar o local do grupo, clique no novo grupo e arraste a pasta para o novo local em sua árvore de navegação.

Copiando um item para outro grupo

Você pode copiar um bloco de regra ou construção de um grupo para outros grupos.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Clique em **Grupos**.
4. Na árvore de navegação, selecione o bloco de regra ou construção que deseja copiar para outro grupo.
5. Clique em **Copiar**.
6. Selecione a caixa de seleção para o grupo ao qual você deseja copiar a regra ou o bloco de construção.
7. Clique em **Copiar**.

Excluindo um item de um grupo

É possível excluir um item de um grupo. Quando você excluir um item de um grupo, a regra ou bloco de construção é apenas excluído do grupo; ele permanece disponível na página Regras.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Clique em **Grupos**.
4. Usando a árvore de navegação, navegue e selecione o item que deseja excluir.
5. Clique em **Remover**.
6. Clique em **OK**.

Excluindo um grupo

Você pode excluir um grupo. Ao excluir um grupo, as regras ou os blocos de construção desse grupo permanecerão disponíveis na página Regras.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Clique em **Grupos**.
4. Usando a árvore de navegação, selecione e navegue até o grupo que você deseja excluir.
5. Clique em **Remover**.
6. Clique em **OK**.

Editando blocos de construção

É possível editar qualquer um dos blocos de construção padrão para corresponder com as necessidades de sua implementação.

Sobre Esta Tarefa

Um bloco de construção é uma pilha de testes da regra reutilizável que você pode incluir como um componente em outras regras.

Por exemplo, você pode editar o BB:HostDefinition: bloco de construção dos servidores de correio para identificar todos os servidores de correio na sua implementação. Em seguida, você pode configurar qualquer regra para excluir seus servidores de correio dos testes de regras.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Regras**.
3. Na caixa de listagem **Exibir**, selecione **Blocos de construção**.
4. Dê um clique duplo o bloco de construção que você deseja editar.
5. Atualize o bloco de construção, conforme necessário.
6. Clique em **Avançar**.
7. Continue pelo assistente. Para obter mais informações, consulte Criando uma regra personalizada.
8. Clique em **Concluir**.

Parâmetros de página Regra

Uma descrição dos parâmetros na página Regras.

A lista de regras implementadas fornece as seguintes informações para cada regra:

Tabela 27. Parâmetros da página Regras

Parâmetro	Descrição
Nome da Regra	Exibe o nome da regra.
Grupo	Exibe o grupo ao qual esta regra é designada. Para obter mais informações sobre grupos, consulte Gerenciamento de regras de grupo.
Rule Category	Exibe a categoria de regra para a regra. As opções incluem Regra personalizada e Regra de detecção de anomalias.
Tipo de Regras	Exibe o tipo de regra.
Ativado	Indica se a regra está ativada ou desativada. Para obter mais informações sobre a ativação e desativação de regras, consulte Ativando e desativando regras.

Tabela 27. Parâmetros da página Regras (continuação)

Parâmetro	Descrição
Response	Exibe a resposta da regra, se houver. Respostas de regra incluem: <ul style="list-style-type: none"> • Enviar Novo Evento • Email • Notificação de log • SNMP • Conjunto de referência • Dados de referência • Resposta IF-MAP Para obter mais informações sobre as respostas de regra, consulte Respostas de regra.
Contagem de eventos	Exibe o número de eventos que são associados a esta regra quando a regra contribuir para uma ofensa.
Origin	Exibe se essa regra será uma regra padrão (Sistema) ou uma regra customizada (Usuário).
Data de Criação	Especifica a data e hora que essa regra foi criada.
Data da Modificação	Especifica a data e hora que essa regra foi modificada.

Barra de ferramentas da página Regras

A barra de ferramentas da página Regras é usada para exibir as regras, blocos de construção ou grupos. É possível gerenciar grupos de regras e trabalhar com regras.

A barra de ferramentas da página Regras fornece as seguintes funções:

Tabela 28. Função da barra de ferramentas da página Regras

Função	Descrição
Exibir	Na caixa de listagem, selecione se deseja exibir as regras ou blocos de construção na lista de regras.
Grupo	Na caixa de listagem, selecione qual grupo de regra que deseja que seja exibido na lista de regras.
Grupos	Clique em Grupos para gerenciar grupos de regra.

Tabela 28. Função da barra de ferramentas da página Regras (continuação)

Função	Descrição
Ações	<p>Clique em Ações e selecione uma das opções a seguir:</p> <ul style="list-style-type: none"> • Nova regra de evento – Selecione esta opção para criar uma nova regra de evento. • Ativar/Desativar – Selecione esta opção para ativar ou desativar as regras selecionadas. • Duplicar – Selecione esta opção para copiar uma regra selecionada. • Editar – Selecione esta opção para editar uma regra selecionada. • Excluir – Selecione esta opção para excluir uma regra selecionada. • Designar grupos – Selecione esta opção para designar regras selecionadas para grupos de regra.
Reverter regra	<p>Clique em Reverter regra para reverter uma regra do sistema modificada para o valor padrão. Ao clicar em Reverter regra, uma janela de confirmação será exibida. Ao reverter uma regra, quaisquer modificações anteriores são removidas permanentemente.</p> <p>Para reverter a regra e manter uma versão modificada, duplique a regra e use a opção Reverter regra na regra modificada.</p>
Procurar regras	<p>Digite seus critérios de procura no campo Procurar regras e clique no ícone Procurar regras ou pressione Enter no teclado. Todas as regras que correspondem aos seus critérios de procura serão exibidas na lista de regras.</p> <p>Procura-se, nos parâmetros a seguir, uma correspondência com seus critérios de procura:</p> <ul style="list-style-type: none"> • Nome da Regra • Rule (description) • Comunicados • Response <p>O recurso Procurar regra tenta localizar uma correspondência da sequência de texto direta. Se nenhuma correspondência for encontrada, o recurso Procurar regra tentará uma correspondência de expressão regular (regex).</p>

Parâmetros da página Resposta de regra

Há parâmetros para a página Resposta de regra.

A tabela a seguir fornece os parâmetros da página Resposta de regra.

Tabela 29. Parâmetros de página Resposta de regra comum, de fluxo e de evento

Parâmetro	Descrição
Gravidade	Selecione esta caixa de seleção se quiser que essa regra configure ou ajuste a severidade. Quando selecionada, será possível usar as caixas de listagem para configurar o nível de severidade apropriado.
Credibilidade	Selecione esta caixa de seleção se quiser que essa regra configure ou ajuste credibilidade. Quando selecionada, será possível usar as caixas de listagem para configurar o nível de credibilidade apropriado.
Relevância	Selecione esta caixa de seleção se quiser que essa regra configure ou ajuste a relevância. Quando selecionada, será possível usar as caixas de listagem para configurar o nível de relevância apropriado.
Annotate event	Selecione essa caixa de seleção se desejar incluir uma anotação a este evento e digite a anotação que deseja incluir no evento.
Drop the detected event	Selecione esta caixa de seleção para forçar um evento, que normalmente é enviado para o componente Magistrate, a ser enviado para o banco de dados Ariel, para geração de relatórios ou pesquisa.
Enviar Novo Evento	Selecione essa caixa de seleção para enviar um novo evento além do evento original, que é processado como todos os outros eventos no sistema. Os parâmetros Dispatch New Event serão exibidos ao selecionar esta caixa de seleção. Por padrão, a caixa de seleção não é selecionada.
Nome do evento	Digite um nome exclusivo do evento que deseja que seja exibido na guia Atividade de log .
Descrição do Evento	Digite uma descrição do evento. A descrição é exibida na área de janela Anotações dos detalhes do evento.
Gravidade	Na caixa de listagem, selecione a severidade do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 0. A Severidade é exibida na área de janela Anotação dos detalhes do evento.
Credibilidade	Na caixa de listagem, selecione a credibilidade do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 10. A credibilidade é exibida na área de janela Anotação dos detalhes do evento.
Relevância	Na caixa de listagem, selecione a relevância do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 10. A relevância é exibida na área de janela Anotação dos detalhes do evento.
High-Level Category	Na caixa de listagem, selecione a categoria de evento de alto nível que deseja que esta regra use ao processar eventos.

Tabela 29. Parâmetros de página Resposta de regra comum, de fluxo e de evento (continuação)

Parâmetro	Descrição
Low-Level Category	Na caixa de listagem, selecione a categoria de evento de baixo nível que deseja que esta regra use ao processar eventos.
Email	Selecione essa caixa de seleção para exibir as opções de email. Por padrão, a caixa de seleção não é selecionada.
Enter email addresses to notify	Digite o endereço de email para enviar uma notificação se esta regra for gerada. Use uma vírgula para separar vários endereços de email.
SNMP Trap	<p>Esse parâmetro só será exibido quando os parâmetros SNMP Settings forem definidos nas configurações do sistema.</p> <p>Selecione esta caixa de seleção para ativar que esta regra envie uma notificação SNMP (trap).</p> <p>A saída de trap SNMP inclui o tempo do sistema, o OID de trap e os dados de notificação, conforme definidos pelo MIB.</p>
Enviar para syslog local	<p>Selecione essa caixa de seleção se desejar registrar o evento localmente.</p> <p>Por padrão, essa caixa de seleção está limpa.</p> <p>Nota: Apenas os eventos normalizados podem ser registrados localmente em um dispositivo. Se desejar enviar dados do evento brutos, deverá usar a opção Enviar para destinos de encaminhamento para enviar os dados para um host syslog remoto.</p>
Enviar para Destinos de Encaminhamento	<p>Esta caixa de seleção será exibida apenas para regras de eventos.</p> <p>Selecione essa caixa de seleção se desejar registrar o evento ou fluxo em um destino de encaminhamento. Um destino de encaminhamento é um sistema fornecedor, como SIEM, chamado ou sistemas de alerta. Ao selecionar essa caixa de seleção, uma lista de destinos de encaminhamento será exibida. Selecione a caixa de seleção para o destino de encaminhamento para o qual deseja enviar este evento ou fluxo.</p> <p>Para incluir, editar ou excluir um destino de encaminhamento, clique no link Gerenciar destinos.</p>
Notify	<p>Selecione essa caixa de seleção se desejar que os eventos que são gerados como resultado desta regra sejam exibidos no item Notificações do sistema na guia Painel.</p> <p>Se ativar notificações, configure o parâmetro Response Limiter.</p>

Tabela 29. Parâmetros de página Resposta de regra comum, de fluxo e de evento (continuação)

Parâmetro	Descrição
Add to Reference Set	<p>Selecione essa caixa de seleção se desejar que eventos que são gerados como resultado desta regra incluam dados em um conjunto de referência.</p> <p>Para incluir dados em um conjunto de referência:</p> <ol style="list-style-type: none"> 1. Usando a caixa de listagem pela primeira vez, selecione os dados que deseja incluir. As opções incluem todos os dados normalizados ou customizados. 2. Usando a segunda caixa de listagem, selecione a referência que está configurada para a qual você deseja incluir os dados especificados. <p>A resposta de regra Incluir ao conjunto de referência fornece as seguintes funções:</p> <p>Atualizar Clique em Atualizar para atualizar a primeira caixa de listagem para assegurar-se de que a lista é atual.</p> <p>Configurar Conjuntos de Referência Clique em Configurar conjuntos de referência para configurar o conjunto de referência. Esta opção estará disponível apenas se tiver permissões administrativas.</p>

Tabela 29. Parâmetros de página Resposta de regra comum, de fluxo e de evento (continuação)

Parâmetro	Descrição
Incluir de Dados de Referência	<p>Antes de poder usar essa resposta de regra, você deverá criar a coleta de dados de referência usando a interface da linha de comandos (CLI). Para obter mais informações sobre como criar e usar as coletas de dados de referência, consulte o <i>Guia de Administração</i> do seu produto.</p> <p>Selecione essa caixa de seleção se desejar que eventos que são gerados como resultado dessa regra sejam incluídos em uma coleta de dados de referência. Após selecionar a caixa de seleção, selecione uma das seguintes opções:</p> <p>Incluir em um Mapa de Referência Selecione esta opção para enviar dados para uma coleção de pares de chave única/valor múltiplo. Deve-se selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência no qual deseja incluir o registro de dados.</p> <p>Incluir em um Mapa de Referência de Conjuntos Selecione esta opção para enviar dados para uma coleção de pares de chave/valor único. Deve-se selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência de conjuntos no qual deseja incluir o registro de dados.</p> <p>Incluir em um Mapa de Referência de Mapas Selecione esta opção para enviar dados para uma coleção de pares de chave múltipla/valor único. É necessário selecionar uma chave para o primeiro mapa, uma chave para o segundo mapa e, em seguida, o valor para o registro de dados. Deve-se também selecionar o mapa de referência de mapas nos quais deseja incluir o registro de dados.</p> <p>Incluir em uma Tabela de Referência Selecione esta opção para enviar dados para uma coleção de pares de chave única/valor múltiplo, onde um tipo foi designado para as chaves secundárias. Selecione a tabela de referência para a qual deseja incluir dados e, em seguida, selecione uma chave primária. Selecione suas chaves internas (chaves secundárias) e seus valores para os registros de dados.</p>
Publish on the IF-MAP Server	Se os parâmetros IF-MAP estiverem configurados e implementados nas configurações do sistema, selecione esta opção para publicar as informações de evento do servidor IF-MAP.
Limitador de Resposta	Selecione esta caixa de seleção e use as caixas de listagem para configurar a frequência com a qual deseja que esta regra responda.
Enable Rule	Selecione esta caixa de seleção para ativar esta regra.

Uma notificação SNMP pode se parecer com:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -  
Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:  
ICMP Destination Unreachable Communication with Destination Host is  
Administratively Prohibited, QID: 1000156, Category: 1014, Notes:  
Offense description"
```

Uma saída de syslog pode se parecer com:

```
Sep 28 12:39:01 localhost.localdomain ECS:  
Rule 'Name of Rule' Fired: 172.16.60.219:12642  
-> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:  
1000398, Category: 1011, Notes: Event description
```

Capítulo 9. Perfis de ativos

Os perfis de ativos fornecem informações sobre cada ativo conhecido em sua rede, incluindo quais serviços estão em execução em cada ativo.

A informação do perfil de ativos é usada para finalidades de correlação para ajudar a reduzir positivos falsos. Por exemplo, se uma origem tentar explorar um serviço específico em execução em um ativo, em seguida, o QRadar determinará se o ativo está vulnerável a este ataque correlacionando o ataque com o perfil de ativos.

Perfis de ativos serão descobertos automaticamente se você tiver as varreduras de avaliação de vulnerabilidades (VA) configuradas.

Sobre as vulnerabilidades

É possível usar o QRadar Vulnerability Manager e os scanners de terceiros para identificar vulnerabilidades.

Scanners de terceiros identificam e relatam as vulnerabilidades descobertas usando referências externas, como o Banco de Dados de Vulnerabilidade de Software Livre (OSVDB), Banco de Dados de Vulnerabilidade Nacional (NVDB) e Critical Watch. Exemplos de scanners de terceiros incluem QualysGuard e nCircle ip360. O OSVDB designa um identificador de referência exclusiva (ID do OSVDB) para cada vulnerabilidade. Referências externas designam um identificador de referência exclusivo para cada vulnerabilidade. Exemplos de IDs de referência de dados externos incluem ID de Common Vulnerability and Exposures (CVE) ou ID de Bugtraq. Para obter mais informações sobre os scanners e avaliação de vulnerabilidades, consulte o *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

QRadar Vulnerability Manager é um componente que você pode adquirir separadamente e ativar usando uma chave de licença. QRadar Vulnerability Manager é uma plataforma de varredura de rede que fornece reconhecimento das vulnerabilidades existentes nos aplicativos, sistemas ou dispositivos em sua rede. Depois que as varreduras identificarem vulnerabilidades, você poderá procurar e revisar dados de vulnerabilidade, corrigir vulnerabilidades e executar novamente varreduras para avaliar o novo nível de risco.

Quando QRadar Vulnerability Manager for ativado, você pode executar tarefas de avaliação de vulnerabilidades na guia **Vulnerabilidades**. Na guia **Ativos**, é possível executar varreduras nos ativos selecionados.

Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Vulnerability Manager*

Visão geral da guia Ativos

A guia **Ativos** fornece a você uma área de trabalho a partir da qual você pode gerenciar seus ativos de rede e investigar as vulnerabilidades de ativo, portas, aplicativos, histórico e outras associações.

Usando a guia **Ativos**, você pode:

- Visualizar todos os ativos descobertos.
- Inclua perfis de ativos manualmente.
- Procurar ativos específicos.
- Visualizar informações sobre ativos descobertos.
- Edite perfis de ativos para ativos manualmente incluídos ou descobertos.
- Ajustar vulnerabilidades de positivo falso.
- Importar ativos.
- Imprima ou exporte perfis de ativo.
- Descubrir os ativos.
- Configurar e gerenciar varreduras de vulnerabilidade de terceiros.
- Inicie varreduras de Gerenciador de Vulnerabilidade QRadar.

Para obter mais informações sobre a opção Varrer VA na área de janela de navegação, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.

Lista da guia Ativo

A página de Perfis de ativos fornece informações sobre ID, endereço IP, nome do ativo, pontuação do CVSS agregado, vulnerabilidades e serviços.

A página de Perfis de ativos fornece as seguintes informações sobre cada ativo:

Tabela 30. Parâmetros da página Perfil de Ativos

Parâmetro	Descrição
ID	Exibe o número de ID de Ativo do ativo. O número de ID do Ativo é gerado automaticamente quando você inclui um perfil de ativos manualmente ou quando os ativos são descobertos pelas varreduras de evento ou vulnerabilidade.
Endereço IP	Exibe o último endereço IP conhecido do ativo.
Nome do ativo	Exibe o nome fornecido, nome do NetBios, nome de DSN ou o endereço MAC do ativo. Se desconhecido, esse campo exibirá o último endereço IP conhecido. Nota: Estes valores são exibidos em ordem de prioridade. Por exemplo, se o ativo não tiver um nome fornecido, o nome do NetBios agregado será exibido. Se o ativo for descoberto automaticamente, esse campo será preenchido automaticamente, no entanto, você poderá editar o nome do ativo, se necessário.

Tabela 30. Parâmetros da página Perfil de Ativos (continuação)

Parâmetro	Descrição
Pontuação de risco	<p>Exibe uma das seguintes pontuações do Common Vulnerability Scoring System (CVSS):</p> <ul style="list-style-type: none"> • Pontuação do CVSS ambiental agregado unido • Pontuação do CVSS temporal agregado • Pontuação base do CVSS agregado • <p>Essas pontuações são exibidas em ordem de prioridade. Por exemplo, se a pontuação do CVSS ambiental agregado unido não estiver disponível, pontuação do CVSS temporal agregado será exibida.</p> <p>Uma pontuação de CVSS é uma métrica de avaliação para a gravidade de uma vulnerabilidade. Você pode usar pontuações do CVSS para medir o quanto uma vulnerabilidade garante em comparação a outras vulnerabilidades.</p> <p>A pontuação do CVSS é calculada nos seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> • Potencial de Danos Colaterais • Requisitos de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade <p>Para obter mais informações sobre como configurar esses parâmetros, consulte “Incluindo ou editando um perfil de ativo” na página 106.</p> <p>Para obter mais informações sobre CVSS, consulte http://www.first.org/cvss/.</p>
Vulnerabilidades	Exibe o número de vulnerabilidades exclusivas que são descobertas neste ativo. Este valor também inclui o número de vulnerabilidades ativas e passivas.
Serviços	Exibe o número de aplicativos de Camada 7 exclusivos executados neste ativo.
Último Usuário	Exibe o último usuário associado ao ativo.
Último Usuário Visto	Exibe a hora em que o último usuário associado ao ativo foi visto.

Barra de ferramentas da guia Ativos

A barra de ferramentas da página de Perfis de ativos permite que você procure, salve, inclua, limpe, edite e execute outras ações nos ativos.

A barra de ferramentas da página de Perfis de ativos fornece as seguintes funções:

Tabela 31. Funções da barra de ferramentas da página de Perfis de Ativos

Função	Descrição
Procurar	<p>Clique em Procurar para executar procuras avançadas em ativos. As opções incluem:</p> <ul style="list-style-type: none"> • Nova procura – Selecione esta opção para criar uma nova procura de ativo. • Editar procura – Selecione esta opção para editar uma procura de ativo. <p>Para obter mais informações sobre o recurso de procura, consulte Procurando perfis de ativos.</p>
Procuras rápidas	<p>Nessa caixa de listagem, é possível executar procuras salvas anteriormente. As opções são exibidas na caixa de listagem Procuras rápidas apenas quando você tiver critérios de procura salva que especificam a opção Incluir em minhas procuras rápidas.</p>
Salvar critérios	<p>Clique em Salvar critérios para salvar os critérios de procura atuais.</p>
Incluir filtro	<p>Clique em Incluir filtro para incluir um filtro aos resultados da procura atual.</p>
Incluir ativo	<p>Clique em Incluir ativo para incluir um perfil de ativos. Consulte Incluindo ou editando um perfil de ativos.</p>
Editar ativo	<p>Clique em Editar ativo para editar um perfil de ativos. Esta opção é ativada apenas se você tiver selecionado um perfil de ativos na lista de resultados. Consulte “Incluindo ou editando um perfil de ativo” na página 106.</p>

Tabela 31. Funções da barra de ferramentas da página de Perfis de Ativos (continuação)

Função	Descrição
Ações	<p>Clique em Ações para executar as seguintes ações:</p> <ul style="list-style-type: none"> • Excluir ativo – Selecione esta opção para excluir os perfis de ativos selecionados. Consulte Excluindo ativos. • Excluir listados – Selecione esta opção para excluir todos os perfis de ativos que estão listados na lista de resultados. Consulte Excluindo ativos. • Importar ativos – Selecione essa opção para importar ativos. Consulte Importando perfis de ativos. • Exportar para XML – Selecione esta opção para exportar perfis de ativos no formato XML. Consulte Exportando ativos. • Exportar para CSV – Selecione esta opção para exportar perfis de ativos no formato CSV. Consulte Exportando ativos. • Imprimir – Selecione esta opção para imprimir perfis de ativos que são exibidos na página. • <p>O menu Ações estará disponível apenas se você tiver privilégios administrativos.</p>
Limpar filtro	<p>Depois de aplicar um filtro usando a opção Incluir filtro, você pode clicar em Limpar filtro para remover o filtro.</p>

Opções de menu ativado pelo botão direito

Clicar com o botão direito em um ativo na guia Ativo exibe os menus Navegar, Informações e Executar varredura de QVM para obter mais informações sobre filtro de eventos.

Na guia **Ativos**, é possível clicar com o botão direito em um ativo para acessar mais informações de filtro de eventos.

Tabela 32. Opções de menu ativado pelo botão direito

Opção	Descrição
Informações	<p>O menu Informações fornece as seguintes opções:</p> <ul style="list-style-type: none"> • Consulta DNS – Procura por entradas de DNS que são baseadas no endereço IP. • Consulta WHOIS - Procura o proprietário registrado de um endereço IP remoto. O servidor WHOIS padrão é whois.arin.net. • Varredura de porta – Desempenha uma varredura de Mapeador de Rede (NMAP) do endereço IP selecionado. Essa opção estará disponível apenas se o NMAP estiver instalado em seu sistema. Para obter mais informações sobre a instalação do NMAP, consulte a documentação do seu fornecedor. • Perfil de ativo – Exibe informações de perfil de ativo. Essa opção de menu só ficará disponível quando um dado de perfil for adquirido ativamente por uma varredura. • Procurar eventos – Selecione a opção Procurar eventos para procurar eventos que são associados a este endereço IP.
Executar varredura do QVM	<p>Selecione esta opção para executar uma varredura do Gerenciador de Vulnerabilidades no ativo selecionado.</p> <p>Essa opção será exibida somente depois que você instalar o QRadar Vulnerability Manager.</p>

Visualizando um perfil de ativos

Na lista de ativos na guia **Ativos**, você pode selecionar e visualizar um perfil de ativos. Um perfil de ativos fornece as informações sobre cada perfil.

Sobre Esta Tarefa

As informações do perfil de ativos são descobertas automaticamente por meio do Discovery Server ou configuradas manualmente. Você pode editar automaticamente as informações do perfil de ativos geradas.

A página Perfil de ativos fornece as informações sobre o ativo organizado em várias áreas. Para visualizar uma área de janela, você pode clicar na seta (>) na área de janela para visualizar mais detalhes ou selecionar a área da caixa de listagem **Exibir** na barra de ferramentas.

A barra de ferramentas da página Perfil de ativos fornece as seguintes funções:

Tabela 33. Funções da barra de ferramentas da página perfil de ativos

Opções	Descrição
Retornar à lista de ativos	Clique nesta opção para retornar à lista de ativos.
Exibir	<p>Na caixa de listagem, você pode selecionar a área de janela que deseja visualizar na área de janela do Perfil de Ativos. As áreas de janela Resumo de Ativos e Resumo de Interface de Rede são sempre exibidas.</p> <p>Para obter mais informações sobre os parâmetros exibidos em cada área de janela, consulte Parâmetros da página do perfil.</p>
Editar ativos	Clique nesta opção para editar o Perfil de Ativos. Consulte “Incluindo ou editando um perfil de ativo” na página 106.
Visualizar resumo de destino	Se este ativo for o destino de uma ofensa, esta opção permitirá que você visualize as informações de resumo de destino.
Histórico	<p>Clique em Histórico para visualizar as informações de histórico de evento para este ativo. Quando você clica no ícone Histórico, a janela Procura de eventos é exibida, pré-preenchida com o critério de procura de eventos:</p> <p>Você pode customizar os parâmetros de procura, se necessário. Clique em Procura para visualizar as informações de histórico de eventos.</p>
Aplicativos	<p>Clique em Aplicativos para visualizar as informações do aplicativo para este ativo. Quando você clica no ícone Aplicativos, a janela Procura de fluxo é exibida, pré-preenchida com o critério de procura do evento.</p> <p>Você pode customizar os parâmetros de procura, se necessário. Clique em Procura para visualizar as informações do aplicativo.</p>
Procurar conexões	<p>Clique em Procurar conexões para procurar por conexões. A janela Procurar conexão é exibida.</p> <p>Esta opção será exibida apenas quando o IBM Security QRadar Risk Manager for comprado e licenciado. Para obter mais informações, consulte o <i>Guia do Usuário do IBM Security QRadar Risk Manager</i>.</p>
Visualização da topologia	Esta opção será exibida apenas quando o IBM Security QRadar Risk Manager for comprado e licenciado. Para obter mais informações, consulte o <i>Guia do Usuário do IBM Security QRadar Risk Manager</i> .
Ações	<p>Na lista Ações, selecione Histórico de vulnerabilidade.</p> <p>Esta opção será exibida apenas quando o IBM Security QRadar Risk Manager for comprado e licenciado. Para obter mais informações, consulte o <i>Guia do Usuário do IBM Security QRadar Risk Manager</i>.</p>

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**
3. Clique duas vezes no ativo que você deseja visualizar.
4. Use as opções na barra de ferramentas para exibir as várias áreas de janela das informações do perfil de ativos. Consulte Editando um perfil de ativos.
5. Para pesquisar as vulnerabilidades associadas, clique em cada vulnerabilidade na área de janela Vulnerabilidades. Consulte a Tabela 10-10.
6. Se necessário, edite o perfil de ativos. Consulte Editando um perfil de ativos.
7. Clique em **Retornar à lista de ativos** para selecionar e visualizar outro ativo, se necessário.

Incluindo ou editando um perfil de ativo

Os perfis de ativos são descobertos e incluídos automaticamente; no entanto, pode ser necessário incluir um perfil manualmente

Sobre Esta Tarefa

Quando os ativos forem descobertos usando a opção Descoberta de Servidor, alguns detalhes do perfil de ativos serão preenchidos automaticamente. É possível incluir manualmente as informações no perfil de ativo e editar determinados parâmetros.

Você pode editar somente os parâmetros que foram inseridos manualmente. Os parâmetros que foram gerados pelo sistema são exibidos em itálico e não são editáveis. Você pode excluir os parâmetros gerados pelo sistema, se necessário.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Escolha uma das opções a seguir:
 - Para incluir um ativo, clique em **Incluir ativo** e insira o endereço IP ou o intervalo do CIDR do ativo no campo **Novo endereço IP**.
 - Para editar um ativo, dê um clique duplo no ativo que você deseja visualizar e clique em **Editar ativo**.
4. Configure os parâmetros na área de janela Endereço IP & MAC. Configure uma ou mais das seguintes opções:
 - Clique no ícone **Novo endereço MAC** e insira um Endereço MAC na caixa de diálogo.
 - Clique no ícone **Novo endereço IP** e insira um endereço IP na caixa de diálogo.
 - Se **NIC desconhecido** for listado, você poderá selecionar esse item, clicar no ícone **Editar** e inserir um novo endereço MAC na caixa de diálogo.
 - Selecione um endereço IP ou MAC na lista, clique no ícone **Editar** e insira um novo endereço MAC na caixa de diálogo.
 - Selecione um endereço IP ou MAC na lista e clique no ícone **Remover**.
5. Configure os parâmetros na área de janela Nomes & Descrição. Configure uma ou mais das seguintes opções:

Parâmetro	Descrição
DNS	Escolha uma das opções a seguir: <ul style="list-style-type: none"> • Insira um nome de DNS e clique em Incluir. • Selecione um nome DNS na lista e clique em Editar. • Selecione um nome do DNS na lista e clique em Remover.
NetBIOS	Escolha uma das opções a seguir: <ul style="list-style-type: none"> • Insira um nome de NetBIOS e clique em Incluir. • Selecione um nome de NetBIOS na lista e clique em Editar. • Selecione um nome de NetBIOS na lista e clique em Remover.
Nome Dado	Insira um nome para esse perfil de ativos.
Local	Insira um local para esse perfil de ativos.
Descrição	Insira uma descrição para o perfil de ativos.
AP Wireless	Insira o Ponto de Acesso (AP) wireless para esse perfil de ativos.
SSID Wireless	Insira o Service Set Identifier (SSID) do wireless para esse perfil de ativos.
ID do Computador	Insira o ID do computador para esse perfil de ativos.
ID da Porta do Computador	Insira o ID de porta do computador para esse perfil de ativos.

6. Configure os parâmetros na área de janela Sistema Operacional:
 - a. Na caixa de listagem **Fornecedor**, selecione um fornecedor do sistema operacional.
 - b. Na caixa de listagem **Produto**, selecione o sistema operacional para o perfil de ativos.
 - c. Na caixa de listagem **Versão**, selecione a versão para o sistema operacional selecionado.
 - d. Clique no ícone **Incluir**.
 - e. Na caixa de listagem **Substituir**, selecione uma das opções a seguir:
 - **Até a próxima varredura** – selecione essa opção para especificar que o scanner forneça as informações do sistema operacional e as informações que possam ser editadas temporariamente. Se você editar os parâmetros do sistema operacional, o scanner irá restaurar as informações em sua próxima varredura.
 - **Contínuo** – selecione essa opção para especificar que você deseja inserir manualmente as informações do sistema operacional e desativar o scanner de atualizar as informações.
 - f. Selecione um sistema operacional na lista.
 - g. Selecione um sistema operacional e clique no ícone **Alternar substituição**.
7. Configure os parâmetros na área de janela CVSS & Peso. Configure uma ou mais das seguintes opções:

Parâmetro	Descrição
Potencial de Danos Colaterais	<p>Configure esse parâmetro para indicar o potencial de perda ativos de vidas ou físicos através de danos ou furtos desse ativo. Você também pode usar esse parâmetro para indicar um potencial de perda econômica de produtividade ou renda. O potencial de dano colateral maior aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem Potencial de dano colateral, selecione uma das opções a seguir:</p> <ul style="list-style-type: none"> • Nenhum • Baixo • Médio baixo • Médio alto • Alto • Não definido <p>Ao configurar o parâmetro Collateral Damage Potential, o parâmetro Weight será atualizado automaticamente.</p>
Requisitos de Confidencialidade	<p>Configure esse parâmetro para indicar o impacto sobre a confidencialidade de uma vulnerabilidade explorada com êxito nesse ativo. O impacto de confidencialidade maior aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem Requisito de confidencialidade, selecione uma das opções a seguir:</p> <ul style="list-style-type: none"> • Baixo • Médio • Alto • Não definido
Requisito de Disponibilidade	<p>Configure esse parâmetro para indicar o impacto na disponibilidade do ativo quando uma vulnerabilidade for explorada com sucesso. Os ataques que consumem a largura da banda da rede, os ciclos do processador ou o espaço em disco impactará a disponibilidade de um ativo. O impacto de disponibilidade maior aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem Requisito de disponibilidade, selecione uma das opções a seguir:</p> <ul style="list-style-type: none"> • Baixo • Médio • Alto • Não definido

Parâmetro	Descrição
Requisito de Integridade	<p>Configure esse parâmetro para indicar o impacto na integridade do ativo quando uma vulnerabilidade for explorada com êxito. A integridade refere-se à fidelidade e a veracidade garantida de informações. O impacto de integridade maior aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem Requisito de integridade, selecione uma das opções a seguir:</p> <ul style="list-style-type: none"> • Baixo • Médio • Alto • Não definido
Peso	<p>Na caixa de listagem Peso, selecione um peso para esse perfil de ativos. O intervalo é 0 – 10.</p> <p>Ao configurar o parâmetro Weight, o parâmetro Collateral Damage Potential será atualizado automaticamente.</p>

8. Configure os parâmetros na área de janela Proprietário. Escolha uma ou mais das seguintes opções:

Parâmetro	Descrição
Proprietário de Negócios	Insira o nome do proprietário de negócios do ativo. Um exemplo de um proprietário de negócios é um gerente do departamento. O comprimento máximo é de 255 caracteres.
Contato do Proprietário de Negócios	Insira as informações de contato para o proprietário de negócios. O comprimento máximo é de 255 caracteres.
Responsável Técnico	Insira o proprietário técnico do ativo. Um exemplo de um proprietário de negócios é o gerente de TI ou diretor. O comprimento máximo é de 255 caracteres.
Contato do Responsável Técnico	Insira as informações de contato para o responsável técnico. O comprimento máximo é de 255 caracteres.
Usuário Técnico	<p>Na caixa de listagem, selecione o nome do usuário que você deseja associar a esse perfil de ativos.</p> <p>Você também pode usar esse parâmetro para ativar a correção de vulnerabilidade automática para o IBM Security QRadar Vulnerability Manager. Para obter mais informações sobre a correção automática, consulte o <i>Guia do Usuário do IBM Security QRadar Vulnerability Manager</i>.</p>

9. Clique em **Salvar**.

Procurando perfis de ativos

Você pode configurar os parâmetros de procura para exibir apenas os perfis de ativos que você deseja investigar a partir da página Ativo na guia **Ativos**.

Sobre Esta Tarefa

Ao acessar a guia **Ativos**, a página Ativo é exibida preenchida com todos os ativos descobertos em sua rede. Para refinar esta lista, você pode configurar os parâmetros de procura para exibir apenas os perfis de ativos que você deseja investigar.

Na página Procura de ativos, você pode gerenciar os Grupos de Procura de Ativos. Para obter mais informações sobre Grupos de Procura de Ativos, consulte Consulte grupos de procura de ativos.

O recurso de procura permite que você procure perfis do host, ativos e informações de identificação. As informações de identificação fornecem mais detalhes sobre as origens de log em sua rede, incluindo informações de DNS, logins do usuário e endereços MAC.

Usando o recurso de procura de ativo, você pode procurar por ativos pelas referências de dados externos para determinar se as vulnerabilidades conhecidas existem em sua implementação.

Por exemplo:

Você receberá uma notificação de que ID CVE: CVE-2010-000 é ativamente usada no campo. Para verificar se quaisquer hosts em sua implementação são vulneráveis a esta exploração, você pode selecionar **Referência externa de vulnerabilidade** na lista de parâmetros de procura, selecionar **CVE**, e, em seguida, inserir o 2010-000

Para visualizar uma lista de todos os hosts vulneráveis a este ID CVE específico.

Nota: Para obter mais informações sobre o OSVDB, consulte <http://osvdb.org/> . Para obter mais informações sobre o NVDB, consulte <http://nvd.nist.gov/> .

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Na barra de ferramentas, clique em **Procura > Nova procura**.
4. Escolha uma das opções a seguir:
 - Para carregar uma procura salva anteriormente, vá para a Etapa 5.
 - Para criar uma nova procura, vá para a Etapa 6.
5. Selecione uma procura salva anteriormente:
 - a. Escolha uma das opções a seguir:
 - Opcional. Na caixa de listagem **Grupo**, selecione o grupo de procura de ativo que você deseja exibir na lista **Procuras salvas disponíveis**.
 - Na lista **Procuras salvas disponíveis**, selecione a procura salva que você deseja carregar.

- No campo **Digitar procura salva ou selecionar na lista**, digite o nome da procura que você deseja carregar.
 - b. Clique em **Carregar**.
6. Na área de janela Parâmetros de Procura, defina seus critérios de procura:
 - a. Na primeira caixa de listagem, selecione o parâmetro de ativos que você deseja procurar. Por exemplo, **Nome do host**, **Classificação de risco de vulnerabilidade** ou **Responsável técnico**.
 - b. Na segunda caixa de listagem, selecione o modificador que você deseja usar para a procura.
 - c. No campo de entrada, digite as informações específicas relacionadas ao seu parâmetro de procura.
 - d. Clique em **Incluir filtro**.
 - e. Repita estas etapas para cada filtro que você deseja incluir no critério de procura.
 7. Clique em **Procurar**.

Resultados

Você pode salvar seu critério de procura de ativo. Consulte Salvando critério de procura de ativo.

Salvando critérios de procura de ativos

Na guia **Ativo**, você pode salvar os critérios de procura configurados para que você possa reutilizar os critérios. Os critérios de procura salvos não expiram.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Execute uma procura. Consulte Procurando perfis de ativos.
4. Clique em **Salvar critérios**.
5. Insira os valores para os parâmetros:

Parâmetro	Descrição
Enter the name of this search	Digite o nome exclusivo que deseja designar a esses critérios de procura.
Manage Groups	Clique em Gerenciar grupos para gerenciar grupos de procura. Para obter mais informações, consulte Grupos de procuras de ativos. Essa opção será exibida somente se você tiver as permissões administrativas.
Assign Search to Group(s)	Selecione a caixa de seleção para o grupo que você deseja designar a essa procura salva. Se você não selecionar um grupo, essa procura salva será designada para o grupo Outros por padrão. Para obter mais informações, consulte Grupos de procuras de ativos.
Include in my Quick Searches	Selecione essa caixa de seleção para incluir essa procura na caixa de listagem Procura rápida que está na barra de ferramentas da guia Ativos .

Parâmetro	Descrição
Set as Default	Selecione essa caixa de seleção para configurar essa procura como a procura padrão ao acessar a guia Ativos .
Share with Everyone	Selecione essa caixa de seleção para compartilhar esses requisitos de procura com todos os usuários.

Grupos de procura de ativos

Usando a janela Grupos de procura de ativos, você pode criar e gerenciar grupos de procura de ativos.

Esses grupos permitem que você localize facilmente critérios de procura salva na guia **Ativos**.

Visualizando grupos de procura

Use a janela Grupos de procura de ativos para visualizar uma lista de grupos e subgrupos.

Sobre Esta Tarefa

Na janela Grupos de procura de ativos, você pode visualizar detalhes sobre cada grupo, incluindo uma descrição e a data em que o grupo foi modificado pela última vez.

Todas as procuras salvas não designadas a um grupo estão no grupo **Outros**.

A janela Grupos de procura de ativos exibe os seguintes parâmetros para cada grupo:

Tabela 34. Funções da barra de ferramentas da janela grupos de procura de ativos

Função	Descrição
Novo grupo	Para criar um grupo de procura novo, você pode clicar em Novo grupo . Consulte Consulte criando um grupo de procura novo.
Editar	Para editar um grupo de procura existente, você pode clicar em Editar . Consulte Consulte editando um grupo de procura.
Copiar	Para copiar uma procura salva para outro grupo de procura, você pode clicar em Copiar . Consulte Consulte copiando uma procura salva para outro grupo.
Remover	Para remover um grupo de procura ou uma procura salva de um grupo de procura, selecione o item que deseja remover, e, em seguida, clique em Remover . Consulte Consulte removendo um grupo ou uma procura salva de um grupo.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procura > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Visualize os grupos de procura.

Criando um novo grupo de procura

Na janela Grupos de procura de ativos, você pode criar um novo grupo de procura.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a pasta para o grupo no qual você deseja criar o novo grupo.
6. Clique em **Novo grupo**.
7. No campo **Nome**, digite um nome exclusivo para o novo grupo.
8. Opcional. No campo **Descrição**, digite uma descrição.
9. Clique em **OK**.

Editando um grupo de procura

Você pode editar os campos **Nome** e **Descrição** de um grupo de procura.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione o grupo que você deseja editar.
6. Clique em **Editar**.
7. Digite um novo nome no campo **Nome**.
8. Insira uma nova descrição no campo **Descrição**.
9. Clique em **OK**.

Copiando uma procura salva em outro grupo

Você pode copiar uma procura salva para outro grupo. Você também pode copiar a procura salva em mais de um grupo.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a procura salva que deseja copiar.
6. Clique em **Copiar**.

7. Na janela Grupos de itens, marque a caixa de seleção para o grupo para o qual você deseja copiar a procura salva.
8. Clique em **Designar grupos**.

Removendo um grupo ou uma procura salva de um grupo

Você pode usar o ícone **Remove** para remover uma procura de um grupo ou remover um grupo de procura.

Sobre Esta Tarefa

Ao remover uma procura salva de um grupo, ela não será excluída do sistema. A procura salva é removida do grupo e movida automaticamente para o grupo **Outros**.

Não é possível remover os seguintes grupos do sistema:

- Grupos de Procura de Ativos
- Outros

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a procura salva que você deseja remover do grupo:
 - Selecione a procura salva que você deseja remover do grupo.
 - Selecione o grupo que você deseja remover.

Tarefas de gerenciamento de perfil do ativo

É possível excluir, importar e exportar perfis do ativo usando a guia **Ativos**.

Sobre Esta Tarefa

Usando a guia **Ativos**, você pode excluir, importar e exportar perfis de ativos.

Excluindo ativos

Você pode excluir os ativos específicos ou todos os perfis de ativos listados.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione o ativo que você deseja excluir e, em seguida, selecione **Excluir ativo** na caixa de listagem **Ações**.
4. Clique em **OK**.

Importando perfis de ativos

É possível importar informações do perfil de ativos.

Antes de Iniciar

O arquivo importado deve ser um arquivo CSV no seguinte formato:

```
ip,name,weight,description
```

Em que:

- **IP** – especifica qualquer endereço IP válido no formato de número com decimal. Por exemplo: 192.168.5.34.
- **Nome** – especifica o nome desse ativo de até 255 caracteres de comprimento. As vírgulas não são válidas nesse campo e invalidam o processo de importação. Por exemplo: WebServer01 está correto.
- **Peso** – especifica um número de 0 a 10 que indica a importância desse ativo em sua rede. Um valor de 0 denota pouca importância e 10 é muita importância.
- **Descrição** – especifica uma descrição textual para esse ativo de até 255 caracteres de comprimento. Esse valor é opcional.

Por exemplo, as entradas a seguir podem ser incluídas em um arquivo CSV:

- 192.168.5.34,WebServer01,5,Main Production Web Server
- 192.168.5.35,MailServ01,0,

O processo de importação mescla os perfis de ativos importados com as informações do perfil de ativos que você tem atualmente armazenado no sistema.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Na caixa de listagem **Ações**, selecione **Importar ativos**.
4. Clique em **Pesquisar** para localizar e selecionar o arquivo CSV que você deseja importar.
5. Clique em **Importar ativos** para iniciar o processo de importação.

Exportando ativos

Você pode exportar perfis de ativos listados para um arquivo de Linguagem de Marcação Estendida (XML) ou Valor Separado por Vírgula (CSV).

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Na caixa de listagem **Ações**, selecione uma das opções a seguir:
 - Exportar para XML
 - Exportar para CSV
4. Visualizando a janela de status para o status do processo de exportação.
5. Opcional: Se você deseja usar outras guias e páginas enquanto a exportação estiver em andamento, clique no link **Notificar quando pronto**.
Quando a exportação for concluída, a janela Download de arquivo será exibida.
6. Na janela Download de arquivo, escolha uma das opções a seguir:
 - **Abrir** – Selecione esta opção para abrir os resultados da exportação em sua opção de navegador.

- **Salvar** – Selecione esta opção para salvar os resultados em sua área de trabalho.

7. Clique em **OK**.

Pesquisar vulnerabilidades de ativos

A área de janela Vulnerabilidades na página Perfil de ativos exibe uma lista de vulnerabilidades descobertas para o ativo.

Sobre Esta Tarefa

Você pode dar um clique duplo na vulnerabilidade para exibir mais detalhes sobre a vulnerabilidade.

A janela Pesquisar detalhes da vulnerabilidade fornece os detalhes a seguir:

Parâmetro	Descrição
Vulnerability ID	Especifica o ID da vulnerabilidade. O ID de Vuln é um identificador exclusivo gerado pelo Vulnerability Information System (VIS).
Published Date	Especifica a data na qual os detalhes de vulnerabilidade foram publicados no OSVDB.
Name	Especifica o nome da vulnerabilidade.
Ativos	Especifica o número de ativos em sua rede que possuem essa vulnerabilidade. Clique no link para visualizar a lista de ativos.
Assets, including exceptions	Especifica o número de ativos em sua rede que possuem exceções de vulnerabilidade. Clique no link para visualizar a lista de ativos.
CVE	Especifica o identificador de CVE para a vulnerabilidade. Os identificadores de CVE são fornecidos pelo NVDB. Clique no link para obter mais informações. Ao clicar no link, o website do NVDB será exibido em uma nova janela do navegador.
xforce	Especifica o identificador X-Force para a vulnerabilidade. Clique no link para obter mais informações. Ao clicar no link, o website do IBM Internet Security Systems será exibido em uma nova janela do navegador.
OSVDB	Especifica o identificador do OSVDB para a vulnerabilidade. Clique no link para obter mais informações. Ao clicar no link, o website do OSVDB será exibido em uma nova janela do navegador.

Parâmetro	Descrição
CVSS Score	<p>Exibe a pontuação de Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação de CVSS é uma métrica de avaliação para a gravidade de uma vulnerabilidade. Você pode usar pontuações do CVSS para medir o quanto uma vulnerabilidade garante em comparação a outras vulnerabilidades.</p> <p>A pontuação de CVSS é calculada usando os seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> • Potencial de Danos Colaterais • Requisitos de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade <p>Para obter mais informações sobre como configurar esses parâmetros, consulte “Incluindo ou editando um perfil de ativo” na página 106.</p> <p>Para obter mais informações sobre o CVSS, consulte http://www.first.org/cvss/.</p>
Impact	Exibe o tipo de prejuízo ou dano que pode ser esperado se essa vulnerabilidade for explorada.
Métricas Base de CVSS	<p>Exibe as métricas usadas para calcular a pontuação CVSS de base, incluindo:</p> <ul style="list-style-type: none"> • Vetor de Acesso • Complexidade de Acesso • Autenticação • Impacto de Confidencialidade • Impacto de Integridade • Impacto de disponibilidade
Descrição	Especifica uma descrição da vulnerabilidade detectada. Esse valor está disponível somente quando o sistema integra as ferramentas de VA.
Dúvida	Especifica os efeitos que a vulnerabilidade pode ter em sua rede.
Solução	Siga as instruções fornecidas para resolver a vulnerabilidade.
Correção Virtual	Exibe as informações de correção virtual associadas a essa vulnerabilidade, se disponível. Uma correção virtual é uma solução de mitigação de curto prazo para uma vulnerabilidade recentemente descoberta. Essas informações são derivadas de eventos do Intrusion Protection System (IPS). Se você deseja instalar a correção virtual, consulte as informações do fornecedor de IPS.

Parâmetro	Descrição
Referência	<p>Exibe uma lista de referências externas, incluindo:</p> <ul style="list-style-type: none"> • Tipo de referência – especifica o tipo de referência listada, como uma URL consultiva ou uma lista de post de correio. • URL – especifica a URL na qual você pode clicar para visualizar a referência. <p>Clique no link para obter mais informações. Ao clicar no link, o recurso externo será exibido em uma nova janela do navegador.</p>
Produtos	<p>Exibe uma lista de produtos associados a essa vulnerabilidade.</p> <ul style="list-style-type: none"> • Fornecedor – especifica o fornecedor do produto. • Produto – especifica o nome do produto. • Versão – especifica o número da versão do produto.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione um perfil de ativos.
4. Na área de janela Vulnerabilidades, clique no valor do parâmetro **ID** ou **Vulnerability** para a vulnerabilidade que você deseja investigar.

Parâmetros da página Perfil de ativo

É possível localizar as descrições de parâmetro da página Perfil de ativo para a área de janela Resumo de ativo, Interface de rede, Vulnerabilidade, Serviços, Pacotes, Correções do Windows, Propriedades, Políticas de risco e Produtos.

Esta referência inclui tabelas que descrevem os parâmetros que são exibidos em cada área de janela da guia **Perfil de ativo**.

Área de janela de resumo de ativo

É possível localizar descrições de Parâmetros para a área de janela de Resumo de Ativo que você acessa na página Perfil de ativos.

A área de janela do Resumo de Ativo na página Perfil de ativos fornece as seguintes informações:

Parâmetros da área de janela de Resumo de Ativo de 10-8 da tabela

Parâmetro	Descrição
Asset ID	Exibe o número do ID que é designado para o perfil de ativo.
IP Address	Exibe o último endereço IP reportado do ativo.

Parâmetro	Descrição
MAC Address	Exibe o último endereço MAC conhecido do ativo.
Network	Exibe a última rede relatada que está associada ao ativo.
NetBIOS Name	Exibe o nome do NetBIOS do ativo, se conhecido. Se o ativo tiver mais de um nome de NetBIOS, este campo indicará o número de nomes do NetBIOS. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de nomes do NetBIOS associado.
DNS Name	Exibe o endereço IP ou nome do DNS do ativo, se conhecido. Se o ativo tiver mais de um nome do DNS, este campo indicará o número de nomes do DNS. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de nomes do DNS associado.
Given Name	Exibe o nome do ativo. Por padrão, esse campo fica vazio. Para fornecer um nome dado para o ativo, edite o perfil do ativo.
Group Name	Exibe o último grupo de usuários conhecido do ativo, se conhecido.
Last User	Exibe o último usuário conhecido do ativo. As informações do usuário são derivadas de eventos da identidade. Se mais de um usuário estiver associado a este ativo, você poderá clicar no link para exibir todos os usuários.
Operating System	<p>Exibe o sistema operacional que está sendo executado no ativo. Se o ativo tiver mais de um sistema operacional, este campo indicará o número de sistemas operacionais. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de sistemas operacionais associados.</p> <p>Você pode editar esse parâmetro diretamente se o parâmetro Override for especificado como Até a próxima varredura ou Indefinidamente.</p>
Weight	Exibe o nível de importância que está associado a este ativo. O intervalo vai de 0 (Não importante) a 10 (Muito importante). Por padrão, esse campo fica vazio. Para fornecer um peso para o ativo, edite o perfil de ativos.

Parâmetro	Descrição
Aggregate CVSS Score	<p>Exibe a pontuação de Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação de CVSS é uma métrica de avaliação para a gravidade de uma vulnerabilidade. Você pode usar pontuações do CVSS para medir o quanto uma vulnerabilidade garante em comparação a outras vulnerabilidades.</p> <p>A pontuação de CVSS é calculada usando os seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> • Potencial de Danos Colaterais • Requisitos de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade <p>Para obter mais informações sobre como configurar esses parâmetros, consulte “Incluindo ou editando um perfil de ativo” na página 106.</p> <p>Para obter mais informações sobre o CVSS, consulte http://www.first.org/cvss/.</p>
Business Owner	Exibe o nome do proprietário de negócios do ativo. Um exemplo de um proprietário de negócios é um gerente do departamento.
Business Owner Contact Info	Exibe as informações de contato para o proprietário de negócios.
CVSS Collateral Damage Potential	<p>Exibe o potencial que este ativo possui para danos colaterais. Este valor é incluído na fórmula para calcular o parâmetro CVSS Score.</p> <p>Por padrão, esse campo não está definido. Para fornecer um local para o ativo, edite o perfil de ativos.</p>
Technical Owner	Exibe o responsável técnico do ativo. Um exemplo de um responsável técnico é um gerente ou diretor de TI.
Technical Owner Contact Info	Exibe as informações de contato do responsável técnico.
CVSS Availability	Exibe o impacto para a disponibilidade do ativo quando uma vulnerabilidade é explorada com êxito.
Wireless AP	Exibe o Ponto de Acesso (PA) wireless para esse perfil de ativos.
Wireless SSID	Exibe o Service Set Identifier (SSID) wireless para este perfil de ativos.
CVSS Confidentiality Requirements	Exibe o impacto na confidencialidade de uma vulnerabilidade explorada com êxito nesse ativo.

Parâmetro	Descrição
Switch ID	Exibe o ID do comutador para este perfil de ativos.
Switch Port ID	Exibe o ID da porta do comutador para este perfil de ativos.
CVSS Integrity Requirements	Exibe o impacto para integridade do ativo quando uma vulnerabilidade é explorada com êxito.
Technical User	Especifica o nome do usuário que está associado a este perfil de ativos.
Open Services	Exibe o número de aplicativos de Camada 7 exclusivos executados neste perfil de ativos.
Vulnerabilidades	Exibe o número de vulnerabilidades que são descobertas nesse perfil de ativos.
Location	Especifica o local físico do ativo. Por padrão, esse campo fica vazio. Para fornecer um local para o ativo, edite o perfil de ativos.
Asset Description	Especifica uma descrição para este ativo. Por padrão, esse campo fica vazio. Para fornecer uma descrição para o ativo, edite o perfil de ativos.
Extra Data	Especifica quaisquer informações estendidas que são baseadas em um evento.

Área de janela de resumo da interface de rede

É possível localizar descrições de Parâmetros para a área de janela de Resumo da Interface de Rede que você acessa na página Perfil de ativos.

A área de janela de Resumo da Interface de Rede na página Perfil de ativos fornece as seguintes informações:

Parâmetros da área de janela de Resumo da Interface de Rede 1 de Tabela

Parâmetro	Descrição
Endereço MAC	Exibe o endereço MAC do ativo, se conhecido.
Endereço IP	Exibe o endereço IP que é detectado para este endereço MAC.
Rede	Exibe a rede a que o endereço IP está associado, se conhecido.
Visto pela última vez	Exibe a data e a hora em que o endereço IP foi detectado pela última vez nesse endereço MAC.

Área de janela de vulnerabilidade

É possível localizar descrições de Parâmetros para a área de Vulnerabilidade que você acessa na página de Perfil de ativos.

A área de janela de Vulnerabilidade na página de Perfil de ativos fornece as seguintes informações:

Tabela 35. Parâmetros da área de janela de vulnerabilidade

Parâmetro	Descrição
ID	Exibe o ID da vulnerabilidade. O ID é um identificador exclusivo que é gerado pelo Sistema de Informações de Vulnerabilidade (VIS).
Severity	Exibe a gravidade da Indústria de Segurança de Pagamento (PCI) que está associada à vulnerabilidade.
Risk	Nível de risco que está associado à vulnerabilidade. A classificação nessa coluna deve ser pelo código de nível de risco subjacente.
Service	O serviço que está associado à vulnerabilidade (como descoberto pela varredura). Se somente 1 serviço estiver associado, então, exiba o serviço. Caso contrário, exiba Vários (N) onde N indica ao número total de serviços associados a esta vulnerabilidade.
Port	Exibe o número da porta que esta vulnerabilidade foi descoberta. Se a vulnerabilidade foi descoberta em mais de uma porta, este campo indicará o número de números de portas. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de números de porta.
Vulnerability	Nome ou título dessa vulnerabilidade.
Details	Texto detalhado específico que está associado a essa vulnerabilidade, conforme determinado pela varredura. Se somente 1 Detalhe estiver associado, então, exiba o texto desse Detalhe. Caso contrário, exiba Vários (N) onde N indica o número total de Detalhes que estão associados a esta vulnerabilidade.

Tabela 35. Parâmetros da área de janela de vulnerabilidade (continuação)

Parâmetro	Descrição
CVSS Score	<p>Exibe a pontuação de Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação de CVSS é uma métrica de avaliação para a gravidade de uma vulnerabilidade. Você pode usar pontuações do CVSS para medir o quanto uma vulnerabilidade garante em comparação a outras vulnerabilidades.</p> <p>A pontuação de CVSS é calculada usando os seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> • Potencial de Danos Colaterais • Requisitos de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade <p>Para obter mais informações sobre como configurar esses parâmetros, consulte “Incluindo ou editando um perfil de ativo” na página 106.</p> <p>Para obter mais informações sobre o CVSS, consulte http://www.first.org/cvss/.</p>
Found	Exibe a data em que esta vulnerabilidade foi originalmente encontrada em uma varredura.
Last seen	Exibe a data em que esta vulnerabilidade foi vista em uma varredura.

Área de janela de serviços

É possível localizar descrições de Parâmetros para a área de janela de Serviços que você acessa na página de Perfil de ativos.

A área de janela de Serviços na página de Perfil de ativos fornece as seguintes informações:

Tabela 36. Parâmetros da área de janela de serviços

Parâmetro	Descrição
Serviço	Exibe o nome do serviço aberto.
Produto	Exibe o produto que executa neste serviço, se conhecido.
Porta	Exibe a porta que o aplicativo de Camada 7 foi descoberto. Se esse serviço tiver mais que uma porta, esse campo indicará o número de portas. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de números de porta.
Protocolo	Exibe uma lista separada por vírgula de protocolos que são descobertos na porta que executa o serviço aberto.

Tabela 36. Parâmetros da área de janela de serviços (continuação)

Parâmetro	Descrição
Passivo pela última vez	Exibe a data e hora em que o serviço foi visto passivamente pela última vez.
Ativo pela última vez	Exibe a data e hora em que o serviço aberto foi visto ativamente pela última vez.
Portas padrão de serviço	Exibe uma lista separada por vírgula de portas conhecidas que o aplicativo de Camada 7 é conhecido para execução.
Vulnerabilidades	Exibe o número de vulnerabilidades que estão associadas a este serviço aberto.

Área de janela de Serviços do Windows

É possível localizar descrições de Parâmetros para a área de janela de Serviços do Windows que você acessa na página de Perfil de ativos. A área de janela de Serviços do Windows é exibida apenas quando QRadar Vulnerability Manager está instalado em seu sistema.

A área de janela de Serviços do Windows na página de Perfil de ativos fornece as seguintes informações:

Tabela 37. Parâmetros da área de janela de Serviços do Windows

Parâmetro	Descrição
Nome	Exibe o nome do serviço do Windows que foi visto ativamente no ativo.
Status	Exibe o status do serviço do Windows. As opções incluem: <ul style="list-style-type: none"> • Ativado • Manual • Desativado

Área de janela de pacotes

É possível localizar descrições de Parâmetros para a área de janela de Pacotes que você acessa na página de Perfil de ativos.

A área de janela de Pacotes será exibida apenas quando QRadar Vulnerability Manager for instalado em seu sistema. A área de janela de Pacotes na página de Perfil de ativos fornece as seguintes informações:

Tabela 38. Parâmetros da área de janela de pacotes

Parâmetro	Descrição
Pacotes	Exibe o nome do pacote que é aplicado ao ativo.
Versão	Exibe a versão do pacote que é aplicada ao ativo.
Revisão	Exibe a revisão do pacote que é aplicada ao ativo.

Área de janela de correções do Windows

É possível localizar descrições de Parâmetro para a área de janela de Correções do Windows que você acessa na página de Perfil de ativos.

A área de janela de Correções do Windows é exibida apenas quando QRadar Vulnerability Manager está instalado em seu sistema. A área de janela de Correções do Windows na página de Perfil de ativos fornece as seguintes informações:

Tabela 39. Parâmetros da área de janela de Correções do Windows

Parâmetro	Descrição
Número de KB da Microsoft	Exibe o número de Base de Conhecimento (KB) da Microsoft da correção do Windows que é executado no ativo.
Descrição	Exibe a descrição da correção do Windows.
ID de boletim	Exibe o número do ID de boletim da correção do Windows.
ID de vulnerabilidade	Exibe o ID de vulnerabilidade da correção do Windows.
ID do CVE	Exibe o ID do CVE associado à correção do Windows. Se mais de um é o ID do CVE estiver associado à correção do Windows, passe o mouse sobre o link Vários para exibir a lista de IDs do CVE. Você pode clicar em um link do ID do CVE para acessar mais informações.
Sistema	Exibe o sistema Windows para a correção.
Service Pack	Exibe o Service Pack para a correção.

Área de janela de propriedades

É possível localizar descrições de Parâmetros para a área de janela de Propriedades que você acessa na página de Perfil de ativos . A área de janela de Propriedades é exibida apenas quando QRadar Vulnerability Manager estiver instalado em seu sistema.

A área de janela de Propriedades na página de Perfil de ativos fornece as seguintes informações:

Tabela 40. parâmetros da área de janela de propriedades

Parâmetro	Descrição
Nome	Exibe o nome da propriedade de configuração que foi vista ativamente no ativo.
Valor	Exibe o valor para a propriedade de configuração.

Área de janela de políticas de risco

É possível localizar descrições de parâmetros para a área de janela de Políticas de Risco que você acessa na página Perfil de ativos. A área de janela de Políticas de Riscos é exibida apenas quando QRadar Vulnerability Manager é instalado em seu sistema.

A área de janela de Políticas de Risco na página Perfil de ativos fornece as seguintes informações:

Tabela 41. Parâmetros da área de janela de Políticas de Risco

Parâmetro	Descrição
Política	Exibe o nome da política associada a esse ativo.
Aprovado/Reprovado	Indica se a política possui um status de Aprovado ou Reprovado .
Avaliado pela última vez	Exibe a data em que esta política foi avaliada pela última vez.

Área de janela de produtos

Você pode localizar descrições de parâmetros para a área de janela de Produtos que você acessa na página Perfil de ativos.

A área de janela de Produtos na página Perfil de ativos fornece as seguintes informações:

Tabela 42. parâmetros da área de janela de produtos

Parâmetro	Descrição
Produto	Exibe o nome do produto que é executado no ativo.
Porta	Exibe a porta que o produto usa.
Vulnerabilidade	Exibe o número de vulnerabilidades que estão associadas a este produto.
ID de vulnerabilidade	Exibe o ID de vulnerabilidade.

Capítulo 10. Gerenciamento de relatório

É possível usar a guia **Relatórios** para criar, editar, distribuir e gerenciar relatórios.

As opções de relatório flexíveis e detalhadas satisfazem seus vários padrões regulatórios, como conformidade de PCI.

É possível criar seus próprios relatórios customizados ou usar relatórios padrão. É possível customizar e remarcar relatórios padrão e distribuí-los para outros usuários.

A guia **Relatórios** poderá requerer um período de tempo estendido para ser atualizada se seu sistema incluir muitos relatórios.

Nota: Se estiver executando o Microsoft Exchange Server 5.5, caracteres de fontes indisponíveis poderão ser exibidos na linha de assunto de relatórios enviados por email. Para resolver isso, faça download e instale o Service Pack 4 do Microsoft Exchange Server 5.5. Para obter mais informações, entre em contato com o suporte da Microsoft.

Considerações sobre fuso horário

Para assegurar-se de que o recurso Relatórios use data e hora corretas para relatar dados, sua sessão deverá estar sincronizada com o fuso horário.

Durante a instalação e configuração de produtos QRadar, o fuso horário é configurado. Verifique com seu administrador, para assegurar-se de que sua sessão do QRadar esteja sincronizada com o fuso horário.

Permissões da guia Relatório

Os usuários administrativos podem visualizar todos os relatórios que são criados por outros usuários.

Os usuários não administrativos podem visualizar somente relatórios que eles criaram ou relatórios que são compartilhados por outros usuários.

Parâmetros da guia Relatório

A guia **Relatórios** exibe uma lista de relatórios padrão e customizados.

Na guia **Relatórios**, é possível visualizar informações estatísticas sobre o modelo de relatórios, executar ações nos modelos de relatório, visualizar os relatórios gerados e excluir conteúdo gerado.

Se um relatório não especificar um planejamento de intervalo, será necessário gerar manualmente o relatório.

É possível passar o mouse sobre qualquer relatório para visualizar um resumo do relatório em uma dica de ferramenta. O resumo especifica a configuração do relatório e o tipo de conteúdo que o relatório gera.

Visão geral da guia Relatórios

É possível criar seus próprios relatórios customizados ou usar relatórios padrão. É possível customizar e remarcar relatórios padrão e distribuí-los para outros usuários.

A guia **Relatórios** poderá requerer um período de tempo estendido para ser atualizada se seu sistema incluir muitos relatórios.

Nota: Se estiver executando o Microsoft Exchange Server 5.5, caracteres de fontes indisponíveis poderão ser exibidos na linha de assunto de relatórios enviados por email. Para resolver isso, faça download e instale o Service Pack 4 do Microsoft Exchange Server 5.5. Para obter mais informações, entre em contato com o suporte da Microsoft.

Considerações sobre fuso horário

Para assegurar-se de que o recurso Relatórios use data e hora corretas para relatar dados, sua sessão deverá estar sincronizada com o fuso horário.

Durante a instalação e configuração de produtos QRadar, o fuso horário é configurado. Verifique com seu administrador, para assegurar-se de que sua sessão do QRadar esteja sincronizada com o fuso horário.

Permissões da guia Relatório

Os usuários administrativos podem visualizar todos os relatórios que são criados por outros usuários.

Os usuários não administrativos podem visualizar somente relatórios que eles criaram ou relatórios que são compartilhados por outros usuários.

Parâmetros da guia Relatório

A guia **Relatórios** exibe uma lista de relatórios padrão e customizados.

Na guia **Relatórios**, é possível visualizar informações estatísticas sobre o modelo de relatórios, executar ações nos modelos de relatório, visualizar os relatórios gerados e excluir conteúdo gerado.

A guia **Relatórios** fornece as seguintes informações:

Tabela 43. Parâmetros da guia Relatório

Parâmetro	Descrição
Flag Column	Se um erro ocorrer, fazendo com que a geração de relatórios falhe, o ícone Erros será exibido nesta coluna.
Report Name	Especifica o nome do relatório.
Grupo	Especifica o grupo ao qual este relatório pertence.

Tabela 43. Parâmetros da guia Relatório (continuação)

Parâmetro	Descrição
Schedule	Especifica a frequência com que o relatório é gerado. Relatórios que especificam um planejamento de intervalo, quando ativados, são automaticamente gerados de acordo com o intervalo especificado. Se um relatório não especificar um planejamento de intervalo, será necessário gerar manualmente o relatório.
Next Run Time	Especifica a duração de tempo, em horas e minutos, até que o próximo relatório seja gerado.
Last Modification	Especifica a última data na qual este relatório foi modificado.
Owner	Especifica o usuário que possui o relatório.
Author	Especifica o usuário que criou o relatório.
Generated Reports	Nessa caixa de listagem, selecione o registro de data do relatório gerado que deseja visualizar. Ao selecionar o registro de data, o parâmetro Format exibe os formatos disponíveis para os relatórios gerados. Se nenhum relatório for gerado, Nenhum será exibido.
Formats	Especifica os formatos de relatório do relatório selecionado atualmente na coluna Relatórios gerados. Clique no ícone para o formato que deseja visualizar.

É possível passar o mouse sobre qualquer relatório para visualizar um resumo do relatório em uma dica de ferramenta. O resumo especifica a configuração do relatório e o tipo de conteúdo que o relatório gera.

Ordem de classificação na guia Relatório

Por padrão, os relatórios são classificados pela coluna **Última modificação**. No menu de navegação **Relatórios**, os relatórios são classificados pelo planejamento de intervalo.

Para filtrar o relatório para exibir somente relatórios de uma frequência específica, clique na seta ao lado do item de menu **Relatório** no menu de navegação e selecione a pasta do grupo (frequência).

Barra de ferramentas da guia Relatório

É possível usar a barra de ferramentas para executar várias ações em relatórios.

A tabela a seguir identifica e descreve as opções da barra de ferramentas Relatórios.

Tabela 44. Opções da barra de ferramentas Relatórios

Opção	Descrição
Grupo	

Tabela 44. Opções da barra de ferramentas Relatórios (continuação)

Opção	Descrição
Gerenciar grupos	Clique em Gerenciar grupos para gerenciar os grupos de relatórios. Usando o recurso Gerenciar grupos, é possível organizar seus relatórios em grupos funcionais.
Ações	<p>Clique em Ações para executar as seguintes ações:</p> <ul style="list-style-type: none"> • Criar – Selecione esta opção para criar um novo relatório. • Editar – Selecione esta opção para editar o relatório selecionado. É possível também clicar duas vezes em um relatório para editar o conteúdo. • Duplicar – Selecione esta opção para duplicar ou renomear o relatório selecionado. • Designar grupos – Selecione esta opção para designar o relatório selecionado para um grupo de relatórios. • Compartilhar – Selecione essa opção para compartilhar o relatório selecionado com outros usuários. Deve-se ter privilégios administrativos para compartilhar relatórios. • Alternar planejamento – Selecione esta opção para alternar o relatório selecionado para o estado Ativo ou Inativo. • Executar relatório – Selecione esta opção para gerar o relatório selecionado. Para gerar vários relatórios, mantenha pressionada a tecla Control e clique nos relatórios que deseja gerar. • Executar relatório em dados brutos – Selecione esta opção para gerar o relatório selecionado usando dados brutos. Essa opção será útil quando desejar gerar um relatório antes que os dados acumulados requeridos estejam disponíveis. Por exemplo, se desejar executar um relatório semanal antes que uma semana completa tenha decorrido desde a criação do relatório, será possível gerar o relatório usando esta opção. • Excluir relatório – Selecione esta opção para excluir o relatório selecionado. Para excluir vários relatórios, mantenha a tecla Control pressionada e clique nos relatórios que deseja excluir. • Excluir conteúdo gerado – Selecione esta opção para excluir todo o conteúdo gerado nas linhas selecionadas. Para excluir vários relatórios gerados, mantenha pressionada a tecla Control e clique em gerar relatórios que deseja excluir.

Tabela 44. Opções da barra de ferramentas Relatórios (continuação)

Opção	Descrição
Ocultar relatórios interativos	Selecione esta caixa de seleção para ocultar os modelos de relatório inativo. A guia Relatórios será atualizada automaticamente e exibirá apenas os relatórios ativos. Limpe a caixa de seleções para mostrar os relatórios inativos ocultos.
Relatórios de procura	<p>Digite seus critérios de procura no campo Relatórios de procura e clique no ícone Relatórios de procura. Uma pesquisa é executada nos parâmetros a seguir para determinar quais correspondem seus critérios especificados:</p> <ul style="list-style-type: none"> • Título do Relatório • Descrição do relatório • Grupo de relatórios • Grupos de relatórios • Nome de usuário do autor do relatório

Barra de status

A barra de status exibe o número de resultados da procura (Exibindo 1 de 10 itens) atualmente exibido e a quantidade de tempo (Tempo decorrido:) necessária para processar os resultados da procura.

Layout de relatório

Um relatório pode consistir em vários elementos de dados e pode representar dados de rede e de segurança em vários estilos, como tabelas, gráficos de linha, gráficos de pizza e gráficos de barras.

Quando você seleciona o layout de um relatório, considere o tipo de relatório que você deseja criar. Por exemplo, não escolha um pequeno contêiner de gráfico para o conteúdo de gráfico que exibe muitos objetos. Cada gráfico inclui uma legenda e uma lista de redes a partir das quais o conteúdo é derivado; escolha um contêiner suficientemente grande para conter os dados. Para visualizar como cada gráfico exibe dados, consulte Tipos de diagrama.

Tipos de gráfico

Ao criar um relatório, você deve escolher um tipo de gráfico para cada gráfico que você deseja incluir no relatório.

O tipo de gráfico determina como o relatório gerado apresenta dados e objetos da rede. É possível colocar em gráfico dados com diversas características e criar os gráficos em um único relatório gerado.

É possível usar qualquer um dos seguintes tipos de gráficos:

- **Nenhum** – Use esta opção para exibir um contêiner vazio no relatório. Essa opção pode ser útil para criar espaço em branco em seu relatório. Se selecionar a opção **Nenhum** para qualquer contêiner, nenhuma configuração adicional será necessária para esse contêiner.
- **Vulnerabilidades do ativo** - Use este gráfico para visualizar dados de vulnerabilidade para cada ativo definido em sua implementação. Você poderá

gerar gráficos de Vulnerabilidade de Ativo quando vulnerabilidades forem detectadas por uma varredura de VA. Este gráfico estará disponível após você instalar IBM Security QRadar Vulnerability Manager.

- **Vulnerabilidades** – A opção Vulnerabilidades será exibida somente quando o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

Para obter mais informações sobre esses tipos de gráfico, consulte Parâmetros do contêiner de gráfico.

Tipos de diagrama

Cada tipo de gráfico suporta vários tipos de diagrama que podem ser usados para exibir dados.

Os seguintes tipos de diagramas estão disponíveis para relatórios do QRadar Log Manager:

- Gráfico de linhas
- Gráfico de linhas empilhadas
- Gráfico de barras
- Gráfico de barras empilhadas
- Gráfico de pizza
- Gráfico de tabela

Para exibir o conteúdo em uma tabela, deve-se projetar um relatório com um contêiner com largura de página inteira.

Criando relatórios customizados

É possível usar o assistente de Relatório para criar um novo relatório.

Antes de Iniciar

Você deve ter permissões da rede apropriadas para compartilhar um relatório gerado com outros usuários.

Para obter mais informações sobre permissões, consulte o *Guia de Administração do IBM Security QRadar Log Manager*.

Sobre Esta Tarefa

O assistente de Relatório fornece um guia passo a passo sobre como projetar, planejar e gerar relatórios.

O assistente usa os seguintes elementos chave para ajudar a criar um relatório:

- **Layout** – Posição e tamanho de cada contêiner
- **Contêiner** - Marcador para o conteúdo de recurso
- **Conteúdo** – Definição do gráfico que é colocado no contêiner

Depois de criar um relatório que gera semanalmente ou mensalmente, o tempo planejado deve ter decorrido antes que o relatório gerado retorne resultados. Para obter um relatório planejado, você deve aguardar o período de tempo planejado

para os resultados construam. Por exemplo, uma procura semanal requer sete dias para construir os dados. Esta procura não retorna resultados antes que sete dias tenham decorrido.

Quando você especifica o formato de saída para o relatório, considere que o tamanho do arquivo de relatórios gerados podem ser de um a 2 megabytes, dependendo do formato de saída selecionado. O formato PDF é menor em tamanho e não consome uma grande quantidade de espaço de armazenamento em disco.

Procedimento

1. Clique na guia **Relatórios**.
2. Na caixa de listagem de **Ações**, selecione **Criar**.
3. Nas Boas vindas da alteração do assistente de Relatório, clique em **Avançar** para acessar a próxima página do assistente de Relatório.
4. Selecione uma das seguintes opções:

Opção	Descrição
Manualmente	Gera um relatório uma vez. Essa é a configuração padrão; no entanto, você pode gerar esse relatório sempre que necessário.
Por hora	Planeja o relatório a ser gerado no final de cada hora usando os dados da hora anterior. Se você escolher a opção Por Hora , configurações adicionais serão necessárias. Nas caixas de listagem, selecione um prazo para começar e terminar o ciclo do relatório. Um relatório é gerado para cada hora dentro desse prazo. O horário está disponível em incrementos de meia hora. O padrão é 1h da manhã para os campos De e Para .
Semanalmente	Planeja o relatório para gerar semanalmente usando os dados da semana anterior. Se você escolher a opção Semanalmente , configurações adicionais serão necessárias. Selecione o dia que você deseja gerar o relatório. O padrão é Segunda-feira. Na caixa de listagem, selecione uma hora para iniciar o ciclo do relatório. O horário está disponível em incrementos de meia hora. O padrão é 1h da manhã.
Mensalmente	Planeja o relatório para gerar mensalmente usando os dados do mês anterior. Se você escolher a opção Mensalmente , configurações adicionais serão necessárias. Na caixa de listagem, selecione a data que você deseja gerar o relatório. O padrão é o primeiro dia do mês. Além disso, use a caixa de listagem para selecionar uma hora para iniciar o ciclo do relatório. O horário está disponível em incrementos de meia hora. O padrão é 1h da manhã.

5. Na área de janela **Permitir que este relatório gere manualmente, Sim** ou **Não**.

6. Configure o layout do relatório:
 - a. Na caixa de listagem **Orientação**, selecione a orientação da página: Retrato ou Paisagem.
 - b. Selecione uma das seis opções de layout exibidas no assistente de Relatório.
 - c. Clique em **Avançar** para mover para a próxima página do assistente de Relatório.
 7. Especifique valores para os seguintes parâmetros:
 - **Título do relatório** – Digite um título do relatório. O título pode ter até 100 caracteres de comprimento. Não use caracteres especiais.
 - **Logotipo** – Na caixa de listagem, selecione um logotipo.
 -
 8. Configure cada contêiner no relatório:
 - a. Na caixa de listagem **Tipo de gráfico**, selecione um tipo de gráfico.
 - b. Na janela Detalhes do contêiner - <chart_type>, configure os parâmetros do gráfico.
 - c. Clique em **Salvar detalhes do contêiner**.
 - d. Se necessário, repita as etapas de a até c para todos os contêineres.
 - e. Clique em **Avançar** para mover para a próxima página do assistente de Relatório.
 9. Visualize a página de Visualização de layout e, em seguida, clique em **Avançar** para acessar a próxima etapa do assistente de Relatório.
 10. Selecione as caixas de seleção para os formatos de relatório que você deseja gerar e, em seguida, clique em **Avançar**.
- Nota:** A Linguagem de Marcação Extensível está disponível apenas para tabelas.
11. Selecione os canais de distribuição para o relatório e, em seguida, clique em **Avançar**. As opções incluem os seguintes canais de distribuição:

Opção	Descrição
Console de relatório	Selecione esta caixa de seleção para enviar o relatório gerado para a guia Relatórios . Este é o canal de distribuição padrão.
Selecione os usuários que devem ser capazes de visualizar o relatório gerado.	Essa opção é exibida depois que você seleciona a caixa de seleção Console de relatório . Na lista de usuários, selecione os usuários que você deseja conceder permissão para visualizar os relatórios gerados.
Selecionar todos os usuários	Essa opção é exibida somente depois que você selecionar a caixa de seleção Console de relatório . Selecione essa caixa de seleção se você desejar conceder permissão a todos os usuários para visualizar os relatórios gerados. Você deve ter permissões da rede apropriadas para compartilhar o relatório gerado com outros usuários.

Opção	Descrição
Email	Selecione essa caixa de seleção se você desejar distribuir o relatório gerado usando email.
Insira o(s) endereço(s) de email de distribuição de relatório	Essa opção é exibida somente depois que você seleciona a caixa de seleção Email . Digite o endereço de email para cada destinatário de relatório gerado; separe uma lista de endereços de email com vírgulas. Os caracteres máximos para este parâmetro são 255. Destinatários de email recebem este email do no_reply_reports@qradar.
Incluir Relatório como anexo (apenas não HTML)	Essa opção é exibida somente depois que você seleciona a caixa de seleção Email . Selecione esta caixa de seleção para enviar o relatório gerado como um anexo.
Incluir link no Console de Relatórios	Essa opção é exibida somente depois que você seleciona a caixa de seleção Email . Selecione essa caixa de seleção para incluir um link no Console de Relatórios no email.

12. Na página Concluindo, insira valores para os seguintes parâmetros:

Opção	Descrição
Descrição do relatório	Digite uma descrição para este relatório. A descrição é exibida na página Resumo de relatório e no email de distribuição de relatório gerado.
Grupos	Selecione os grupos aos quais você deseja designar esse relatório. Para obter mais informações sobre grupos, consulte Grupos de Relatório.
Deseja executar o relatório agora?	Selecione essa caixa de seleção se você desejar gerar o relatório quando o assistente for concluído. Por padrão, a caixa de seleção é selecionada.

13. Clique em **Avançar** para visualizar o resumo do relatório.

14. Na página Resumo de relatório, selecione as guias disponíveis no relatório de resumo para visualizar suas configurações do relatório.

Resultados

O relatório é gerado imediatamente. Se você limpou a caixa de seleção **Você gostaria de executar o relatório agora** na página final do assistente, o relatório será salvo e irá gerar na hora programada. O título do relatório é o título padrão para o relatório gerado. Se você reconfigurar um relatório para inserir um novo título de relatório, o relatório será salvo como um novo relatório com o novo nome; no entanto, o relatório original permanecerá o mesmo.

Tarefas de gerenciamento de relatório

A guia Relatórios e o assistente de relatórios são usados para gerenciar relatórios.

É possível editar, duplicar, compartilhar e marcar relatórios. É possível também excluir relatórios gerados.

Editando um relatório

Usando o assistente Relatório, você pode editar qualquer relatório padrão ou customizado a ser alterado.

Sobre Esta Tarefa

Você pode usar ou customizar um número significativo de relatórios padrão. A guia padrão **Relatórios** exibe a lista de relatórios. Cada relatório captura e exibe os dados existentes.

Procedimento

1. Clique na guia **Relatórios**.
2. Dê um clique duplo no relatório que você deseja customizar.
3. No assistente Relatório, altere os parâmetros para customizar o relatório para gerar o conteúdo que necessitar.

Resultados

Se você configurar novamente um relatório para inserir um novo título de relatório, o relatório será salvo como um novo relatório com o novo nome; no entanto, o relatório original permanecerá o mesmo.

Visualizando relatórios gerados

Na guia **Relatórios**, um ícone será exibido na coluna **Formatos** se um relatório possuir conteúdo gerado. Você pode clicar no ícone para visualizar o relatório.

Sobre Esta Tarefa

Quando um relatório gerado possui conteúdo, a coluna **Relatórios gerados** exibe uma caixa de listagem. A caixa de listagem exibe todo o conteúdo gerado, que é organizado pelo registro de data e hora do relatório. Os relatórios mais recentes são exibidos no topo da lista. Se um relatório não possui conteúdo gerado, o valor **Nenhum** é exibido na coluna **Relatórios gerados**.

Ícones que representam o formato do relatório do relatório gerado são exibidos na coluna de **Formatos**.

Os relatórios podem ser gerados nos formatos de PDF, HTML, RTF, XML e XLS.

Nota: Os formatos XML e XLS estão disponíveis apenas para relatórios que usam um formato de tabela de gráfico único (retrato ou paisagem).

Você pode visualizar apenas os relatórios para o qual você tenha recebido acesso do administrador. Os usuários administrativos podem acessar todos os relatórios.

Se você usar o navegador da web Mozilla Firefox e selecionar o formato do relatório RTF, o navegador da web Mozilla Firefox iniciará uma nova janela do navegador. Essa ativação da nova janela é o resultado da configuração do navegador da web Mozilla Firefox e não afeta o QRadar. Você pode fechar a janela e continuar com a sessão QRadar.

Procedimento

1. Clique na guia **Relatórios**.
2. Na caixa de listagem da coluna **Relatórios gerados**, selecione o registro de data e hora de relatório que você deseja visualizar.
3. Clique no ícone para o formato que deseja visualizar.

Excluindo conteúdo gerado

Ao excluir o conteúdo gerado, todos os relatórios que foram gerados a partir do modelo de relatório serão eliminados, mas o modelo de relatório será retido.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione os relatórios para o qual você deseja excluir o conteúdo gerado.
3. Na caixa de listagem **Ações**, clique em **Excluir conteúdo gerado**.

Gerando um relatório manualmente

Um relatório pode ser configurado para gerar automaticamente; entretanto, você pode gerar um relatório manualmente a qualquer momento.

Sobre Esta Tarefa

Enquanto um relatório é gerado, a coluna **Próximo tempo de execução** exibirá uma das três mensagens a seguir:

- **Gerando** – o relatório está sendo gerado.
- **Enfileirado (posição na fila)** – o relatório é enfileirado para a geração. A mensagem indica a posição que o relatório está na fila. Por exemplo, 1 de 3.
- **(x hora(s) x min.(s) y seg.(s))** – o relatório é planejado para ser executado. A mensagem é um cronômetro de contagem decrescente que especifica quando o relatório irá executar o próximo.

Você pode selecionar o ícone **Atualizar** para atualizar a visualização, incluindo as informações na coluna **Próximo tempo de execução**.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que deseja gerar.
3. Clique em **Executar relatório**.

O que Fazer Depois

Depois que o relatório for gerado, será possível visualizar o relatório gerado na coluna **Relatórios gerados**.

Duplicando um relatório

Para criar um relatório muito parecido com um relatório existente, você pode duplicar o relatório que deseja modelar e, em seguida, customizá-lo.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que deseja duplicar.
3. Na caixa de listagem **Ações**, clique em **Duplicar**.

4. Insira um novo nome, sem espaços, para o relatório.

O que Fazer Depois

Você pode customizar o relatório duplicado.

Compartilhando um relatório

Você pode compartilhar relatórios com outros usuários. Ao compartilhar um relatório, você fornecerá uma cópia do relatório selecionado para outro usuário editar ou planejar.

Sobre Esta Tarefa

Quaisquer atualizações que o usuário fizer em um relatório compartilhado não afetarão a versão original do relatório.

Você deve ter os privilégios administrativos para compartilhar os relatórios. Além disso, para um novo usuário visualizar e acessar relatórios, um usuário administrativo deverá compartilhar todos os relatórios necessários com o novo usuário.

Você só pode compartilhar o relatório com usuários que possuam o acesso apropriado.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione os relatórios que você deseja compartilhar.
3. Na caixa de listagem **Ações**, clique em **Compartilhar**.
4. Na lista de usuários, selecione os usuários com quem você deseja compartilhar esse relatório.

Relatórios de marca

Para colocar marca em relatórios, você pode importar logotipos e imagens específicas. Para colocar marca em relatórios com logotipos customizados, você deve fazer upload e configurar os logotipos antes de começar a usar o assistente de relatório.

Antes de Iniciar

Assegure-se de que o gráfico que você deseja usar seja de 144 x 50 pixels com um plano de fundo branco.

Para se certificar de que seu navegador exiba o novo logotipo, limpe o cache do navegador.

Sobre Esta Tarefa

Atribuir marca ao relatório será benéfico para sua empresa se você suportar mais de um logotipo. Ao fazer upload de uma imagem, a imagem é automaticamente salva como Gráfico de Rede Móvel (PNG).

Quando você faz upload de uma nova imagem e configura a imagem como seu padrão, a nova imagem padrão não é aplicada aos relatórios que foram gerados

anteriormente. Atualizar o logotipo nos relatórios gerados anteriormente requer que você gere manualmente o novo conteúdo do relatório.

Se você fizer upload de uma imagem que seja maior em comprimento do que o cabeçalho do relatório pode suportar, a imagem será automaticamente redimensionada para ajustar o cabeçalho; isso é de aproximadamente 50 pixels de altura.

Procedimento

1. Clique na guia **Relatórios**.
2. No menu de navegação, clique em **Atribuir marca**.
3. Clique em **Navegar** para procurar os arquivos que estão localizados em seu sistema.
4. Selecione o arquivo que contém o logotipo que você deseja fazer upload. Clique em **Abrir**.
5. Clique em **Carregar imagem**.
6. Selecione o logotipo que você deseja usar como padrão e clique em **Configurar imagem padrão**.

Grupos de relatórios

É possível classificar relatórios em grupos funcionais. Se categorizar relatórios em grupos, será possível organizar de forma eficiente e localizar os relatórios.

Por exemplo, é possível visualizar todos os relatórios que são relacionados à conformidade com o Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento (PCIDSS).

Por padrão, a guia **Relatórios** exibe a lista de todos os relatórios, no entanto, é possível categorizar relatórios em grupos como:

- Conformidade
- Executivo
- Fontes de log
- Gerenciamento de redes
- Segurança
- VoIP
- Outros

Ao criar um novo relatório, será possível designar o relatório em um grupo existente ou criar um novo grupo. Deve-se ter acesso administrativo para criar, editar ou excluir grupos.

Para obter mais informações sobre funções de usuário, consulte o *Guia de Administração do IBM Security QRadar Log Manager*.

Criando um grupo de relatórios

Você pode criar novos grupos.

Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.

3. Usando a árvore de navegação, selecione o grupo no qual você deseja criar um novo grupo.
4. Clique em **Novo grupo**.
5. Insira valores para os seguintes parâmetros:
 - **Nome** - Digite o nome para o novo grupo. O nome pode ter até 255 caracteres de comprimento.
 - **Descrição** - Opcional. Digite uma descrição para este grupo. A descrição pode ter até 255 caracteres de comprimento.
6. Clique em **OK**.
7. Para alterar o local do novo grupo, clique no novo grupo e arraste a pasta para o novo local na árvore de navegação.
8. Feche a janela Grupos de relatórios.

Editando um grupo

Você pode editar um grupo de relatórios para alterar o nome ou a descrição.

Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Na árvore de navegação, selecione o grupo que você deseja editar.
4. Clique em **Editar**.
5. Atualize os valores para os parâmetros, conforme necessário:
 - **Nome** - Digite o nome para o novo grupo. O nome pode ter até 255 caracteres de comprimento.
 - **Descrição** - Opcional. Digite uma descrição para este grupo. A descrição pode ter até 255 caracteres de comprimento. Esse campo é opcional.
6. Clique em **OK**.
7. Feche a janela Grupos de relatórios.

Designar um relatório a um grupo

Você pode usar a opção **Designar grupos** para designar um relatório para outro grupo.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que deseja designar para um grupo.
3. Na caixa de listagem **Ações**, selecione **Designar grupos**.
4. Na lista **Grupos de itens**, selecione a caixa de seleção do grupo que deseja designar para este relatório.
5. Clique em **Designar grupos**.

Copiando um relatório para outro grupo

Use o ícone **Copiar** para copiar um relatório para um ou mais grupos de relatórios

Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Na árvore de navegação, selecione o relatório que você deseja copiar.

4. Clique em **Copiar**.
5. Selecione o grupo ou grupos aos quais você deseja copiar o relatório.
6. Clique em **Designar grupos**.
7. Feche a janela Grupos de relatórios.

Removendo um relatório

Use o ícone **Remove** para remover um relatório de um grupo.

Sobre Esta Tarefa

Ao remover um relatório de um grupo, ele ainda existirá na guia **Relatórios**. O relatório não é removido do sistema.

Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Na árvore de navegação, navegue até a pasta que contém o relatório ao qual você deseja remover.
4. Na lista de grupos, selecione o relatório que você deseja remover.
5. Clique em **Remove**.
6. Clique em **OK**.
7. Feche a janela Grupos de relatórios.

Contêiner do gráfico

O tipo de gráfico determina como o relatório gerado apresenta dados e objetos da rede.

É possível colocar em gráfico dados com diversas características e criar os gráficos em um único relatório gerado.

Parâmetros de contêiner do gráfico Vulnerabilidades do ativo

A tabela a seguir descreve os parâmetros de contêiner do gráfico Vulnerabilidades do ativo:

Parâmetro	Descrição
Detalhes do contêiner – Ativos	
Título do Gráfico	Digite um título de gráfico de, no máximo, 100 caracteres.
Chart Sub-Title	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limit Assets to Top	Na caixa de listagem, selecione quantos ativos você deseja incluir nesse relatório.

Parâmetro	Descrição
Tipo de Gráfico	<p>Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem:</p> <ul style="list-style-type: none"> • Tabela agregada – exibe os dados em uma tabela agregada, que é uma tabela que contém subtabelas (sub-relatórios). Ao selecionar essa opção, você deverá configurar os detalhes do sub-relatório. A opção Tabela está disponível somente para o contêiner de largura de página inteira. • Barras - Exibe os dados em um gráfico de barras. Ao selecionar essa opção, o relatório não incluirá os dados do sub-relatório. Esse é o padrão. Este tipo de gráfico requer que a procura salva seja uma procura agrupada. • Pizza - Exibe os dados em um gráfico de pizza. Ao selecionar essa opção, o relatório não incluirá os dados do sub-relatório. Este tipo de gráfico requer que a procura salva seja uma procura agrupada. <p>Para visualizar os exemplos de cada tipo de dados do gráfico, consulte Consultar tipos de gráficos.</p>
Order Assets By	<p>Selecione o tipo de dados no qual você deseja que o gráfico seja ordenado. As opções incluem:</p> <ul style="list-style-type: none"> • Peso do ativo – ordena os dados pelo peso do ativo definido no perfil de ativo. • Risco CVSS - ordena os dados pelo nível de risco do Common Vulnerability Scoring System (CVSS). Para obter mais informações sobre o CVSS, consulte http://www.first.org/cvss/ . • Contagem de vulnerabilidade – ordena os dados pela contagem de vulnerabilidade dos ativos.
Sub-Report Details	
Sub-report	Especifica o tipo de informações exibidas no sub-relatório.

Parâmetro	Descrição
Order Subreport By	<p>Selecione o parâmetro pelo qual você deseja organizar os dados do sub-relatório. As opções incluem:</p> <ul style="list-style-type: none"> • Risco (Pontuação Básica) • ID do OSVDB • Título do OSVDB • Última Data de Modificação • Data de Divulgação • Data da Descoberta <p>Para obter mais informações sobre o Open Source Vulnerability Database (OSVDB), consulte http://osvdb.org/.</p>
Limit Sub-report to Top	Na caixa de listagem, selecione quantas vulnerabilidades você deseja incluir nesse sub-relatório.
Conteúdo do Gráfico	
Vulnerabilidades	<p>Para especificar as vulnerabilidades, você deseja relatar:</p> <ol style="list-style-type: none"> 1. Clique em Pesquisar. 2. Na caixa de listagem Procurar por, selecione o atributo de vulnerabilidade o qual você deseja procurar. As opções incluem CVE ID, Bugtraq ID, OSVDB ID e OSVDB Title. Para obter mais informações sobre os atributos de vulnerabilidade, consulte o Gerenciamento de ativos. 3. Na lista Resultados da procura, selecione as vulnerabilidades que você deseja relatar. Clique em Incluir. 4. Clique em Enviar.
Endereço IP	Insira o endereço IP, CIDR ou uma lista delimitada por vírgulas dos endereços IP que você deseja relatar. Os CIDRs parciais são permitidos.
Redes	Na árvore de navegação, selecione uma ou mais redes na qual reunir os dados do gráfico.

Parâmetros do contêiner do gráfico Eventos/logs

A tabela a seguir descreve os parâmetros do contêiner do gráfico Eventos/logs

Tabela 45. Parâmetros do contêiner do gráfico Eventos/logs

Parâmetro	Descrição
<i>Detalhes do contêiner – Eventos/logs</i>	
Título do Gráfico	Digite um título de gráfico de, no máximo, 100 caracteres.

Tabela 45. Parâmetros do contêiner do gráfico Eventos/logs (continuação)

Parâmetro	Descrição
Chart Sub-Title	Limpe a caixa de seleção para alterar o subtítulo automaticamente criado. Digite um título de, no máximo, 100 caracteres.
Limit Events/Logs to Top	Na caixa de listagem, selecione o número de eventos/logs a serem exibidos no relatório gerado.
Tipo de Gráfico	<p>Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem:</p> <ul style="list-style-type: none"> • Barras - Exibe os dados em um gráfico de barras. Esse é o tipo de gráfico padrão. Este tipo de gráfico requer que a procura salva seja uma procura agrupada. • Linha – Exibe os dados em um gráfico de linha. • Pizza - Exibe os dados em um gráfico de pizza. Este tipo de gráfico requer que a procura salva seja uma procura agrupada. • Barras empilhadas – Exibe os dados em um gráfico de barras empilhadas. • Linhas empilhadas – Exibe os dados em um gráfico de linhas empilhadas. • Tabela – Exibe os dados em formato de tabela. A opção Tabela está disponível somente para o contêiner com largura de página completa. <p>Para visualizar exemplos de cada tipo de dado de gráfico de diagramas, consulte Consulte tipos de diagrama.</p>

Tabela 45. Parâmetros do contêiner do gráfico *Eventos/logs* (continuação)

Parâmetro	Descrição
<p>Manual Scheduling</p>	<p>A área de janela Planejamento manual será exibida somente se foi selecionada a opção planejamento Manualmente no assistente de relatório.</p> <p>Usando as opções de Planejamento manual, é possível criar um planejamento manual que pode executar um relatório ao longo de um período de tempo definido customizado, com a opção para incluir somente dados a partir dos dias e horas selecionados. Por exemplo, é possível planejar um relatório para ser executado de 1 de outubro a 31 de outubro, incluindo os dados que são gerados apenas durante o horário comercial, como de segunda a sexta, das 8h às 21h.</p> <p>Para criar um planejamento manual:</p> <ol style="list-style-type: none"> 1. Na caixa de listagem De, digite a data inicial que deseja para o relatório ou selecione a data usando o ícone Calendário. O padrão é a data atual. 2. Nas caixas de listagem, selecione o horário de início que deseja para o relatório. O horário está disponível em incrementos de meia hora. O padrão é 1h da manhã. 3. Na caixa de listagem Para, digite a data de encerramento que deseja para o relatório, ou selecione a data usando o ícone Calendário. O padrão é a data atual. 4. Nas caixas de listagem, selecione o horário de encerramento que deseja para o relatório. O horário está disponível em incrementos de meia hora. O padrão é 1h da manhã. 5. Na caixa de listagem Fuso horário, selecione o fuso horário que deseja usar para o relatório. 6. Ao configurar o parâmetro Timezone, considere o local dos Processadores de eventos que estão associados à procura de evento usada para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como GMT -5.00 America/New_York, os dados da Europa relatam o fuso horário incorretamente.

Tabela 45. Parâmetros do contêiner do gráfico Eventos/logs (continuação)

Parâmetro	Descrição
Manual Scheduling (continuação)	<p>Para refinar ainda mais seu planejamento:</p> <ol style="list-style-type: none"> 1. Selecione a caixa de seleção Seleção de dados de destino. Opções adicionais são exibidas. 2. Selecione a caixa de seleção Apenas horas a partir de e, usando as caixas de listagem, selecione o intervalo de tempo que deseja para o relatório. Por exemplo, é possível selecionar apenas horas das 8h às 17h. 3. Selecione a caixa de seleção para cada dia da semana para o qual deseja programar o relatório.
Hourly Scheduling	<p>A área de janela Planejamento horário será exibida apenas se a opção planejamento Horário for selecionada no assistente de relatório.</p> <ul style="list-style-type: none"> • Na caixa de listagem Fuso horário, selecione o fuso horário que deseja usar para o relatório. • Ao configurar o parâmetro Timezone, considere o local dos Processadores de evento associados à procura de eventos usados para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como GMT -5.00 America/New_York, os dados da Europa relatam o fuso horário incorretamente. <p>O Planejamento Horário coloca em gráficos automaticamente todos os dados da hora anterior.</p>

Tabela 45. Parâmetros do contêiner do gráfico Eventos/logs (continuação)

Parâmetro	Descrição
Daily Scheduling	<p>A área de janela Planejamento diário será exibida apenas se a opção planejamento Diário for selecionada no assistente de relatório.</p> <ol style="list-style-type: none"> 1. Escolha uma das opções a seguir: 2. Todos os dados do dia anterior (24 horas) 3. Dados do dia anterior a partir de – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O horário está disponível em incrementos de meia hora. O padrão é 1h da manhã. 4. Na caixa de listagem Fuso horário, selecione o fuso horário que deseja usar para o relatório. 5. Ao configurar o parâmetro Timezone, considere o local dos Processadores de evento associados à procura de eventos usados para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como GMT -5.00 America/New_York, os dados da Europa relatam o fuso horário incorretamente.

Tabela 45. Parâmetros do contêiner do gráfico Eventos/logs (continuação)

Parâmetro	Descrição
Weekly Scheduling	<p>A área de janela Planejamento semanal será exibida apenas se a opção de planejamento Semanal for selecionada no assistente de relatório.</p> <ol style="list-style-type: none"> 1. Escolha uma das opções a seguir: 2. Todos os dados da semana anterior 3. Todos os dados da semana anterior a partir de – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é domingo. 4. Na caixa de listagem Fuso horário, selecione o fuso horário que deseja usar para o relatório. 5. Ao configurar o parâmetro Timezone, considere o local dos Processadores de evento associados à procura de eventos usados para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como GMT -5.00 America/New_York, os dados da Europa relatam o fuso horário incorretamente. <p>Para refinar ainda mais seu planejamento:</p> <ol style="list-style-type: none"> 1. Selecione a caixa de seleção Seleção de dados de destino. Opções adicionais são exibidas. 2. Selecione a caixa de seleção Apenas horas a partir de e, usando as caixas de listagem, selecione o intervalo de tempo que deseja para o relatório. Por exemplo, é possível selecionar apenas horas das 8h às 17h. 3. Selecione a caixa de seleção para cada dia da semana para o qual deseja programar o relatório.

Tabela 45. Parâmetros do contêiner do gráfico *Eventos/logs* (continuação)

Parâmetro	Descrição
<p>Monthly Scheduling</p>	<p>A área de janela Planejamento mensal será exibida somente se tiver selecionado a opção de planejamento Mensal no assistente de relatório.</p> <ol style="list-style-type: none"> 1. Escolha uma das opções a seguir: 2. Todos os dados do mês anterior 3. Dados do mês anterior a partir de – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é 1 a 31. 4. Na caixa de listagem Fuso horário, selecione o fuso horário que deseja usar para o relatório. 5. Ao configurar o parâmetro Timezone, considere o local dos Processadores de evento associados à procura de eventos usados para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como GMT -5.00 America/New_York, os dados da Europa relatam o fuso horário incorretamente. <p>Para refinar ainda mais seu planejamento:</p> <ol style="list-style-type: none"> 1. Selecione a caixa de seleção Seleção de dados de destino. Opções adicionais são exibidas. 2. Selecione a caixa de seleção Apenas horas a partir de e, usando as caixas de listagem, selecione o intervalo de tempo que deseja para o relatório. Por exemplo, é possível selecionar apenas horas das 8h às 17h. 3. Selecione a caixa de seleção para cada dia da semana para o qual deseja programar o relatório.
<p>Conteúdo do Gráfico</p>	
<p>Grupo</p>	<p>Na caixa de listagem, selecione um grupo de procura salvo para exibir as procuras salvas pertencentes a esse grupo na caixa de listagem Procuras salvas disponíveis.</p>

Tabela 45. Parâmetros do contêiner do gráfico Eventos/logs (continuação)

Parâmetro	Descrição
<p>Digitar Procura Salva ou Selecionar a partir da Lista</p>	<p>Para refinar a lista Procuras salvas disponíveis, digite o nome da procura que deseja localizar no campo Digitar procura salva ou Selecionar a partir da lista. É possível também digitar uma palavra-chave para exibir uma lista de procuras que incluam essa palavra-chave. Por exemplo, digite <i>Firewall</i> para exibir uma lista de todas as procuras que incluem Firewall no nome de procura.</p>
<p>Procuras Salvas Disponíveis</p>	<p>Fornece uma lista de procuras salvas disponíveis. Por padrão, todas as procuras salvas disponíveis são exibidas; no entanto, é possível filtrar essa lista selecionando um grupo na caixa de listagem Grupo ou digitando o nome de uma procura salva conhecida no campo Digitar procura salva ou Selecionar a partir da lista.</p>
<p>Criar Nova Procura de Evento</p>	<p>Clique em Criar nova procura de evento para criar uma nova procura. Para obter mais informações sobre como criar uma procura de evento, consulte Consulte investigação de atividade de log.</p>

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 documentação em outros países. Consulte seu representante IBM local para obter informações sobre os 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 garante ao Cliente nenhum direito 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 consultas sobre licenças a respeito de informações do conjunto de caracteres de byte duplo (DBCS), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie consultas, por escrito, para:

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

O parágrafo a seguir não se aplica ao Reino Unido ou a qualquer país em que tais disposições não estejam de acordo com a legislação local:

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

Estas informações podem incluir imprecisões técnicas ou erros tipográficos. 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.

Quaisquer referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes 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 ele para o propósito de ativação: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações que foram trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-14
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

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

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

Todos os dados sobre desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais poderão variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão as mesmas em sistemas disponíveis em geral. Além disso, algumas medidas podem ter sido estimadas por meio de 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 instruções relativas às direções ou intenções futuras da IBM estão sujeitas a mudanças ou retirada sem aviso prévio, e apenas representam metas e objetivos.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso. Os preços dos revendedores podem variar.

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

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

Marcas registradas

IBM, o logotipo IBM e ibm.com são marcas ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se esses e outros termos de marca registrada da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca registrada (® ou ™), esses símbolos indicam marcas registradas de direito consuetudinário ou registrado nos Estados Unidos pertencentes à IBM no momento em que essas informações foram publicadas. Tais marcas podem estar registradas ou podem ser marcas registradas de direito consuetudinário em outros países. Uma lista atual de marcas registradas IBM está disponível na Web em Informações de copyright e de marca registrada (www.ibm.com/legal/copytrade.shtml).

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



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

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

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

Considerações de política de privacidade

Os produtos de Software IBM, incluindo soluções de software as a service, (“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 outras finalidades. Em muitos casos, nenhuma informação de identificação pessoal 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 as informações pessoalmente identificáveis, as informações específicas sobre o uso de cookies desta oferta serão apresentadas 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>, a seção intitulada “Cookies, Web Beacons e Outras Tecnologias”, na Declaração de Privacidade Online da IBM em <http://www.ibm.com/privacy/details/br/pt/> e “IBM Software Products and Software-as-a-Service Privacy Statement” em <http://www.ibm.com/software/info/product-privacy>.

Glossário

Este glossário fornece termos e definições para o software e produtos do IBM Security QRadar SIEM.

As seguintes referências cruzadas são usadas neste glossário:

- *Consulte* refere-se a um termo não preferencial para um termo preferencial ou de uma abreviação para o formato completo.
- *Consulte também* encaminha-o para um termo relacionado ou contrastante.

Para outros termos e definições adicionais, consulte o website de Terminologia da IBM (abre em uma nova janela).

"A" "B" "C" "D" na página 156 "E" na página 156 "F" na página 156 "G" na página 157 "H" na página 157 "I" na página 157 "L" na página 157 "M" na página 158 "N" na página 158 "O" na página 158 "P" na página 159 "R" na página 159 "S" na página 160 "T" na página 160 "V" na página 160

A

acumulador

Um registro no qual um operando de uma operação pode ser armazenado e, subsequentemente, substituído pelo resultado dessa operação.

Alta disponibilidade (HA)

Referente a um sistema em cluster que é reconfigurado quando ocorrem falhas de nó ou daemon para que as cargas de trabalho possam ser redistribuídas para os nós restantes no cluster.

anomalia

Um desvio do comportamento esperado da rede.

ARP Consulte Protocolo de Resolução de Endereço.

ASN Consulte número do sistema autônomo.

assinatura de aplicativo

Um conjunto exclusivo de características que são derivadas pela análise de carga útil do pacote e, em seguida, usadas para identificar um aplicativo específico.

B

Banco de Dados de Vulnerabilidade de Origem Aberta (OSVDB)

Criado pela comunidade de segurança de rede para a comunidade de segurança de rede, um banco de dados de origem aberta que fornece informações técnicas sobre vulnerabilidades de segurança da rede.

C

camada de rede

Na arquitetura de OSI, a camada que fornece serviços para estabelecer um caminho entre sistemas abertos com uma qualidade de serviço previsível.

captura de conteúdo

Um processo que captura uma quantidade configurável de carga útil e armazena os dados em um log de fluxo.

CIDR Consulte Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)

Um método para incluir endereços Internet Protocol (IP) de classe C. Os endereços são oferecidos aos Provedores de Serviço da 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 solicita os serviços a partir de um servidor.

Cluster de HA

Uma configuração de alta disponibilidade que consiste em um servidor principal e um servidor secundário.

codificação

Em segurança de computador, o processo de dados de transformação para uma forma ininteligível de tal maneira que os dados originais não possam ser obtidos ou só possam ser obtidos usando um processo de decifração.

Código de Autenticação de Mensagem Baseada em Hash (HMAC)

Um código criptográfico que usa uma função hash de criptografia e uma chave secreta.

Common Vulnerability Scoring System (CVSS)

Um sistema de pontuação pelo qual a gravidade de uma vulnerabilidade é medida.

comportamento

Os efeitos observáveis de uma operação ou de um evento, incluindo seus resultados.

conjunto de referência

Uma lista de elementos únicos derivados de eventos ou fluxos em uma rede. Por exemplo, uma lista de endereços IP ou uma lista de nomes de usuário.

console

Uma estação de exibição a partir da qual um operador pode controlar e observar a operação do sistema.

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 Internet Protocol (IP) segura 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 concede a um usuário ou processo certos direitos de acesso.

credibilidade

Uma classificação numérica entre 0-10 que é usada para determinar a integridade de um evento ou uma ofensa. A credibilidade aumenta à medida que várias origens relatam o mesmo evento ou ofensa.

cronômetro de atualização

Um dispositivo interno que é disparado manualmente ou automaticamente em intervalos de tempo que atualiza os dados da atividade de rede atual.

CVSS Consulte Common Vulnerability Scoring System.

D

dados de carga útil

Os dados do aplicativo contidos em um fluxo de IP, excluindo informações de cabeçalho e administrativas.

destino de encaminhamento

Um ou mais sistemas do fornecedor que recebem dados brutos e normalizados a partir de fontes de log e fontes de fluxo.

destino externo

Um dispositivo que está fora do site primário que recebe fluxo de evento ou de dados de um coletor de eventos.

DHCP Consulte Dynamic Host Configuration Protocol.

DNS Consulte Sistema de Nomes de Domínio.

DSM Consulte Módulo de Suporte de Dispositivo.

duplicar fluxo

Várias instâncias da mesma transmissão de dados recebidos a partir de origens de fluxo diferentes.

E

endereço IP virtual de cluster

Um endereço IP que é compartilhado entre o host primário ou secundário e o cluster de HA.

F

fluxo Uma única transmissão de dados transmitidos através de um link durante uma conversação.

folha Em uma árvore, uma entrada ou um nó que não possui filhos.

FQDN Consulte o nome completo do domínio.

FQNN Consulte o nome da rede qualificada.

funcionário público

Um componente interno que analisa o tráfego de rede e eventos de segurança com relação a regras customizadas definidas.

G

gateway

Um dispositivo ou programa usado para conectar redes ou sistemas com diferentes arquiteturas de rede.

gravidade

Uma medida da ameaça relativa que uma origem apresenta em um destino.

H

HA Consulte alta disponibilidade.

hierarquia de rede

Um tipo de contêiner que constitui uma coleta hierárquica de objetos da rede.

HMAC

Consulte Código de Autenticação de Mensagem em Hash.

host de HA primário

O computador principal que é conectado ao cluster de HA.

host de HA secundário

O computador de espera que está conectado ao cluster de HA. O host de HA secundário assumirá a responsabilidade do host de HA primário se este falhar.

I

ICMP Consulte Internet Control Message Protocol.

Identidade

Uma coleção de atributos de uma fonte de dados que representa uma pessoa, organização, lugar ou um item.

IDS Consulte sistema de detecção de intrusão.

interconexão de sistemas abertos (OSI)

A interconexão de sistemas abertos em concordância com padrões da Organização Internacional para Normatização (ISO) para a troca de informações.

Internet Control Message Protocol (ICMP)

Um protocolo da Internet que é usado por um gateway para comunicar com outro host como, por exemplo, relatar um erro em um datagrama.

Internet Protocol (IP)

Um protocolo que roteia dados através de uma rede ou redes interconectadas. Esse protocolo age como um intermediário entre as camadas de protocolo mais altas e a rede física. Consulte também Protocolo de Controle de Transmissões.

intervalo de relatório

Um intervalo de tempo configurável no final do qual o processador de evento deve enviar todos os dados de fluxo e eventos capturados para o console.

intervalo de união

O intervalo no qual os eventos são empacotados. O pacote configurável de eventos ocorre em intervalos de 10 segundos 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 Internet Protocol.

IPS Consulte sistema de prevenção de intrusão.

ISP Consulte o Provedor de serviço da Internet.

L

LAN Consulte local area network (rede local).

LAN (Rede Local)

Uma rede que conecta diversos dispositivos em uma área limitada (com um único edifício ou campus) e que pode ser conectada a uma rede maior.

LDAP Consulte protocolo LDAP.

L2L Consulte Local para Local.

Local para Local (L2L)

Relativo ao tráfego interno de uma rede local para outra rede local.

Local Para Remoto (L2R)

Relativo ao tráfego interno de uma rede local para outra rede remota.

log de fluxo

Uma coleta de registros de fluxo.

L2R Consulte Local Para Remoto.

M

magnitude

Uma medida da importância relativa de uma determinada ofensa. Magnitude é um valor ponderado calculado a partir de relevância, gravidade e credibilidade.

mapa de referência

Um registro de dados do 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 diversos valores. Por exemplo, o mapeamento de uma lista de usuários privilegiados para um host.

mapa de referência de mapas

Um registro de dados com duas chaves mapeadas para vários valores. Por exemplo, o mapeamento do total de bytes de um aplicativo para um IP de origem.

Mapa QID

Uma taxonomia que identifica cada evento exclusivo e mapeia os eventos para as categorias de nível inferior e de 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.

Módulo de Suporte de Dispositivo (DSM)

Um arquivo de configuração que analisa os eventos recebidos a partir de várias origens de log e converte-os em um formato de taxonomia padrão que pode ser exibido como saída.

multicast em IP

Transmissão de um datagrama de IP (Internet Protocol) a um conjunto de sistemas que formam um grupo de multicast.

N

NAT Consulte Conversão de Endereço de Rede.

NetFlow

Um protocolo de rede Cisco que monitora dados do fluxo de tráfego de rede. Os

dados NetFlow incluem as informações do cliente e do servidor, quais portas são usadas e o número de bytes e pacotes que fluem através dos comutadores e roteadores conectados a uma rede. Os dados são enviados para coletores NetFlow onde a análise de dados ocorre.

nome completo da rede qualificada (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.

número de sistema autônomo (ASN)

Em TCP/IP, um número que é designado para um sistema autônomo pela mesma autoridade central que designa endereços IP. O número de sistema autônomo torna possível para algoritmos de roteamento automatizado distinguir sistemas autônomos.

O

objeto de folha de dados

Um objeto terminal ou um nó em uma hierarquia de banco de dados.

objeto de 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 se uma política foi violada ou se a rede está sofrendo um ataque.

origem de log

O equipamento de segurança ou equipamento de rede do qual um log de eventos se origina.

origem externa

Um dispositivo que está fora do site primário que envia dados normalizados para um coletor de eventos.

origens de fluxo

A origem a partir do qual o fluxo é

capturado. Uma fonte de fluxo é classificada como interna quando o fluxo é proveniente do hardware instalado em um host gerenciado ou é classificado como externa quando o fluxo é enviado para um coletor de fluxo.

OSI Consulte interconexão de sistemas abertos.

OSVDB
Consulte Banco de Dados de Vulnerabilidade de Origem Aberta.

P

peso de rede
O valor numérico aplicado a 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.

positivo falso
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).

protocolo
Um conjunto de regras que controla a comunicação e transferência de dados entre dois ou mais dispositivos ou sistemas em uma rede de comunicação.

Protocolo de Configuração de Host Dinâmico (DHCP)

Um protocolo de comunicação que é usado para gerenciar centralmente as informações de configuração. Por exemplo, o DHCP designa automaticamente endereços IP a computadores em uma rede.

Protocolo de Controle de Transmissões (TCP)

Um protocolo de comunicação usado na Internet e em qualquer rede que segue os padrões do IETF (Internet Engineering Task Force) para o protocolo de interligação de redes. O TCP fornece um protocolo de host para host confiável nas redes de comunicação comutadas por pacote e em sistemas interconectados dessas redes. Consulte também Internet Protocol.

Protocolo de Resolução de Endereço (ARP)

Um protocolo que mapeia dinamicamente um endereço IP para um endereço de adaptador de rede em uma rede local.

Protocolo LDAP

Um protocolo aberto que usa TCP/IP para fornecer acesso a diretórios que suportam um modelo X.500 e que não incorre nos requisitos de recurso do Directory Access Protocol (DAP) X.500 mais complexo. Por exemplo, o LDAP pode ser usado para localizar pessoas, organizações e outros recursos em um diretório da Internet ou da intranet.

Protocolo Simples de Gerenciamento de Rede

Um conjunto de protocolos para sistemas de monitoramento e dispositivos em redes complexas. As informações sobre os dispositivos gerenciados são definidas e armazenadas em uma Management Information Base (MIB).

Provedor de serviço da Internet (ISP)

Uma organização que fornece acesso à Internet.

R

Redirecionamento do ARP

Um método ARP para notificar o host se existir 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 atendidos 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, de uma categoria ou ofensa na rede.

Remoto Para Local (R2L)

O tráfego externo a partir de uma rede remota para uma rede local.

Remoto Para Remoto (R2R)

O tráfego externo a partir de uma rede remota para outra rede remota.

R2L Consulte Remoto Para Local.

R2R Consulte Remoto Para Remoto.

S**servidor whois**

Um servidor que é usado para recuperar as informações sobre recursos da Internet registrada, como nomes de domínio e alocações de endereço IP.

sistema ativo

Em um cluster de alta disponibilidade (HA), o sistema que tem todos os seus serviços em execução.

sistema de detecção de intrusão (IDS)

Software que detecta as tentativas e ataques bem-sucedidos em recursos monitorados que fazem parte de uma rede ou sistema host.

sistema de espera

Um sistema que automaticamente se torna ativo quando o sistema ativo falhar. Se a replicação de disco estiver ativada, replicará os 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 prevenção de intrusão (IPS)

Um sistema que tenta negar a atividade potencialmente dolosa. Os mecanismos de negação poderiam envolver a filtragem, rastreamento ou configuração dos limites de taxa.

SNMP

Consulte Protocolo Simples de Gerenciamento de Rede.

SOAP Um protocolo leve, baseado em XML para troca de informações em um ambiente distribuído e descentralizado. O SOAP pode ser usado para consultar e retornar informações e chamar os serviços através da Internet.

sub-procura

Uma função que permite que uma consulta de procura seja executada dentro de um conjunto de resultados de procura concluída.

sub-rede

Consulte sub-rede.

sub-rede (subnet)

Uma rede dividida em subgrupos independentes menores, que ainda estão interconectados.

superfluxo

Um fluxo único que seja 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 mapeie as chaves que possuem um tipo designado para outras chaves que, então, são mapeadas para um valor único.

TCP Consulte Protocolo de Controle de Transmissões.

V**violação**

Um ato que ignora ou desrespeita a política corporativa.

visualização dos sistemas

Uma representação visual dos hosts primários e gerenciados que compõem um sistema.

Índice Remissivo

A

- administrador da rede vii
- ajuda 12
- ajuda online 12
- área de janela de correções do Windows, 118
- área de janela de interface de rede 118
- Área de janela de pacotes 118
- Área de janela de políticas de risco 118
- Área de janela de produtos 118
- área de janela de propriedades 118
- Área de janela de serviços 118
- Área de janela de vulnerabilidade 118
- as funções da barra de ferramentas de detalhes do evento 44
- assistente de regras customizadas 6, 18
- assistente Regra de Detecção de Anomalias 85
- ativar regras 87
- atividade de log 9, 12, 15, 19, 22, 25, 45, 51, 52, 53, 57, 65, 66, 68, 69, 70, 71, 73, 81
 - critérios de procura 63
 - visão geral 25
- atividade de rede 12, 22, 51, 53, 57, 65
- ativo 101
- ativos 5, 12, 15
- atualizando detalhes do usuário 12
- atualizar dados 9

B

- barra de ferramenta atividade de log 29
- barra de ferramentas 25
- barra de ferramentas da página regras 92
- barra de ferramentas de detalhes do evento 44
- barra de status 30, 131
- blocos de construção 81
 - editando 91

C

- caixa de lista de exibição 36
- cancelar uma procura 68
- classificar resultados em tabelas 8
- coluna de dados do PCAP 47, 48
- compartilhar relatórios 138
- configurando atividade de log 20
- configurando conexões 20
- configurando gráficos 53
- configurando itens do painel 20
- configurar e gerenciar redes, plug-ins e componentes 6
- configurar e gerenciar sistemas 6
- configurar e gerenciar usuários 6
- configurar tamanho da página 15
- Contêiner do gráfico 141
- conteúdo de ajuda 12

- controles 6
- copiar procura salva 71, 113
- copiar um item para um grupo 90
- copiar uma regra 87
- criando grupos de procura 69
- criando regras customizadas 84
- criando um novo grupo de procura 70
- criar novo grupo de procura 113
- criar relatórios 5
- criar um grupo de regras 89
- critérios de procura
 - excluindo 64
 - guia atividade de log 64
 - salvando 63
 - salvos disponíveis 64

D

- dados de captura de pacote (PCAP) 46
- dados do evento bruto 34
- dados do evento não analisados 34
- dados do PCAP 47, 48
- desativar regras 87
- descrição do evento 41
- designar itens para um grupo 89
- detalhes da vulnerabilidade 116
- detalhes do evento 44
- detalhes do evento único 41
- distribuir relatórios 5
- download do arquivo de dados 48
- Duplicar um relatório 137

E

- editar ativo 106
- editar blocos de construção 91
- editar grupo de procura 113
- editar um grupo 89, 140
- editar um grupo de procura 70
- endereço IP 9, 100
- especificar número de objetos de dados para visualizar 20
- especificar tipo de gráfico 20
- eventos 17, 53, 57
- eventos de monitoramento 15
- eventos normalizados 31
- excluindo ativos 114
- excluindo uma procura 69
- excluir painel 22
- excluir perfil de ativo 114
- excluir uma regra 88
- executando uma procura 65
- executar dados 9
- exibir em uma nova janela 21
- exibir itens 17
- exportando ativos 115
- exportando eventos 49
- exportar perfil do ativo 114

F

- fazer download do arquivo PCAP 48
- filtro rápido 29, 57
- fluxo de eventos 31
- fluxos 53, 57
- funções 81
- fuso horário 128

G

- gerar um relatório manualmente 137
- Gerenciador de Vulnerabilidade QRadar 99
- gerenciamento de grupo de regras 88
- gerenciamento de painel 15
- gerenciamento de regras 81, 86
- gerenciando grupos de procura 69
- Gerenciar grupos 113
- gerenciar rede 99
- gerenciar relatórios 5, 129
- gerenciar resultados da procura 68, 69
- glossário 155
- gráfico de série temporal 52
- grupo
 - copiando um item 90
 - designando itens 89
 - editando 89
 - excluindo 90
 - excluindo um item 90
 - removendo 71
- grupo de procura
 - criando 70
 - editando 70
- grupo de procura de eventos 70
- grupo de regras
 - criando 89
 - visualizando 88
- grupos de procura
 - gerenciando 69
 - visualizando 69
- grupos de procura de ativos 112
- guia Admin 6
- guia atividade de log 4, 8, 25, 30, 31, 34, 36, 47, 49, 57, 66
- guia atividade de rede 8, 57
- guia ativo 99, 100, 103, 112
- guia ativos 5, 99, 101, 104, 106, 112, 113, 114, 115
- guia ofensas 8
- guia padrão 4
- guia painel 4, 6, 15, 19, 21, 22
- Guia Painel 4, 15
- guia relatório 128, 129
- guia relatórios 5, 8, 128
- guias 4
- guias da interface com o usuário 4, 6

H

- hosts 5

I

- IBM Security QRadar Vulnerability Manager 5
- ícone remover 114
- ID 100
- imagem
 - relatórios
 - atribuição de marca 138
 - upload 138
- importar ativos 115
- importar perfil de ativo 114
- imprimir perfil de ativo 99
- incluindo itens de eventos 22
- incluindo itens de procura de fluxo 22
- incluir ativo 99, 106
- incluir filtro 65
- incluir itens 19, 22
- informações de login 4
- informações de login padrão 4
- informações do filtro de eventos 103
- informações sobre o usuário 12
- interface com o usuário 4
- introdução vii
- investigando eventos 15
- investigar a atividade de log 25
- investigar ativo 99
- investigar os logs de eventos 4
- item de painel da notificação do sistema 18
- item de painel resumo do sistema 17
- item do painel 22
- itens do painel atividade de log 15

J

- janela de grupos de procura 69

L

- Layout de relatório 131
- legendas do gráfico 53
- lista de eventos 41

M

- manter a regra customizada 81
- manter regras customizadas 81
- mapear evento 45
- mensagem de notificação 18
- menu ativado pelo botão direito 30
- menu de mensagens 6
- modificar mapeamento de evento 45
- modo de documento
 - Navegador da web do Internet Explorer 3
- modo do navegador
 - Navegador da web do Internet Explorer 3
- mostrar painel 21, 22

N

- Navegador da web
 - versões suportadas 3
- navegar no QRadar 3

- nome de usuário 4
- nome dos ativos 100
- nomes de usuário 11
- notificação do sistema 22
- notificações do sistema 6
- nova procura 113
- novos recursos
 - visão geral da versão 7.2.2 do guia do usuário 1

O

- O que há de novo
 - visão geral da versão 7.2.2 do guia do usuário 1
- objetos do gráfico 53
- ofensas 15, 57, 70
- ofensas atualizadas 17
- opções de eventos agrupados 36
- opções de menu ativado pelo botão direito 103
- ordem de classificação 129
- organizar os itens do painel 15
- origem de log 34

P

- página de detalhes do evento 41
- página de perfis de ativos 100
- página de procura de ativo 110
- página perfil de ativos 116, 118, 121, 123, 124, 125, 126
- painel 22
- painel de gerenciamento de vulnerabilidade 17
- parâmetros da área de janela de correções do Windows 125
- Parâmetros da área de janela de pacotes 124
- parâmetros da área de janela de políticas de risco 126
- parâmetros da área de janela de produtos 126
- parâmetros da área de janela de propriedades 125
- parâmetros da área de janela de resumo da interface de rede 121
- parâmetros da área de janela de resumo de ativo 118
- parâmetros da área de janela de serviço do Windows 124
- Parâmetros da área de janela de serviços 123
- Parâmetros da área de janela de vulnerabilidade 121
- parâmetros da guia relatório 128
- parâmetros da página perfil de ativos 118
- parâmetros de eventos agrupados 36
- parâmetros de regra 91
- pausar dados 9
- perfil de ativo 104, 106
- perfis de ativos 99, 111, 112, 113, 115
- Perfis de ativos 101, 114
- permissão de regra 81
- permissões 128

- permissões (*continuação*)
 - propriedades customizadas 73
- pontuação do CVSS agregado 100
- positivos falsos 99
- procurando 57
- procurando perfis de ativos 110
- procurar 113
 - copiando para um grupo 71
- procurar por ativo 99
- procuras de dados 57
- propriedade
 - copiando customizada 79
 - modificando customizada 78
- propriedade customizada 80
- propriedade de cálculo 76
- propriedade regex 74
- propriedades de evento customizado 73

Q

- QID 45

R

- redimensionar colunas 12
- regra
 - copiando 87
 - editar 87
 - respostas 82
- regra de detecção de anomalias 85
- regra de evento 81
- regras 81
 - ativando 87
 - desativando 87
 - visualizando 83
- relatório
 - editando 136
- relatórios 12, 15
 - visualizando 136
- Relatórios gerados mais recentemente 17
- relatórios personalizados 132
- remover grupo 71, 114
- remover item do painel 21
- remover procura salva 114
- remover procura salva de um grupo 71
- remover um item do painel 21
- renomear painel 21
- Resposta de Regra 94
- resultados da procura
 - cancelar 68
 - excluindo 69
 - salvando 66
 - visualizando gerenciado 66
- resultados do processador de evento 30
- resumo de atividade nas últimas 24 horas 17

S

- salvando critérios de procura de evento e de fluxo 31
- salvando resultados da procura 66
- salvar critérios 111
- salvar critérios de procura de ativos 111
- scanner de terceiros 99
- senha 4

serviços 100
servidores 5
sinalizador 18
sincronizar tempo 128

T

tabelas 15
tempo do console 11
tempo do sistema 11
tempo real 31
tempo real (fluxo) 9
testes 81
tipo de propriedade calculada 73

tipo de propriedade regex 73
tipos de diagrama 132
tipos de gráfico 131
tipos de propriedade 73

U

último minuto (atualização automática) 9

V

vários painéis 15
visão geral de gráficos 51

visualização de dados 48
visualização de eventos agrupados 36
visualização de mensagens 6
visualização do grupo de regra 88
visualizando eventos de fluxo 31
visualizando grupos de procura 69, 112
visualizando perfil de ativos 104
visualizando resultados da procura gerenciada 66
visualizar ativos 99
visualizar notificações do sistema 22
visualizar regras customizadas 81
vulnerabilidades 99
Vulnerabilidades 100
vulnerabilidades de ativo 116