

IBM Security QRadar Log Manager
Versão 7.2.5

Guia dos Usuários



Observação

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 161.

Informações do produto

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

© Copyright IBM Corporation 2012, 2015.

Índice

Sobre o Guia do Usuário do QRadar Log Manager	vii
Capítulo 1. O que há de novo para os usuários no QRadar Log Manager V7.2.5.	1
Capítulo 2. QRadar Log Manager	3
Navegadores da Web Suportados	3
Ativando o Modo de Documento e o Modo de Navegador no Internet Explorer	3
Login do IBM Security QRadar	4
Guias da interface com o usuário	4
Guia Paineis	4
Guia Atividade de log	4
Guia Ativos.	4
Guia Relatórios	5
Guia IBM Security QRadar Vulnerability Manager	5
Guia Administração	5
Procedimentos comuns do QRadar	6
Visualizando mensagens	6
Classificando resultados	8
Atualizando e pausando a interface com o usuário	8
Investigando endereços IP	9
Investigar nomes de usuário	11
Tempo do sistema	11
Atualizando preferências do usuário	11
Redimensionar colunas	12
Tamanho da página	12
Capítulo 3. Gerenciamento de painel	13
Atividade de log	13
Relatórios mais recentes	15
Resumo do sistema	15
Itens de gerenciamento de vulnerabilidade	15
Notificação do sistema.	16
Incluindo itens do painel	17
Usando o painel para investigar a atividade de log	17
Configurando gráficos.	18
Removendo itens do painel	19
Removendo um item do painel.	19
Renomeando um painel	20
Excluindo um painel	20
Gerenciando notificações do sistema	20
Incluindo itens baseados em painel para a lista Incluir Itens	21
Capítulo 4. Investigação de atividade de log	23
Visão geral da guia Atividade de log	23
Barra de ferramentas da guia Atividade de log	23
Opções de menu ativado pelo botão direito.	27
Barra de status	27
Monitorando a atividade de log	28
Visualizando eventos de fluxo	28
Visualizando eventos normalizados	28
Visualizando eventos brutos.	31
Visualizando eventos agrupados	33
Detalhes do evento	38
Barra de ferramentas de detalhes do evento	41

Visualizando ofensas associadas	42
Modificando mapeamento de eventos	43
dados do PCAP	44
Exibindo a coluna de dados do PCAP	44
Visualizando informações do PCAP	45
Fazendo download do arquivo PCAP para seu sistema de desktop	46
Exportando eventos	46
Capítulo 5. Visão geral de gerenciamento de ativos	49
Origens de dados de ativo	49
Atualizações nos dados de ativo	50
Mesclagem de ativo	52
Desvios de crescimento de ativo	52
Notificações do sistema para desvios de crescimento de ativo	53
A resolução de problemas nos perfis de ativos que excedem o limite de tamanho normal	54
Os dados de ativo novo são incluídos nas	
listas de bloqueio de ativo	55
Listas de bloqueio de ativos	56
Regras de exclusão de reconciliação de ativo	56
Exemplo: Regras de exclusão de ativo que são ajustadas para excluir endereços IP da lista de bloqueio.	58
Exemplo: Como os erros de configuração para extensões de origem de log podem causar desvios de crescimento de ativo	59
Capítulo 6. Gerenciamento de gráfico	61
Visão geral do gráfico de série temporal	61
Legendas do gráfico	63
Configurando gráficos	63
Capítulo 7. Procuras de dados	67
Procurando por itens que correspondem aos seus critérios.	67
Salvando critérios de procura	73
Procura planejada	74
Opções de procura avançada	75
Exemplos de sequência de caracteres de procura AQL	77
Opções de procura de filtro rápido	80
Usando uma subprocura para refinar resultados da procura	81
Gerenciando resultados da procura	82
Excluindo critérios de procura	82
Salvando resultados da procura	83
Visualizando resultados da procura gerenciada	83
Cancelando uma procura	85
Excluindo uma procura	86
Gerenciando grupos de procura	86
Visualizando grupos de procura	86
Criando um novo grupo de procura	87
Editando um grupo de procura	87
Copiando uma procura salva em outro grupo	87
Removendo um grupo ou uma procura salva de um grupo	88
Capítulo 8. Propriedades de evento customizado	89
Permissões requeridas	89
Tipos de propriedades customizadas	89
Criando uma propriedade customizada baseada em regex	90
Criando uma propriedade customizada baseada em cálculo	92
Modificando uma propriedade customizada	93
Copiando uma propriedade customizada	95
Excluindo uma propriedade customizada	95
Capítulo 9. Gerenciamento de regra	97
Considerações sobre permissão de regra	97

Visão geral de regras	97
Regra de evento	97
Condições da regra	97
Respostas da regra	98
Visualizando regras.	99
Criando uma regra customizada	100
Criando uma regra de detecção de anomalia	101
Tarefas de gerenciamento de regra	103
Ativando e desativando regras	103
Editando uma regra	103
Copiando uma regra	104
Excluindo uma regra	104
Gerenciamento de grupo de regras	104
Visualizando um grupo de regra	105
Criando um grupo	105
Designando um item a um grupo	105
Editando um grupo	105
Copiando um item para outro grupo	106
Excluindo um item de um grupo	106
Excluindo um grupo	106
Editando blocos de construção	107
Parâmetros de página Regra	107
Barra de ferramentas da página Regras.	108
Parâmetros da página Resposta de regra	110
Capítulo 10. Perfis de ativos	115
Vulnerabilidades	115
Visão geral da guia Ativos	115
Lista da guia Ativo	116
Barra de ferramentas da guia Ativos.	117
Opções de menu ativado pelo botão direito	119
Visualizando um perfil de ativos	120
Incluindo ou editando um perfil de ativo	122
Procurando perfis de ativos	126
Salvando critérios de procura de ativos.	127
Grupos de procura de ativos	128
Visualizando grupos de procura	128
Criando um novo grupo de procura.	129
Editando um grupo de procura	129
Copiando uma procura salva em outro grupo	130
Removendo um grupo ou uma procura salva de um grupo	130
Tarefas de gerenciamento de perfil do ativo	130
Excluindo ativos	131
Importando perfis de ativos	131
Exportando ativos.	131
Pesquisar vulnerabilidades de ativos	132
Parâmetros da página Perfil de ativo	135
Área de janela de resumo de ativo	135
Área de janela de resumo da interface de rede	138
Área de janela Vulnerabilidade	138
Área de janela Serviços	139
Área de janela de Serviços do Windows	140
Área de janela de pacotes	140
Área de janela de correções do Windows	141
Área de janela de propriedades	141
Área de janela Políticas de risco	142
Área de janela Produtos	142
Capítulo 11. Gerenciamento de relatório	143
Visão geral da guia Relatórios.	144

Considerações sobre fuso horário	144
Permissões da guia Relatório	144
Parâmetros da guia Relatório	144
Ordem de classificação na guia Relatório	145
Barra de ferramentas da guia Relatório	145
Layout de relatório	148
Tipos de gráfico	148
Tipos de diagrama.	149
Criando relatórios customizados	149
Tarefas de gerenciamento de relatório	153
Editando um relatório	153
Visualizando relatórios gerados	153
Excluindo conteúdo gerado.	154
Gerando um relatório manualmente.	154
Duplicando um relatório	155
Compartilhando um relatório	155
Relatórios de marca	155
Grupos de relatórios	156
Criando um grupo de relatórios	157
Editando um grupo	157
Compartilhando grupos de relatórios	157
Designar um relatório a um grupo	159
Copiando um relatório para outro grupo	159
Removendo um relatório	159
Avisos	161
Marcas comerciais	163
Considerações sobre política de privacidade	163
Glossário	165
A	165
B	165
C	165
D	166
E	167
F	167
G	167
H	167
I	167
L	168
M	168
N	168
O	169
P	169
R	169
S	170
T	171
V	171
Índice Remissivo.	173

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

Entrando em contato com o suporte ao cliente

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

Declaração de boas práticas de segurança

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

Observe:

O uso deste Programa pode implicar várias leis ou regulamentos, incluindo aqueles relacionados à privacidade, à proteção de dados, ao emprego, às comunicações eletrônicas e ao armazenamento. O IBM Security QRadar pode ser usado apenas para propósitos legais e de uma forma legal. O cliente concorda em usar este Programa conforme as leis, os regulamentos e as políticas aplicáveis e assume toda a responsabilidade de obedecê-los. O licenciado declara que irá obter ou obteve quaisquer consentimentos, permissões ou licenças necessários para ativar o uso legal do IBM Security QRadar.

Capítulo 1. O que há de novo para os usuários no QRadar Log Manager V7.2.5

IBM Security QRadar Log Manager V7.2.5 apresenta aprimoramentos de relatório, novas opções de procura avançada e mais..

Aprimoramentos de relatório

É possível compartilhar os relatórios com grupos de usuários. É possível incluir um relatório em um grupo de relatórios que é compartilhado com qualquer pessoa ou um grupo que esteja compartilhado somente com usuários que possuem funções de usuário específico e perfis de segurança.  Saiba mais...

É possível configurar uma classificação para um relatório, como confidencial ou somente interno, que aparece no cabeçalho do relatório e rodapé. Também é possível incluir números de página e criar relatórios que sejam baseados em procuras de ativos salvas.  Saiba mais...

Opções de pesquisa mais avançadas

Use o operador TEXT SEARCH para executar procuras completas de texto e encontrar textos específicos nas propriedades customizadas para eventos.  Saiba mais...

Modificar uma regra customizada mantém as informações de estado para todas as regras

Ao editar uma regra customizada e salvar as mudanças, somente a regra que você está modificando e quaisquer regras que dependam dessa regra são afetadas. Todas as informações de estado, contadores e resultados de regra para outras regras são mantidas. Nas liberações anteriores, quando você editou uma regra customizada, todas as regras e contadores no mecanismo de regra customizada foram reconfiguradas. Por exemplo, se você estiver rastreando uma sequência de eventos, como 5 logons com falha seguidos por um logon bem-sucedido, a contagem foi reconfigurada quando modificou e salvou alguma regra.

Para obter mais informações, consulte Contador de texto de regra APAR (<http://www-01.ibm.com/support/docview.wss?crawler=1&uid=swg1IV46111>).

Capítulo 2. 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.

Navegue para o 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 em produtos IBM Security QRadar funcionarem corretamente, 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 do usuário e a senha devem ser configurados com antecedência pelo administrador.

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

Tabela 1. Navegadores da Web Suportados para Produtos QRadar

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

Ativando o Modo de Documento e o Modo de Navegador no Internet Explorer

Se 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. No seu navegador da Web Internet Explorer, pressione F12 para abrir a janela Ferramentas do 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 **Padrões do Internet Explorer 9**.
 - Para o Internet Explorer V10.0, selecione **Padrões do Internet Explorer 10**.

Login do 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 sobre os dados do evento.

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

Guia Ativos

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

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

Por exemplo, um ataque tenta usar um serviço específico que está em execução em um ativo específico. Nesta situação, o QRadar pode determinar se o ativo está vulnerável a este ataque correlacionando o ataque com o 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 criar, distribuir e gerenciar relatórios para quaisquer dados no QRadar.

O recurso Relatórios permitirá a criação de relatórios customizados para uso operacional e executivo. Para criar um relatório, é possível combinar 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. Após varreduras identificarem vulnerabilidades, será possível procurar e revisar dados de vulnerabilidade, corrigir vulnerabilidades e executar varreduras novamente 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 Administração

Os administradores usam a guia Administração para configurar e gerenciar os usuários, sistemas, redes, plug-ins e componentes. Os usuários com privilégios de administração 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	Configure o sistema e as opções de gerenciamento do usuário.
Origens de Dados	Configure origens de log.
Configuração de Redes e Serviços Remotos	Configure redes remotas e grupos de serviços.
Plug-ins	Acesse 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 mostradas na janela **Mensagens**, o administrador deve criar uma regra baseada em cada tipo de mensagem de notificação e selecionar a caixa de opções **Notificar** no **Assistente de regras customizadas**.

Sobre Esta Tarefa

O menu **Mensagens** indica quantas notificações não lidas do sistema 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. É possível 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 executar na janela **Mensagens** são propagadas para a guia **Painel** e a janela pop-up. Por exemplo, se você fechar uma notificação do sistema da 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 de mensagens

Função	Descrição
Todos	Clique em Todos para visualizar todas as notificações do sistema. Essa opção é o padrão, portanto, você clicará em Todos apenas se você selecionar outra opção e deseja exibir todas as notificações do sistema novamente.
Funcionamento	Clique em Funcionamento para visualizar apenas as notificações do sistema que tenham um nível de severidade de funcionamento.
Erros	Clique em Erros para visualizar apenas as notificações do sistema que tenham um nível de severidade de erro.
Avisos	Clique em Avisos para visualizar apenas as notificações do sistema que tenham um nível de severidade de aviso.
Informações	Clique em Informações para visualizar apenas as notificações do sistema que tenham um nível de severidade de informações.
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 funcionamento • Descartar todos os avisos • Descartar todos os avisos • Descartar todas as informações

Tabela 4. Funções disponíveis na janela de 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 funcionamento • Visualizar todos os avisos • Visualizar todas as informações
Descartar	Clique no ícone 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, clique em **Mensagens**.
3. Na janela **Mensagens**, visualize 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 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 da 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

É possível atualizar, pausar e executar manualmente os dados exibidos nas guias.

Sobre Esta Tarefa

A guia **Atividade de log** atualizará automaticamente a cada 60 segundos, se você estiver visualizando a guia no modo 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 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 do painel pausa automaticamente a guia. 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 o cronômetro estiver pausado.

Investigando endereços IP

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

Sobre Esta Tarefa

É possível 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 de WHOIS padrão é whois.arin.net.
Informações > Varredura de porta	Executa uma varredura de Mapeador de Rede (NMAP) do endereço IP selecionado. Essa opção estará disponível somente se o NMAP estiver instalado em seu sistema. Para obter mais informações sobre a instalação do NMAP, consulte a documentação do seu fornecedor.

Tabela 5. Informações de endereços IP (continuação)

Opção	Descrição
Informações > Perfil de ativo	Exibe 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 associadas a esse endereço IP.
Informações > Procurar conexões	Procura por conexões associados a esse endereço IP. Essa opção será exibida somente 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 <i>Guia do Usuário do IBM Security QRadar Risk Manager</i> .
Informações > Consulta de porta de computador	
Informações > Visualizar topologia	Exibe a guia que representa a topologia da camada 3 de 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.
Executar Varredura de Vulnerabilidade	Selecione a opção Executar Varredura de Vulnerabilidade para uma varredura do IBM Security QRadar Vulnerability Manager nesse endereço IP. Essa opção será exibida somente quando o IBM Security QRadar Vulnerability Manager estiver sendo 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 no endereço IP ou no nome do recurso 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.

Será possível investigar 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 do menu para investigação do 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 durante as 24 horas anteriores.
Visualizar eventos	Exibe os eventos que estão associados ao nome de usuário selecionado. Para obter mais informações sobre a janela Lista de eventos, consulte Registrar monitoramento de atividade.

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

Tempo do sistema

O canto direito da interface com o usuário do 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 desktop.

Ao aplicar filtros e procuras com base em tempo na guia **Atividade de log**, será necessário 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 IBM Security QRadar SIEM.

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 1 caractere especial • Conter 1 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 seguintes idiomas: inglês, chinês simplificado, chinês tradicional, japonês, coreano, francês, alemão, italiano, espanhol, russo e português (Brasil). Se você escolher um idioma diferente, a interface com o usuário será exibida em inglês. Outras convenções culturais associadas, como tipo de caractere, ordenação, formato de data e hora, unidade de moeda são usadas.
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.

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.

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 quando é efetuado login.

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

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 dentro de uma sessão afetam apenas o seu sistema.

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

- Incluir e remover itens de painel dos seus painéis.
- Mover e posicionar itens para atender seus requisitos. Ao posicionar itens, cada item será automaticamente redimensionado proporcionalmente ao painel.
- Incluir itens de painel customizados que são baseados em quaisquer dados.

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 do 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 fechados ou ocultos 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. Os 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 em seu menu da guia 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 dados reais de última hora 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 crime representa em relação a quão preparado o destino está 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 Origens 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.

O monitor 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 nas últimas 24 horas.

Dentro do item de resumo, é possível 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 Gerenciamento de vulnerabilidade serão exibidos 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*.

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

O QRadar inclui o critério de procura salvo padrão que é pré-configurado para exibir itens de procura no 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 Notificação do sistema exibe notificações de eventos que são recebidos pelo sistema.

Para notificações para mostrar no item de 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 do evento e criar regras de evento, consulte o *Guia de Administração IBM Security QRadar Log Manager*.

No item de painel **Notificações do sistema**, é possível visualizar as seguintes informações:

- **Sinalizador** – Exibe um símbolo para indicar o nível de severidade da notificação. Aponte para o símbolo para visualizar mais detalhes sobre o nível de severidade.
 - Ícone **Funcionamento**
 - Ícone **Informações (?)**
 - Ícone **Erro (X)**
 - Ícone **Aviso (!)**
- **Criado** - Exibe a quantidade de tempo decorrida desde que a notificação foi criada.
- **Descrição** – Exibe informações sobre a notificação.
- **Descartar ícone (x)** – Permitirá que seja fechada uma notificação do sistema.

É possível apontar o mouse sobre uma notificação para visualizar mais detalhes:

- **IP de host** – Exibe o endereço IP do host do host que originou a notificação.
- **Severidade** – Exibe o nível de severidade do incidente que criou esta notificação.
- **Categoria de nível inferior** – 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 decorrida desde que a notificação foi criada.

Ao incluir o item de painel **Notificações do sistema**, as notificações do sistema também poderão ser exibidas como notificações pop-up na interface com o usuário do QRadar. Estas notificações pop-up são exibidas no canto inferior direito da interface com o usuário, independentemente da guia selecionada.

Notificações pop-ups estão disponíveis apenas para usuários com permissões administrativas e são ativados por padrão. Para desativar notificações pop-up, selecione **Preferências do usuário** e limpe 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 a 12) for exibido no cabeçalho, a notificação atual é 1 de 12 notificações a serem exibidas.

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

- **Próximo ícone (>)** – 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 de um item do painel **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 do 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
Barras, Pizza e Tabela	A guia de Atividade de log exibe um gráfico de barras, gráfico de pizza e tabela de detalhes.

Tipo de gráfico	Descrição
Séries temporais	<p>A guia Atividade de log exibe gráficos de acordo com os seguintes critérios:</p> <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 intervalo de tempo for maior do que 1 hora, um gráfico da séries temporais 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 no gráfico. As opções incluem todos os eventos normalizados e customizados ou parâmetros de fluxo incluídos em seus parâmetros de procura.
Tipo de gráfico	<p>Na caixa de listagem, selecione o tipo de gráfico que você deseja visualizar. As opções incluem:</p> <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 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 .

Tabela 8. Configurando gráficos (continuação). Opções de parâmetros.

opção	descrição
Capturar Dados de Série Temporal	Selecione essa caixa de seleção para ativar a captura de séries temporais. Ao selecionar essa caixa de seleção, o recurso gráfico começará a acumular dados para os gráficos de séries temporais. Por padrão, esta opção está desativada.
Intervalo de tempo	Na caixa de listagem, selecione o intervalo de tempo que você deseja visualizar.

As configurações de gráfico customizado são retidas, para que sejam exibidas conforme configuradas a cada vez que você acessa 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. Os parâmetros acumulados são indicados por um asterisco (*) na caixa de listagem **Valor para Gráfico**. Se você selecionar um valor para gráfico que não esteja acumulado (sem asterisco), os dados de séries temporais não estarão disponíveis.

Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel que contenha o item que você deseja customizar.
3. No cabeçalho do item do 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

É possível 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 do painel e exibi-lo em uma nova janela no sistema do desktop.

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

É possível 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**, insira 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

É possível 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

É possível 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** foi 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**

É possível incluir itens de painel baseados em procura no seu menu **Incluir itens**.

Antes de Iniciar

Para incluir um item de painel de eventos no menu **Incluir item** na guia **Painel**, deve-se acessar a guia **Atividade de log** para criar critérios de procura que especificam que os resultados da procura podem ser exibidos na guia **Painel**. O critério de procura também deve especificar que os resultados sejam agrupados em um parâmetro.

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 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 origem de log, como um dispositivo de firewall ou roteador, que descreve uma ação em uma rede ou host.

É necessário ter permissão para visualizar a guia **Atividade de log**.

Barra de ferramentas da guia **Atividade de log**

É possível acessar várias opções a partir da 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
Procura	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	Nesta caixa de listagem, é possível executar procuras salvas anteriormente. As opções são exibidas na caixa de listagem Procuras rápidas apenas quando forem salvos os critérios de procura que especificam a opção Incluir em minhas procuras salvas .
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 a conclusão de uma procura. 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 estará visível apenas 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 critérios de procura agregados porque os critérios da procura salvos especificam os parâmetros requeridos. <p>Nota: As opções de regra de detecção de anomalias serão visíveis apenas se tiver a permissão Atividade de log > Manter regras customizadas.</p> <ul style="list-style-type: none"> • Incluir limite de regra – Selecione esta opção para criar uma regra de limite. Uma regra de limite testa o tráfego do evento para a atividade que excede um limite configurado. Os limites podem ser baseados em quaisquer dados que são coletados QRadar. Por exemplo, se for criada uma regra de limite indicando que não mais de 220 clientes podem efetuar login no servidor entre 8h e 17h, as regras gerarão um alerta quando o cliente 221º tentar efetuar login. <p>Ao selecionar a opção Incluir regra de limite, o assistente de regras é exibido, pré-preenchido 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 730"> <p>• Incluir regra comportamental – Selecione esta opção para criar uma regra comportamental. Uma regra comportamental testa o tráfego de eventos da 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 durante a última hora. Se houver uma alteração de mais de 40%, a regra irá gerar uma resposta.</p> <p>Ao selecionar a opção Incluir regra comportamental, o assistente de regras será exibido e pré-preenchido com as opções apropriadas para criar uma regra comportamental.</p> <li data-bbox="959 892 1453 1270"> <p>• Incluir regra de anomalia – Selecione esta opção para criar uma regra de anomalia. Uma regra de anomalia testa o tráfego de evento da 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 pré-preenchido com as opções apropriadas para criar uma regra de anomalia.</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. Esta é a opção recomendada. Consulte Exportando eventos. • Exportar para XML > Exportação integral (todas as colunas) – Selecione esta opção para exportar todos os parâmetros de evento. Uma exportação integral pode demorar um longo período de tempo para ser concluída. Consulte Exportando eventos. • Exportar para CSV > Colunas visíveis – Selecione esta opção para exportar somente as colunas que estão visíveis na guia Atividade de log. Esta 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 evento e de fluxo. • Notificar – Selecione esta opção para especificar que deseja uma notificação por email na conclusão das procuras selecionadas. Esta opção é 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
Barra de ferramentas de procura	<p>Procura avançada Selecione Procura avançada na caixa de listagem para inserir uma sequência de caracteres de procura Ariel Query Language (AQL) para especificar os campos que você deseja que sejam retornados.</p> <p>Filtro rápido Selecione Filtro rápido na caixa de listagem para procurar cargas úteis usando palavras ou frases simples.</p>

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 de 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 o evento selecionado, dependendo do parâmetro selecionado no evento.
Mais opções:	<p>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.</p> <p>Nota: Esta opção não é exibida no modo de fluxo.</p>

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, permitindo que você visualize 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: Este 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 procurados durante o período de tempo especificado. • Duração – Especifica a duração da procura. 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.

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

Parâmetro	Descrição
Gráficos	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.
Fonte 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 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.

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

É possível 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: Este 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 procurados 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>
Gráficos	<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
Fonte 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.
Fonte 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 depende 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
Agrupar por	Especifica o parâmetro no qual a procura está 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 procurados 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
Gráficos	<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 de 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 deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.</p>
IP de Origem (contagem exclusiva)	<p>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.</p>
IP de Destino (contagem exclusiva)	<p>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.</p>
Porta de destino (contagem exclusiva)	<p>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.</p>
Nome do evento	<p>Especifica o nome normalizado do evento.</p>

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 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.
Contagem	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 do QRadar.
Horário da Fonte de Log	Especifica a hora do sistema, conforme relatada pela fonte de log na carga útil do evento.
Informações de origem e destino	
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 de carga útil	
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.
Fonte 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.

Visualizando ofensas associadas

Na guia Atividades de Log, você pode visualizar a ofensa associada ao evento.

Sobre Esta Tarefa

Se um evento corresponder a uma regra, uma ofensa poderá ser gerada na guia **Ofensas**.

Quando você visualiza uma ofensa na guia **Atividade de Log**, a ofensa poderá não ser exibida se o funcionário público ainda não tiver salvo a ofensa associada ao evento selecionado para o disco ou a ofensa for eliminada do banco de dados. Se isso ocorrer, o sistema o notificará.

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. Clique no ícone **Ofensa** ao lado do evento que você deseja investigar.
4. Visualizar a ofensa associada.

Modificando mapeamento de eventos

É possível 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 do QRadar conhecidos, 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 IBM Security QRadar Log Manager*.

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

- **Eventos definidos pelo usuário** - algumas origens de log, como Snort, permitem que você crie eventos definidos pelo usuário.
- **Eventos novos ou 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 eventos quando a categoria de alto nível for Auditoria 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 você 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 específico:
 - 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** ao qual você deseja associar esse evento.
7. Clique em **OK**.

dados do 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 da série SRX da Juniper deverá ser configurada com o protocolo 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 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 **Por grupo**.
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 PCAP ou fazer o download do arquivo PCAP para seu sistema da área de trabalho.

Antes de Iniciar

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

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 de Informações para download do pacote PCAP será exibida. Na maioria dos casos, o processo de download é rápido e essa janela não é exibida.

Depois que o arquivo for recuperado, uma janela pop-up fornecerá uma versão legível do arquivo PCAP. É possível ler as informações exibidas na janela, ou fazer o download das informações para seu sistema da 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**.
 - Clique com o botão direito do mouse no ícone **PCAP** para o evento e selecione **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 o download das informações para o seu sistema da área de trabalho, escolha uma das opções a seguir:
 - Clique em **Fazer o download do arquivo do PCAP** para fazer o download do arquivo PCAP original a ser usado em um aplicativo externo.
 - Clique em **Fazer o 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

É possível fazer download do arquivo PCAP para seu sistema de desktop para armazenamento ou uso em outros aplicativos.

Antes de Iniciar

Para que seja possível visualizar as informações do PCAP, deve-se 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 do 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

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

Antes de Iniciar

O período de tempo necessário 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. Esta 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**. Esta 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 você não selecionar o ícone **Notificar quando estiver pronto**, a janela de status será exibida.

Capítulo 5. Visão geral de gerenciamento de ativos

Coletar e visualizar os dados de ativo ajuda a identificar as ameaças e as vulnerabilidades. Um banco de dados de ativo exato facilita a conexão de ofensas que são acionadas em seu sistema para ativos físicos ou virtuais em sua rede.

Dados de ativo

Um *ativo* é qualquer terminal de rede que envie ou receba os dados em sua infraestrutura de rede. Por exemplo, blocos de notas, servidores, máquinas virtuais e dispositivos portáteis são todos ativos. Cada ativo no banco de dados de ativo é designado a um identificador exclusivo de modo que possa ser distinguido de outros registros de ativo.

Detectar os dispositivos também é útil na construção de um conjunto de dados de informações históricas sobre o ativo. Rastrear as informações de ativo conforme são alteradas ajuda a monitorar o uso de ativo em sua rede.

Perfis de ativos

Um *perfil de ativo* é uma coleção de todas as informações que o IBM Security QRadar SIEM coletou com o tempo sobre um ativo específico. O perfil inclui informações sobre os serviços que estão sendo executados no ativo e quaisquer informações de identidade que sejam conhecidas.

O QRadar SIEM cria automaticamente os perfis de ativo dos eventos de identidade ou, se estiverem configurados, varreduras de avaliação de vulnerabilidade. Os dados são correlacionados através de um processo que é denominado *reconciliação de ativo* e o perfil é atualizado conforme novas informações aparecem no QRadar. O nome do ativo é derivado das informações na atualização de ativo na ordem de precedência a seguir:

- Nome fornecido
- Nome de host NETBios
- Nome do host DNS
- endereço IP

Perfis de ativo de correlação para reduzir positivos falsos

Os administradores usam os perfis de ativo para relatar, procurar, auditar e criar regras para identificar ameaças, vulnerabilidades e uso de ativos. Os dados de ativo também são usados para propósitos de correlação para ajudar a reduzir positivos falsos. Por exemplo, se um invasor tentar usar um serviço específico que esteja em execução em um ativo, o QRadar pode determinar se o ativo é vulnerável a esse ataque, correlacionando o ataque ao perfil de ativo.

Origens de dados de ativo

Os dados de ativo são recebidos de diversas origens diferentes em sua implementação IBM Security QRadar.

Os dados de ativo são gravados para o banco de dados de ativo incrementalmente, geralmente duas ou três partes de dados por vez. Com exceção das atualizações de scanners de vulnerabilidade da rede, cada atualização de ativo contém informações sobre somente um ativo por vez.

Os dados do ativo geralmente são provenientes das origens de dados de ativo a seguir:

Eventos

Cargas úteis de evento, como aquelas criadas por DHCP ou servidores de autenticação, geralmente contêm logins de usuário, endereços IP, nomes de host, endereços MAC e outras informações de ativo. Esses dados são imediatamente fornecidos para o banco de dados de ativo para ajudar a determinar a qual ativo a atualização de ativo se aplica.

Os eventos são a causa primária para os desvios de crescimento de ativo.

Scanners de vulnerabilidade

O QRadar é integrado a scanners de vulnerabilidade da IBM e de terceiros que podem fornecer dados de ativo como sistema operacional, software instalado e informações de correção. O tipo de dados varia de scanner para scanner, e pode variar de varredura para varredura. Conforme novos ativos, informações de porta e vulnerabilidade são descobertos, os dados são trazidos para o perfil de ativo com base nos intervalos de CIDR que são definidos na varredura.

É possível para os scanners introduzir desvios de crescimento de ativo, mas isso é raro.

Interface com o usuário

Os usuários que possuem a regra de Ativos podem importar ou fornecer informações de ativo diretamente para o banco de dados de ativo. As atualizações de ativo que são fornecidas diretamente por um usuário são para um ativo específico e, portanto, é efetuado bypass do estágio de reconciliação de ativo.

As atualizações de ativo que são fornecidas pelos usuários não apresentam desvios de crescimento de ativo.

Dados de ativo de domínio reconhecido

Quando a origem de dados de ativo é configurada com informações de domínio, todos os dados de ativo provenientes dessa origem de dados são automaticamente identificados com o mesmo domínio. Como os dados no modelo de ativo tem domínio reconhecido, as informações de domínio são aplicadas a todos os componentes do QRadar, incluindo identidades, ofensas, perfis de ativo e descoberta de servidor.

Ao visualizar o perfil de ativo, alguns campos podem estar em branco. Os campos em branco existem quando o sistema não tiver recebido essas informações em uma atualização de ativo ou as informações tiverem excedido o período de retenção de ativo. O período de retenção padrão é de 120 dias. Um endereço IP que aparece como 0.0.0.0 indica que o ativo não contém informações de endereço IP.

Atualizações nos dados de ativo

O IBM Security QRadar usa as informações de identificação em uma carga útil do evento para determinar se deve criar um novo ativo ou atualizar um ativo existente.

Cada atualização de ativo deve conter informações confiáveis sobre um único ativo. Quando o QRadar recebe uma atualização de ativo, o sistema determina a qual ativo a atualização se aplica.

A Reconciliação de ativo é o processo de determinar o relacionamento entre as atualizações de ativo e o ativo relacionado no banco de dados de ativo.

A reconciliação de ativo ocorre depois que o QRadar recebe a atualização mas antes que as informações sejam gravadas para o banco de dados de ativos.

Informações de identificação

Cada ativo deve conter pelo menos uma parte dos dados de identificação. As atualizações subsequentes que contêm uma ou mais partes dos mesmos dados de identificação são reconciliados com o ativo que possui esses dados. As atualizações que são baseadas em endereços IP são manipuladas cuidadosamente para evitar correspondências de ativo positivo falso. As correspondências de ativo positivo falso ocorrem quando um ativo físico tem a propriedade designada de um endereço IP que era anteriormente de propriedade de outro ativo no sistema.

Quando múltiplas partes dos dados de identificação forem fornecidas, o gerenciador de perfis de ativo priorizará as informações na ordem a seguir:

- Endereço MAC (mais determinista)
- Nome do host NetBIOS
- Nome do host DNS
- Endereço IP (menos determinista)

Endereços MAC, nomes de host NetBIOS e nomes de host DNS devem ser exclusivos e, portanto, são considerados como dados de identificação definitivos. As atualizações recebidas que correspondem a um ativo existente somente pelo endereço IP são manipuladas de forma diferente das atualizações que correspondem a dados de identificação mais definitivos.

Fluxo de trabalho de atualizações de ativo

Esse fluxo de trabalho descreve como o QRadar usa as informações de identificação em uma carga útil do evento para determinar se deve criar um novo ativo ou atualizar um ativo existente.

1. O QRadar recebe o evento. O gerenciador de perfis de ativo examina a carga útil do evento para informações de identificação.
2. Se as informações de identificação incluírem um endereço MAC, nomes de host NetBIOS ou nome de host DNS que já estejam associados a um ativo no banco de dados de ativo, esse ativo será atualizado com quaisquer novas informações.
3. Se as únicas informações de identificação disponíveis forem um endereço IP, o sistema reconciliará a atualização para o ativo existente que possui o mesmo endereço IP.
4. Se uma atualização de ativo incluir um endereço IP que corresponde a um ativo existente, mas também inclui mais informações de identificação que não corresponda ao ativo existente, o sistema usará outras informações para descartar uma correspondência de positivo falso antes que o ativo existente seja atualizado.
5. Se as informações de identificação não corresponderem a um ativo existente no banco de dados, um novo ativo será criado com base nas informações na carga útil do evento.

Conceitos relacionados:

“Regras de exclusão de reconciliação de ativo” na página 56

Com cada atualização de ativo que entra no IBM Security QRadar, as regras de exclusão de reconciliação de ativo aplicam testes no endereço MAC, nome do host NetBIOS, nome do host DNS e endereço IP na atualização de ativos.

Mesclagem de ativo

A *mesclagem de ativo* é o processo no qual as informações para um ativo são combinadas com as informações para outro ativo sob a premissa de que eles são realmente o mesmo ativo físico.

A mesclagem de ativos ocorre quando uma atualização de ativo contém dados de identificação que correspondem a dois perfis de ativo diferentes. Por exemplo, uma única atualização que contém um nome de host NetBIOS que corresponde a um perfil de ativo e um endereço MAC que corresponde a um perfil de ativo diferente pode acionar uma mesclagem de ativo.

Alguns sistemas podem causar altos volumes de mesclagem de ativos porque possuem origens de dados de ativos que combinam de forma inadvertida informações de identificação de dois ativos físicos diferentes em uma única atualização de ativos. Alguns exemplos desses sistemas incluem os ambientes a seguir:

- Servidores de syslog centrais que agem como um proxy de eventos
- Máquinas virtuais
- Ambientes de instalação automatizada
- Nomes de host não exclusivos, comuns com ativos como iPads e iPhones.
- As redes privadas virtuais que possuem endereços MAC compartilhados
- Extensões de origem de log em que o campo de identidade é `OverrideAndAlwaysSend=true`

Ativos que possuem vários endereços IP, endereços MAC ou nomes de host mostram desvios no crescimento de ativo e podem acionar notificações do sistema.

Conceitos relacionados:

“Desvios de crescimento de ativo”

Às vezes, as origens de dados de ativo produzem atualizações que causam desvios de crescimento de ativo em IBM Security QRadar.

Desvios de crescimento de ativo

Às vezes, as origens de dados de ativo produzem atualizações que causam desvios de crescimento de ativo em IBM Security QRadar.

Desvios de crescimento de ativo ocorrem quando o número de atualizações de ativo para um ativo alcançam o limite de retenção para um tipo específico de informações de identidade. Para manter o funcionamento do banco de dados do ativo QRadar, a intervenção manual é necessária para resolver a acumulação de dados do ativo.

Espera-se que os perfis de ativo cresçam e enriqueçam nos dados com o tempo. Por exemplo, perfil de ativo inclui mais endereços IP conforme coleta leases IP e coleta mais nomes de usuário conforme novos usuários efetuam login. Os desvios de crescimento de ativo indicam que algo está fazendo com que o perfil de ativo colete uma grande quantidade de dados em um ritmo inesperado.

O exemplo de servidor DHCP de crescimento de ativo não natural em um perfil de ativo

Considere um servidor de rede privada virtual (VPN) em uma rede do Protocolo de Configuração de Host Dinâmico (DHCP). O servidor VPN está configurado para designar endereços IP para clientes VPN recebidos, executando proxy de solicitações DHCP em nome do cliente para o servidor DHCP da rede.

Na perspectiva do servidor DHCP, o mesmo endereço MAC solicita repetidamente várias designações de endereço IP. No contexto de operações de rede, o servidor VPN está delegando os endereços IP para os clientes, mas o servidor DHCP não pode distinguir quando uma solicitação é feita por um ativo em nome de outro.

O log do servidor DHCP, que é configurado como origem de log QRadar, gera um evento de reconhecimento de DHCP (DHCP ACK) que associa o endereço MAC do servidor VPN ao endereço IP que é designado ao cliente VPN. Quando ocorre a reconciliação de ativos, o sistema reconcilia esse evento pelo endereço MAC, que resulta em um único ativo existente que aumenta em um endereço IP para cada evento DHCP ACK que é analisado.

Eventualmente, um perfil de ativo contém cada endereço IP que foi alocado para o servidor VPN. Esse desvio de crescimento de ativo é causado pelas atualizações de ativo que contêm informações sobre mais de um ativo.

Configurações de limite

Quando um ativo no banco de dados atinge um número específico de propriedades, tais como múltiplos endereços IP ou endereços MAC, o QRadar bloqueia esse ativo de receber mais atualizações.

As configurações do limite do Gerenciador de perfis do ativo especificam as condições sob as quais um ativo é bloqueado das atualizações. O ativo é atualizado normalmente até o valor limite. Quando o sistema coleta dados suficientes para exceder o limite, o ativo mostra um desvio no crescimento do ativo. As futuras atualizações para o ativo são bloqueadas até que o desvio de crescimento seja retificado.

Notificações do sistema para desvios de crescimento de ativo

IBM Security QRadar gera notificações do sistema para ajudar a identificar e gerenciar os desvios de crescimento de ativo em seu ambiente.

Os desvios de crescimento de ativo, que são crescimento não natural de dados de ativo, são específicos a um ambiente.

Quando um ativo é identificado por mostrar um desvio de crescimento, uma notificação de sistema aparece na lista **Mensagens** na parte superior direita do Console do QRadar. As notificações também aparecem nas **Notificações do sistema** no painel **Monitoramento de sistemas**.

As mensagens de sistema a seguir indicam que o QRadar identificou desvios de crescimento de ativo em potencial:

- Os perfis de ativo detectados pelo sistema que excedem o limite de tamanho normal
- As regras de lista de bloqueio de ativo incluíram dados de novo ativo nas listas de bloqueio de ativos

As mensagens de notificação do sistema incluem links para que os relatórios ajudem a identificar os ativos que possuem desvios de crescimento.

Conceitos relacionados:

“A resolução de problemas nos perfis de ativos que excedem o limite de tamanho normal”

O IBM Security QRadar gera a notificação de sistema a seguir quando a acumulação de dados em um único ativo excede os limites configurados para os dados de identificação.

“Os dados de ativo novo são incluídos nas listas de bloqueio de ativo” na página 55

IBM Security QRadar gera a notificação de sistema a seguir quando uma parte dos dados de ativo exibe o comportamento que é consistente com o crescimento de ativo de desvio.

A resolução de problemas nos perfis de ativos que excedem o limite de tamanho normal

O IBM Security QRadar gera a notificação de sistema a seguir quando a acumulação de dados em um único ativo excede os limites configurados para os dados de identificação.

Os perfis de ativo detectados pelo sistema que excedem o limite de tamanho normal

Explicação

A carga útil da notificação mostra uma lista dos cinco principais ativos frequentemente em desvios e porque o sistema marcou cada ativo como um desvio de crescimento. Conforme mostrado no exemplo a seguir, a carga útil também mostra o número de vezes em que o ativo tentou aumentar além do limite de tamanho do ativo.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.qllabs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

Quando os dados de ativo excedem o limite configurado, o QRadar bloqueia o ativo de atualizações futuras. Essa intervenção evita que o sistema receba mais dados corrompidos e minimiza os impactos de desempenho que possam ocorrer, se o sistema tentar reconciliar as atualizações recebidas em um perfil de ativo estranhamente grande.

Ação do usuário necessária

Use as informações na carga útil de notificação para identificar os ativos que estão contribuindo para o desvio de crescimento de ativo e determinar o que está causando o crescimento anormal. A notificação fornece um link para um relatório de todos os ativos que estão vivenciando o crescimento de ativo de desvio nas últimas 24 horas.

Depois de resolver o desvio de crescimento de ativo em seu ambiente, é possível executar o relatório novamente.

1. Clique na guia **Atividade de log** e clique em **Procurar > Nova procura**.
2. Selecione a procura salva **Crescimento de ativo de desvio: Relatório de ativo**.

3. Use o relatório para identificar e reparar os dados de ativo inexatos que foram criados durante o desvio.

Se os dados de ativo forem válidos, QRadar os administradores podem aumentar os limites para os endereços IP, endereços MAC, nomes de host NetBIOS e nomes de host DNS na **Configuração do gerenciador de perfis de ativo** na guia QRadar Admin.

Para obter mais informações sobre o gerenciamento de desvios de crescimento de ativo, consulte o *Guia de Administração* do produto.

Conceitos relacionados:

“Notificações do sistema para desvios de crescimento de ativo” na página 53 IBM Security QRadar gera notificações do sistema para ajudar a identificar e gerenciar os desvios de crescimento de ativo em seu ambiente.

Os dados de ativo novo são incluídos nas listas de bloqueio de ativo

IBM Security QRadar gera o notificação de sistema a seguir quando uma parte dos dados de ativo exibe o comportamento que é consistente com o crescimento de ativo de desvio.

As regras de lista de bloqueio de ativo incluíram dados de novo ativo nas listas de bloqueio de ativos

Explicação

As regras de exclusão de ativo monitoram dados de ativo para consistência e integridade. As regras rastreiam partes específicas de dados de ativos com o tempo para assegurar que estão sendo observadas consistentemente com o mesmo subconjunto de dados em um tempo razoável.

Por exemplo, se uma atualização de ativo incluir um endereço MAC e um nome de host DNS, o endereço MAC será associado a esse nome de host DNS por um período sustentado. As atualizações de ativo subsequentes que contêm o endereço MAC também contêm esse mesmo nome de host DNS quando um é incluído na atualização de ativo. Se o endereço MAC for repentinamente associado a um nome de host DNS diferente por um curto período, a mudança será monitorada. Se o endereço MAC mudar novamente em um curto período, o endereço MAC será sinalizado por contribuir com uma instância de desvio ou crescimento de ativo anormal.

Ação do usuário necessária

Use as informações na carga útil de notificação para identificar as regras que são usadas para monitorar os dados de ativo. Clique no link **Desvios de ativo por origem de log** na notificação para ver os desvios de ativo que ocorreram nas últimas 24 horas.

Se os dados de ativo forem válidos, os administradores do QRadar podem configurar QRadar para resolver o problema.

- Se suas listas de bloqueio estiverem sendo preenchidas muito agressivamente, será possível ajustar as regras de exclusão de reconciliação de ativo que as preenche.
- Se você deseja incluir os dados no banco de dados de ativo, é possível remover os dados de ativo da lista de bloqueio e incluí-lo na lista de desbloqueio de

ativo correspondente. Incluir os dados de ativo na lista de desbloqueio evita que eles reapareçam inadvertidamente na lista de bloqueio.

Para obter mais informações sobre o gerenciamento de desvios de crescimento de ativo, consulte o *Guia de Administração* do produto.

Conceitos relacionados:

“Regras de exclusão de reconciliação de ativo”

Com cada atualização de ativo que entra no IBM Security QRadar, as regras de exclusão de reconciliação de ativo aplicam testes no endereço MAC, nome do host NetBIOS, nome do host DNS e endereço IP na atualização de ativos.

“Listas de bloqueio de ativos”

Uma *lista de bloqueio de ativos* é uma coleção de dados que o IBM Security QRadar considera não confiável com base nas regras de exclusão de reconciliação de ativos. Os dados na lista de bloqueio de ativos provavelmente contribuem com os desvios de crescimento de ativo e o QRadar evita que os dados sejam incluídos no banco de dados de ativos.

Listas de bloqueio de ativos

Uma *lista de bloqueio de ativos* é uma coleção de dados que o IBM Security QRadar considera não confiável com base nas regras de exclusão de reconciliação de ativos. Os dados na lista de bloqueio de ativos provavelmente contribuem com os desvios de crescimento de ativo e o QRadar evita que os dados sejam incluídos no banco de dados de ativos.

Cada atualização de ativo no QRadar é comparado às listas de bloqueio do ativo. Os dados de ativo incluídos na lista de bloqueio são aplicados globalmente para todos os domínios. Se a atualização de ativo contiver informações de identificação (endereço MAC, nome do host NetBIOS, nome do host DNS ou endereço IP) que sejam encontradas em uma lista de bloqueio, a atualização recebida será descartada e o banco de dados de ativo não será atualizado.

A tabela a seguir mostra o nome de coleção de referência e o tipo para cada tipo de dados de ativo de identidade.

Tabela 17. Nomes de coleção de referência para dados da lista de bloqueio de ativos

Tipo de dados de identificação	Nome de coleção de referência	Tipo de coleção de referência
Endereços IP (v4)	Lista de bloqueio IPv4 de reconciliação de ativo	Conjunto de referência [Tipo de conjunto: IP]
Nomes do host DNS	Lista negra de DNS de reconciliação de ativo	Conjunto de referência [Tipo de conjunto: ALNIC*]
Nomes do host NetBIOS	Lista de bloqueio NetBIOS de reconciliação de ativo	Conjunto de referência [Tipo de conjunto: ALNIC*]
Endereços MAC	Lista de bloqueio MAC de reconciliação de ativo	Conjunto de referência [Tipo de conjunto: ALNIC*]

* ALNIC é um tipo alfanumérico que pode acomodar os valores de nome do host e de endereço MAC.

Regras de exclusão de reconciliação de ativo

Com cada atualização de ativo que entra no IBM Security QRadar, as regras de exclusão de reconciliação de ativo aplicam testes no endereço MAC, nome do host NetBIOS, nome do host DNS e endereço IP na atualização de ativos.

Por padrão, cada parte dos dados de ativo são controlados sobre um período de duas horas. Se alguma parte dos dados de identificação na atualização do ativo exibir comportamento suspeito duas ou mais vezes em 2 horas, essa parte dos dados será incluída nas listas de bloqueio de ativo. Existe uma lista de bloqueio separada para cada tipo de dados de ativo de identidade que é testada.

Em ambientes de domínio reconhecido, as regras de exclusão de reconciliação de ativo rastreiam o comportamento de dados de ativo separadamente para cada domínio.

As regras de exclusão de reconciliação de ativo testam os cenários a seguir:

Tabela 18. . Respostas de regra para cada cenário testado pelas regras de exclusão de reconciliação de ativo

Cenário	Resposta da regra
Quando um endereço MAC é associado a três ou mais endereços IP diferentes em 2 horas ou menos	Inclua o endereço MAC na lista de bloqueio MAC de domínio de reconciliação de ativo
Quando um nome de host DNS é associado a três ou mais endereços IP diferentes em 2 horas ou menos	Inclua o nome do host DNS na lista negra de DNS de Domínio de reconciliação de ativo
Quando um nome de host NetBIOS é associado a três ou mais endereços IP diferentes em 2 horas ou menos	Inclua o nome do host NetBIOS na lista de bloqueio NetBIOS de Domínio de reconciliação de ativo
Quando um endereço IPv4 é associado a três ou mais endereços MAC diferentes em 2 horas ou menos	Inclua o endereço IP na lista de bloqueio IPv4 de domínio de reconciliação de ativo
Quando um nome de host NetBIOS é associado a três ou mais endereços MAC diferentes em 2 horas ou menos	Inclua o nome do host NetBIOS na lista de bloqueio NetBIOS de Domínio de reconciliação de ativo
Quando um nome de host DNS é associado a três ou mais endereços MAC diferentes em 2 horas ou menos	Inclua o nome do host DNS na lista negra de DNS de Domínio de reconciliação de ativo
Quando um endereço IPv4 é associado a três ou mais nomes de host DNS diferente em 2 horas ou menos	Inclua o endereço IP na lista de bloqueio IPv4 de domínio de reconciliação de ativo
Quando um nome de host NetBIOS é associado a três ou mais nomes de host DNS diferentes em 2 horas ou menos	Inclua o nome do host NetBIOS na lista de bloqueio NetBIOS de Domínio de reconciliação de ativo
Quando um endereço MAC é associado a três ou mais nomes de host DNS diferente em 2 horas ou menos	Inclua o endereço MAC na lista de bloqueio MAC de domínio de reconciliação de ativo
Quando um endereço IPv4 é associado a três ou mais nomes de host NetBIOS diferentes em 2 horas ou menos	Inclua o endereço IP na lista de bloqueio IPv4 de domínio de reconciliação de ativo
Quando um nome de host DNS é associado a três ou mais nomes de host NetBIOS diferentes em 2 horas ou menos	Inclua o nome do host DNS na lista negra de DNS de Domínio de reconciliação de ativo
Quando um endereço MAC é associado a três ou mais nomes de host NetBIOS diferentes em 2 horas ou menos	Inclua o endereço MAC na lista de bloqueio MAC de domínio de reconciliação de ativo

É possível visualizar essas regras na guia **Ofensas**, clicando em **Regras** e, em seguida, selecionando o grupo **exclusão de reconciliação de ativo** na lista suspensa.

Conceitos relacionados:

“Exemplo: Regras de exclusão de ativo que são ajustadas para excluir endereços IP da lista de bloqueio”

É possível excluir endereços IP de estarem incluídos na lista de bloqueio ajustando as regras de exclusão de ativo.

Exemplo: Regras de exclusão de ativo que são ajustadas para excluir endereços IP da lista de bloqueio

É possível excluir endereços IP de estarem incluídos na lista de bloqueio ajustando as regras de exclusão de ativo.

Como administrador de segurança de Rede, gerencie uma rede corporativa que inclua um segmento de rede pública wifi em que os leases de endereço IP geralmente são curtos e frequentes. Os ativos neste segmento da rede tendem a ser transitórios, principalmente blocos de notas e dispositivos portáteis que efetuam login e logout do wifi público frequentemente. Normalmente, um único endereço IP é usado várias vezes por diferentes dispositivos em um curto período.

No restante de sua implementação, você tem uma rede cuidadosamente gerenciada que consiste somente em dispositivos de empresa inventariadas e bem nomeadas. Os leases de endereço IP são muito maiores nessa parte da rede e os endereços IP são acessados somente por autenticação. Nesse segmento de rede, você deve saber imediatamente quando existem quaisquer desvios de crescimento de ativo e você deseja manter as configurações padrão para as regras de exclusão de reconciliação de ativo.

Endereços IP de listagem negra

Nesse ambiente, as regras de exclusão de reconciliação de ativo padrão colocam na lista de bloqueio inadvertidamente a rede inteira em um curto tempo.

Sua equipe de segurança consideram um incômodo as notificações relacionadas ao ativo geradas pelo segmento wifi. Você deseja evitar que o wifi acione quaisquer notificações adicionais de crescimento de ativo de desvio.

Ajustando as regras de reconciliação de ativo para ignorar algumas atualizações de ativo

Revise o relatório **Desvio de ativo por origem de log** na última notificação do sistema. Determine se os dados incluídos na lista de bloqueio são provenientes do servidor DHCP em seu wifi.

Os valores na coluna **Contagem de evento/fluxo** e a coluna **Ofensas** para a linha correspondente pra a regra **AssetExclusion: Excluir IP por endereço MAC** indicam que seu servidor DHCP de wifi está acionando essa regra.

Inclua um teste nas regras de exclusão de reconciliação de ativo existente para impedir que as regras incluam os dados de wifi na lista de bloqueio.

Aplicar AssetExclusion: Excluir IP por endereço MAC em eventos que são detectados pelo sistema Local e NÃO quando o(s) evento(s) foram detectados por um ou mais MicrosoftDHCP @ microsoft.dhcp.test.com

e NÃO quando algum Domínio for a chave e algum IP de identidade for o valor em qualquer Lista de Desbloqueio IPv4 do domínio de reconciliação de ativo - Lista de bloqueio IPv4 de domínio de reconciliação de ativo de IP - IP e quando, pelo menos, 3 eventos forem vistos com o mesmo IP de identidade e diferente MAC de identidade em 2 horas.

A regra atualizada testa somente os eventos das origens de log que não estão em seu servidor DHCP de wifi. Para evitar que eventos DHCP de wifi passem por testes de análise de comportamento e conjunto de referência mais onerosos, você também moveu esse teste para a parte superior da pilha de teste

Exemplo: Como os erros de configuração para extensões de origem de log podem causar desvios de crescimento de ativo

Extensões de origem de log customizadas que são incorretamente configuradas podem causar desvios de crescimento de ativo.

Configure uma extensão de origem de log customizada para fornecer atualizações de ativo para QRadar analisando nomes de usuário da carga útil de eventos que estão em um servidor de log central. Configure a extensão da origem de log para substituir a propriedade de nome de host de evento de modo que as atualizações de ativos geradas pela origem de log customizada sempre especifiquem o nome de host DNS do servidor de log central.

Em vez de o QRadar receber uma atualização que tenha o nome do host do ativo no qual o usuário efetuou login, a origem de log gera várias atualizações de ativo que possuem o mesmo nome de host.

Nessa situação, o desvio de crescimento de ativo é causado por um perfil de ativo que contém vários endereços IP e nomes de usuário.

Capítulo 6. Gerenciamento de gráfico

É possível usar várias opções de 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 quais dados deseja criar um gráfico. 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 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.
- Séries temporais – 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 deve remover a extensão do navegador bloqueador 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 no decorrer do tempo.

Picos e vales que são exibidos nos gráficos representam atividade de volume alta e baixa. Gráficos de série temporais são úteis para tendência de dados a curto e longo prazo.

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

Nota: Deve-se ter permissões de função apropriadas para gerenciar e visualizar gráficos de série temporal.

Para exibir gráficos de série temporal, é necessário criar e salvar uma procura que inclui séries temporais e opções de agrupamento. É possível salvar até 100 procuras de série temporal.

Procuras salvas de série temporal padrão são acessíveis a partir da lista de procuras disponíveis na página de procura de eventos.

É possível identificar facilmente as procuras de série temporal salvas no menu **Procuras rápidas**, pois o nome de procura está anexado ao intervalo de tempo especificado nos critérios de procura.

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

É possível ampliar e verificar 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 19. Funções dos gráficos de séries temporais

Função	Descrição
Exibir dados com mais detalhes	<p>Usando o recurso de zoom, é possível investigar segmentos de tempo menores do tráfego de evento.</p> <ul style="list-style-type: none">• Mova o ponteiro do mouse sobre o gráfico e use o botão de rolagem do mouse para aumentar o gráfico (role o botão de rolagem do mouse para cima).• Destaque a área do gráfico que deseja ampliar. Ao liberar o botão do mouse, o gráfico exibirá um segmento de tempo menor. Agora é possível clicar e arrastar o gráfico para verificar o gráfico. <p>Ao aumentar o gráfico de série temporal, o gráfico será atualizado para exibir um segmento de tempo menor.</p>

Tabela 19. Funções dos gráficos de séries temporais (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. É possível 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 o botão de roda do mouse para expandir a visualização (role o botão de roda do mouse para baixo).
Verifique o gráfico	Quando tiver ampliado um gráfico de série temporal, será possível clicar e arrastar o gráfico para a esquerda ou para a direita para verificar a linha.

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 de 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 dela, se desejar remover a legenda da sua exibição de gráfico.

Configurando gráficos

É possível 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 eventos no modo 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 das 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 evento 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 deseja ativar a captura de dados das séries temporais. Ao selecionar essa caixa de seleção, o recurso de gráfico começará a acumular dados para os gráficos de séries temporais. Por padrão, esta opção está desativada. Essa opção está apenas disponível em gráficos Séries Temporais.
Intervalo de tempo	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 do 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 7. 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, será possível salvar o critério de procura e os resultados da procura.

Procurando por itens que correspondem aos seus critérios

É possível procurar por dados que correspondem ao seu critério de procura.

Sobre Esta Tarefa

Como o banco de dados inteiro é procurado, as procuras podem demorar muito tempo, dependendo do tamanho do seu banco de dados.

É possível usar o parâmetro de procura **Quick Filter** para procurar por itens que correspondem à sua sequência de caracteres de texto na carga útil do evento.

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

Tabela 20. Opções da pesquisa

Opções	Descrição
Grupo	Selecione um grupo de pesquisa do evento para visualizar na lista Procuras salvas disponíveis .
Digitar Procura Salva ou Selecionar a partir da Lista	Digite o nome de uma procura salva ou uma palavra-chave para filtrar a lista de Procuras salvas disponíveis .
Procuras Salvas Disponíveis	Essa lista exibe todas as procuras disponíveis, a menos que você use as opções Procura salva de tipo ou grupo ou Selecionar a partir da lista para aplicar um filtro na lista. É possível selecionar uma procura salva nessa lista para exibir ou editar.
Procura	O ícone Procurar está disponível em várias áreas de janela na página de procura. É possível clicar em Procurar quando você terminar de configurar a procura e desejar visualizar os resultados.
Inclua em Minhas Procuras Rápidas	Selecione essa caixa de seleção para incluir esta procura em seu menu Procura rápida .

Tabela 20. Opções da pesquisa (continuação)

Opções	Descrição
Incluir em Meu Painel	Selecione esta caixa de seleção para incluir os dados da procura salva na guia Painel . Para obter mais informações sobre a guia Painel , consulte Gerenciamento de painel. Nota: Esse parâmetro será exibido somente se a procura for agrupada.
Defina como Padrão	Selecione esta caixa de seleção para configurar essa procura como sua procura padrão.
Compartilhar com Todos	Selecione essa caixa de seleção para compartilhar esta pesquisa 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, você não conseguirá 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 do log atualiza em intervalos de um minuto para exibir as informações mais recentes.
Recente	Selecione um intervalo de tempo predefinido para sua procura. Depois de selecionar essa opção, você deve 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, deve-se selecionar o intervalo de data e hora nos calendários de Horário de início e Horário de encerramento .

Tabela 20. Opções da pesquisa (continuação)

Opções	Descrição
Acumulação de Dados	<p>Esta área de janela será exibida apenas quando você carregar uma procura salva.</p> <p>A ativação de contagens exclusivas em dados acumulados que são compartilhados com muitas outras procuras e relatórios salvos pode diminuir o desempenho do sistema.</p> <p>Quando você carrega uma procura salva, esta área de janela exibe as seguintes opções:</p> <ul style="list-style-type: none"> • Se nenhum dado estiver acumulando para esta procura salva, a mensagem de informação a seguir será exibida: Dados não estão sendo acumulados para esta procura. • Se os dados forem acumulando para esta procura salva, as seguintes opções serão exibidas: <ul style="list-style-type: none"> – colunas – Quando você clica ou passa o mouse sobre esse link, uma lista das colunas que estão acumulando dados é aberta. – Ativar contagens exclusivas/desativar contagens exclusivas – Este link permite que você ative ou desative os resultados da procura para exibir contagens de eventos exclusivos em vez de médias de contagens ao longo do tempo. Depois de clicar no link Ativar contagens exclusivas, uma caixa de diálogo é aberta e indica quais procuras e relatórios salvos compartilham os dados acumulados.
Filtros Atuais	Esta lista exibe os filtros que são aplicados a esta procura. As opções para incluir um filtro estão localizadas acima da lista Filtros atuais .
Salve os resultados quando a procura for concluída	Selecione esta caixa de seleção para salvar e nomear os resultados da procura.
Exibir	Selecione esta lista para especificar uma coluna predefinida que está configurada para exibir nos resultados da procura.
Digitar Coluna ou Selecionar a partir da Lista	<p>É possível usar o campo para filtrar as colunas que são listadas na lista Colunas Disponíveis.</p> <p>Digite o nome da coluna que você deseja localizar ou digite uma palavra-chave para exibir uma lista de nomes de colunas. Por exemplo, digite Dispositivo para exibir uma lista de colunas que incluem Dispositivo no nome da coluna.</p>

Tabela 20. Opções da pesquisa (continuação)

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

Tabela 20. Opções da pesquisa (continuação)

Opções	Descrição
Colunas	<p>Especifica colunas que são escolhidas para a procura. É possível selecionar mais colunas na lista Colunas disponíveis. É possível customizar ainda mais a lista Colunas usando as seguintes opções:</p> <ul style="list-style-type: none"> • Mover para cima – Move a coluna selecionada para cima na lista de prioridades. • Mover para baixo – Move o próprio selecionado 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>
Classificar por	<p>Na primeira caixa de listagem, selecione a coluna pela qual você deseja classificar os resultados da procura. Em seguida, a partir da segunda caixa de listagem, selecione a ordem que você deseja exibir para os resultados de procura. As opções incluem Decrescente e Crescente.</p>
Limite de Resultados	<p>É possível especificar o número de linhas que uma pesquisa retorna na janela Editar Procura. O campo Limitar resultados também aparece na janela Resultados.</p> <ul style="list-style-type: none"> • Para uma procura salva, o limite será armazenado na procura salva e reaplicado no carregamento da procura. • Ao classificar em uma coluna no resultado de procura que tem limite de linha, a classificação será feita dentro das linhas limitadas mostradas na grade de dados. • Para obter um agrupado por procura com gráfico de série temporal ligado, o limite da linha somente se aplica à grade de dados. O suspenso Parte superior no gráfico de série temporal ainda controla quantas séries de tempo 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 seguintes opções: A partir da lista de Procuras Salvas Disponíveis, selecione a procura salva que você deseja carregar. No

- campo Digitar a procura salva ou Selecionar na lista, digite o nome da procura que você 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 do Intervalo de Tempo, selecione as opções para o intervalo de tempo que você deseja capturar para essa procura.
 5. Opcional. Na área de janela de Acumulação de Dados, ative 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 conta exclusiva, 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 a d para cada filtro que você deseja incluir nos critérios de procura.
 7. Opcional. Para salvar automaticamente os resultados da procura quando a procura for concluída, selecione a caixa de seleção **Salvar resultados quando a procura for concluída** e, em seguida, digite um nome para a procura salva.
 8. Na área de janela Definição de Coluna, defina o layout de colunas e colunas que você deseja usar para visualizar os resultados:
 - a. Na caixa de listagem **Exibir**, selecione a coluna pré-configurada que está configurada para associar com essa pesquisa.
 - b. Clique na seta ao lado de **Definição de visualização avançada** para exibir os parâmetros de procura avançada.
 - c. Customize as colunas a serem exibidas nos resultados da procura. Consulte a Tabela 1.
 - d. Opcional. No campo **Limite de resultados**, digite o número de linhas que você deseja que a procura retorne.
 9. Clique em **Filtrar**.

Resultados

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

.

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

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

Conceitos relacionados:

“Opções de procura avançada” na página 75

Use o campo **Procura avançada** para inserir uma Ariel Query Language (AQL) que especifique os campos que você deseja e como você deseja agrupá-los para executar uma consulta.

“Exemplos de sequência de caracteres de procura AQL” na página 77

Use a Ariel Query Language (AQL) para recuperar campos específicos dos eventos, dos fluxos e das tabelas simarc no banco de dados do Ariel.

Salvando critérios de procura

É possível 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.
Gerenciar Grupos	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.
Incluir em minhas procuras rápidas	Selecione essa caixa de seleção para incluir essa procura na caixa de listagem Procura rápida na barra de ferramentas.
Include in my Dashboard	Selecione esta caixa de seleção para incluir os dados da procura salva na guia Painel . Para obter mais informações sobre a guia Painel , consulte Gerenciamento de painel. Nota: Esse parâmetro será exibido somente se a procura for agrupada.
Configurar como Padrão	
Compartilhar com Todos	Selecione essa caixa de seleção para compartilhar esses requisitos de procura com todos os usuários.

5. Clique em **OK**.

Procura planejada

Use a opção Procura planejada para planejar uma procura e visualizar os resultados.

É possível planejar uma procura que seja executada em um horário específico do dia ou da noite.

Exemplo:

Se você planejar uma procura para ser executada na noite, poderá investigar de manhã. Ao contrário dos relatórios, você tem a opção de agrupar os resultados da procura e investigar ainda mais. É possível procurar pelo número de logins com falha no grupo de rede. Se o resultado for geralmente 10 e o resultado da procura for 100, é possível agrupar os resultados da procura para facilitar a investigação. Para ver qual usuário possui mais logins com falha, é possível agrupar pelo nome de usuário. É possível aprofundar a investigação.

É possível planejar uma procura nos eventos ou nos fluxos na guia **Relatórios**. Deve-se selecionar um conjunto de critérios de procura salvo anteriormente para planejamento.

1. Criar um relatório

Especifique as informações a seguir na janela **Assistente de relatório**:

- O tipo de gráfico é Eventos/Logs ou Fluxos.
- O relatório baseia-se em uma procura salva.
- Gerar uma ofensa.

É possível escolher a opção **criar uma ofensa individual** ou a opção **incluir resultado em uma ofensa existente**.

Também é possível gerar uma procura manual.

2. Visualizar resultados da procura

É possível visualizar os resultados da procura planejada na guia **Ofensas**.

- As ofensas da procura planejada são identificadas pela coluna **Tipo de ofensa**. Se você criar uma ofensa individual, será gerada uma ofensa sempre que o relatório for executado. Se incluir o resultado da procura salva em uma ofensa existente, será criada uma ofensa na primeira vez que o relatório for executado. O relatório subsequente é executado anexado a essa ofensa. Se nenhum resultado for retornado, o sistema não anexará ou criará uma ofensa.
- Para visualizar o resultado da procura mais recente na janela Sumarização de ofensas, dê um clique duplo em uma ofensa da procura planejada na lista de ofensas. Para visualizar a lista de todas as execuções de procura planejada, clique em **Resultados da procura** na área de janela **Últimos cinco resultados da procura**.

É possível designar uma ofensa da Procura planejada a um usuário.

Conceitos relacionados:

“Opções de procura avançada”

Use o campo **Procura avançada** para inserir uma Ariel Query Language (AQL) que especifique os campos que você deseja e como você deseja agrupá-los para executar uma consulta.

“Exemplos de sequência de caracteres de procura AQL” na página 77

Use a Ariel Query Language (AQL) para recuperar campos específicos dos eventos, dos fluxos e das tabelas simarc no banco de dados do Ariel.

Opções de procura avançada

Use o campo **Procura avançada** para inserir uma Ariel Query Language (AQL) que especifique os campos que você deseja e como você deseja agrupá-los para executar uma consulta.

O campo **Procura avançada** tem conclusão automática e destaque da sintaxe.

Use a conclusão automática e o destaque da sintaxe para ajudar a criar consultas. Para obter informações sobre os navegadores da web suportados, consulte “Navegadores da Web Suportados” na página 3

Acessando a procura avançada

Acesse a opção **Procura avançada** na barra de ferramentas **Procurar** que está na guia **Atividade de log** para digitar uma consulta AQL.

Selecione **Procura avançada** na caixa de listagem na barra de ferramentas **Procurar**.

Expanda o campo **Procura avançada** seguindo estas etapas:

1. Arraste o ícone de expansão que está à direita do campo.

2. Pressione Shift + Enter para acessar a próxima linha.
3. Pressione Enter.

É possível clicar com o botão direito em qualquer valor no resultado da procura e filtrar por esse valor.

Dê um clique duplo em qualquer linha no resultado da procura para ver mais detalhes.

Todas as procuras, incluindo procuras AQL, são incluídas no log de auditoria.

Exemplos de sequência de caracteres de procura AQL

A tabela a seguir fornece exemplos de sequências de caracteres de procura AQL.

Tabela 21. Exemplos de sequências de caracteres de procura AQL

Descrição	Exemplo
Selecione colunas padrão de eventos.	SELECT * FROM events
Selecione colunas específicas.	SELECT sourceip, destinationip FROM events
Selecione colunas específicas e ordene os resultados.	SELECT sourceip, destinationip FROM events ORDER BY destinationip
Execute uma consulta de procura agregada.	SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip
Execute uma chamada de função em uma cláusula SELECT.	SELECT CATEGORYNAME(category) AS namedCategory FROM events
Filtre os resultados da procura usando uma cláusula WHERE.	SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1
Procure eventos que acionaram uma regra específica, a qual é baseada no nome da regra ou no texto parcial no nome da regra.	SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'
Referencie nomes do campo que contenham caracteres especiais, como caracteres aritméticos ou espaços, colocando o nome do campo entre aspas duplas.	SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'

Para obter informações adicionais sobre funções, campos de procura e operadores, consulte o *Guia de Idioma de Consulta Ariel*.

Conceitos relacionados:

“Procura planejada” na página 74

Use a opção Procura planejada para planejar uma procura e visualizar os resultados.

“Opções de procura de filtro rápido” na página 80

Procure cargas úteis de fluxos e de evento digitando uma sequência de caracteres de procura de texto que use palavras ou frases simples.

Tarefas relacionadas:

“Procurando por itens que correspondem aos seus critérios” na página 67

É possível procurar por dados que correspondem ao seu critério de procura.

Exemplos de sequência de caracteres de procura AQL

Use a Ariel Query Language (AQL) para recuperar campos específicos dos eventos, dos fluxos e das tabelas simarc no banco de dados do Ariel.

Relatando o uso da conta

Comunidades de usuário diferentes podem ter indicadores de uso e de ameaça diferentes.

Use os dados de referência para relatar várias propriedades de usuário, por exemplo, departamento, local ou gerente.

É possível usar dados de referência externa.

A consulta a seguir retorna informações de metadados sobre o usuário de seus eventos de login.

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

Insight em vários identificadores de conta

Nesse exemplo, usuários individuais possuem várias contas na rede. A organização requer uma única visualização de uma atividade de usuários.

Use os dados de referência para mapear IDs do usuário local para um ID global.

A consulta a seguir retorna as contas do usuário usadas por um ID global em eventos sinalizados como suspeitos.

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

A consulta a seguir mostra as atividades concluídas por um ID global.

```
SELECT
QIDNAME(qid) as 'Event name',
starttime as Time,
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event Username',
REFERENCEMAP('GlobalID Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

Identificar indicadores suspeitos de longo prazo

Muitas ameaças usam comando e controle para se comunicarem periodicamente por dias, semanas e meses.

Procuras avançadas podem identificar padrões de conexão com o passar do tempo. Por exemplo, é possível consultar um volume consistente, curto e baixo, o número de conexões por dia/semana/mês entre endereços IP ou um endereço IP e uma localização geográfica.

Use a API REST do IBM Security QRadar para gerar uma ofensa ou para preencher um conjunto de referência ou uma tabela de referência.

A consulta a seguir detecta indicadores diários para um domínio usando eventos de log de proxy. Os tempos dos indicadores não ficam no mesmo horário todos os dias. O lapso de tempo entre os indicadores é curto.

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and 'total events' < 10
LAST 7 days
```

A propriedade `url_domain` é uma propriedade customizada dos logs de proxy.

Inteligência de ameaça externa

Os dados de uso e de segurança correlacionados aos dados de inteligência de ameaça externa podem fornecer indicadores de ameaça importantes.

Procuras avançadas podem fazer uma referência cruzada de indicadores de inteligência de ameaça externa com outros eventos de segurança e dados de uso.

Essa consulta mostra como é possível criar um perfil dos dados de ameaça externa por muitos dias, semanas ou meses para identificar e priorizar o nível de risco de ativos e contas.

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

Inteligência e configuração de ativo

Os indicadores de uso e ameaça variam por tipo de ativo, sistema operacional, variação de vulnerabilidade, classificação e outros parâmetros.

Nessa consulta, as procuras avançadas e o modelo de ativo fornecem insight operacional para um local.

A função **Assetproperty** recupera valores de propriedade dos ativos, os quais permitem que você inclua dados de ativo nos resultados.

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

A função **AssetUser** recupera o nome de usuário do banco de dados de ativo.

Função Network LOOKUP

É possível usar a função **Network LOOKUP** para recuperar o nome da rede que está associado a um endereço IP.

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

Função Rule LOOKUP

É possível usar a função **Rule LOOKUP** para recuperar o nome de uma regra por seu ID.

```
SELECT RULENAME(123) FROM events
```

A consulta a seguir retorna eventos que acionaram um nome da regra específico.

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

TEXT SEARCH Completa

É possível usar o operador TEXT SEARCH para executar procuras de texto completas usando a opção **Procura avançada**.

Nesse exemplo, há uma série de eventos que contêm a palavra "firewall" na carga útil. É possível procurar esses eventos usando a opção **Filtro rápido** e a opção **Procura avançada** na guia **Atividade de log**.

- Para usar a opção **Filtro rápido**, digite o texto a seguir na caixa **Filtro rápido**:
'firewall'
- Para usar a opção **Procura avançada**, digite a consulta a seguir na caixa **Procura avançada**:

```
SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
```

Propriedade customizada

É possível acessar propriedades customizadas para eventos e fluxos quando você usar a opção **Procura avançada**.

A consulta a seguir usa a propriedade customizada "MyWebsiteUrl" para classificar eventos por uma determinada URL da web:

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

Conceitos relacionados:

"Procura planejada" na página 74

Use a opção Procura planejada para planejar uma procura e visualizar os resultados.

“Opções de procura de filtro rápido”

Procure cargas úteis de fluxos e de evento digitando uma sequência de caracteres de procura de texto que use palavras ou frases simples.

Tarefas relacionadas:

“Procurando por itens que correspondem aos seus critérios” na página 67

É possível procurar por dados que correspondem ao seu critério de procura.

Opções de procura de filtro rápido

Procure cargas úteis de fluxos e de evento digitando uma sequência de caracteres de procura de texto que use palavras ou frases simples.

É possível filtrar suas procuras a partir destes locais:

Barras de ferramentas Atividade de log e

Selecione **Filtro rápido** na caixa de listagem na barra de ferramentas

Procurar para digitar uma sequência de caracteres de procura de texto.

Clique no ícone **Filtro rápido** para aplicar seu à lista de eventos ou fluxos.

Caixa de diálogo Incluir filtro

Clique no ícone **Incluir filtro** na guia **Atividade de log** ou .

Selecione **Filtro rápido** como seu parâmetro de filtro e digite uma sequência de caracteres de procura de texto.

Páginas de procura de fluxo

Inclua um filtro rápido na lista de filtros.

Ao visualizar no último modo de intervalo ou no modo de intervalo em tempo real (fluxo), é possível digitar somente palavras ou frases simples no campo **Filtro rápido**. Ao visualizar **eventos** ou em um intervalo de tempo, siga essas diretrizes de sintaxe:

Tabela 22. Diretrizes de sintaxe de filtro rápido.

Descrição	Exemplo
Inclua qualquer texto simples que você espera localizar na carga útil.	Firewall
Procure frases exatas incluindo vários termos entre aspas duplas.	"Negação de firewall"
Inclua curingas de caracteres únicos e múltiplos. O termo de procura não pode começar com um curinga.	F?rwall ou F??ew*
Agrupe termos com expressões lógicas, como AND, OR e NOT. Para serem reconhecidas como expressões lógicas e não como termos de procura, a sintaxe e os operadores devem estar em maiúscula.	(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)
Ao criar critérios de procura que incluem a expressão lógica NOT, deve-se incluir pelo menos um outro tipo de expressão lógica, caso contrário, nenhum resultado será retornado.	(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)
Preceda os seguintes caracteres por uma barra invertida para indicar que o caractere faz parte do termo de pesquisa: + - && ! () {} [] ^ " ~ * ? : \.	"%PIX\ -5\ -304001"

Os termos de procura são combinados em sequência a partir do primeiro caractere na palavra ou frase da carga útil. O usuário do termo de procura corresponde ao user_1 e user_2, mas não corresponde às frases a seguir: ruser, myuser ou anyuser.

Procuras de filtro rápido usam o código de idioma em inglês. *Código de idioma* é uma configuração que identifica o idioma ou a geografia e determina convenções de formatação como ordenação, conversão de caso, classificação de caractere, o idioma de mensagens, a representação de data e hora e a representação numérica.

O código de idioma é configurado pelo seu sistema operacional. É possível configurar o QRadar para substituir a configuração do código de idioma do sistema operacional. Por exemplo, é possível configurar o código de idioma para **inglês** e o Console do QRadar pode ser configurado para **Italiano (Italian)**.

Se você usar caracteres Unicode em sua Consulta de procura de filtro rápido, resultados da procura inesperados podem ser retornados.

Se você escolher um código de idioma que não está em inglês, é possível usar a opção Procura avançada no QRadar para procurar evento e dados de carga útil.

Conceitos relacionados:

“Opções de procura avançada” na página 75

Use o campo **Procura avançada** para inserir uma Ariel Query Language (AQL) que especifique os campos que você deseja e como você deseja agrupá-los para executar uma consulta.

“Exemplos de sequência de caracteres de procura AQL” na página 77

Use a Ariel Query Language (AQL) para recuperar campos específicos dos eventos, dos fluxos e das tabelas simarc no banco de dados do Ariel.

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 pra refinar resultados da procura sem procurar o 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 de base. A área de janela Filtro do Current especifica os filtros aplicados na subprocura. É possível 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 nos critérios de subprocura salva, você ainda terá o acesso aos critérios de subprocura salva. 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.

Excluindo critérios de procura

É possível 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.

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 23. Parâmetros da página gerenciar resultados da procura

Parâmetro	Descrição
Sinalizadores	Indica que uma notificação de email ficará pendente para quando a procura for concluída.
User	Especifica o nome do usuário que iniciou a procura.

Tabela 23. Parâmetros da página gerenciar resultados da procura (continuação)

Parâmetro	Descrição
Name	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 24. 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 está na fila ou em andamento, é possível 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 necessário, será possível excluí-lo 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 da procura que 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 ofensas.

Esses grupos permitem que sejam localizados facilmente 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

É possível visualizar grupos de procura na janela Grupo de procura de eventos.

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

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

Tabela 25. Parâmetros da janela de grupo de procura

Parâmetro	Descrição
Name	Especifica o nome do grupo de procura.
User	Especifica o nome de usuário que criou o grupo de procura.
Descrição	Especifica a descrição do grupo de procura.
Date Modified	Especifica a data que o grupo de procura foi modificado.

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

Tabela 26. Funções da janela barra de ferramentas do grupo de procura

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

Tabela 26. Funções da janela barra de ferramentas do grupo de procura (continuação)

Função	Descrição
Copiar	Para copiar uma procura salva em 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 você deseja remover e 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

É possível 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

É possível 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**.
 - Digite uma nova descrição no campo **Descrição**.
7. Clique em **OK**.

Copiando uma procura salva em outro grupo

É possível 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 item, selecione a caixa de seleção para o grupo que você deseja copiar a procura salva.
7. Clique em **Designar grupos**.

Removendo um grupo ou uma procura salva de um grupo

É possível 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, a procura salva não será excluída do sistema. A procura salva é removida do grupo e automaticamente movida para o grupo **Outros**.

Não é possível remover Grupos de Procura de Eventos do seu 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 **Remove**.
6. Clique em **OK**.

Capítulo 8. 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. É possível copiar e colar as informações de 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 mais informações, consulte 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 os 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 27. 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.
Origem 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 27. 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 28. 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 28. 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

É possível modificar uma propriedade customizada.

Sobre Esta Tarefa

É possível usar a janela Propriedades de evento customizado para modificar uma propriedade customizada.

As propriedades customizadas são descritas na tabela a seguir.

Tabela 29. 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.
Fonte 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 30. 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

É possível 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 9. Gerenciamento de regra

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

Este tópico se aplica a usuários que têm 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 outras regras. Não será necessário criar regras em nenhuma ordem específica porque o sistema irá verificar as dependências cada vez que uma nova regra for incluída, editada ou excluída. Se uma regra que é 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.

Nota: Os blocos de construção não são carregados por padrão. Defina uma regra para construir blocos de construção.

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

Regras específicas do domínio

Se uma regra tiver um teste de domínio, é possível restringir essa regra de modo que seja aplicada apenas a eventos que estejam acontecendo no domínio especificado. Um evento que tem uma marcação de domínio diferente do domínio definido na regra não acionará uma resposta do evento.

Para criar uma regra que teste condições sobre eventos que estão ocorrendo em todo o sistema, configure a condição de domínio como **Qualquer domínio**.

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.
- Inclua 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

É possível 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 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. É possível revisar e editar detalhes da regra.

Criando uma regra customizada

É possível 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**.

É possível 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. É possível 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 110
12. Clique em **Avançar**.
13. Revise a regra configurada. Clique em **Concluir**.

Tarefas de gerenciamento de regra

É possível 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

É possível 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

É possível 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

É possível 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 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 deseje 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

É possível 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 deseje 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

É possível 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

É possível 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 customizada.
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 31. 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 customizada e Regra de detecção de anomalias.

Tabela 31. Parâmetros da página Regras (continuação)

Parâmetro	Descrição
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.
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 32. 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 32. 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 33. 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 33. 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. Nota: Para alterar a configuração Código de idioma do email , selecione Configurações do sistema na guia Administrador .
Insira o endereço de email a ser notificado	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	Esse parâmetro só será exibido quando os parâmetros SNMP Settings forem definidos nas configurações do sistema. Selecione esta caixa de seleção para ativar que esta regra envie uma notificação SNMP (trap). A saída de trap SNMP inclui o tempo do sistema, o OID de trap e os dados de notificação, conforme definidos pelo MIB.
Enviar para syslog local	Selecione essa caixa de seleção se desejar registrar o evento localmente. Por padrão, essa caixa de seleção está limpa. 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.
Enviar para Destinos de Encaminhamento	Esta caixa de seleção será exibida apenas para regras de eventos. 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. Para incluir, editar ou excluir um destino de encaminhamento, clique no link Gerenciar destinos .
Notify	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. Se ativar notificações, configure o parâmetro Response Limiter .

Tabela 33. 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 33. 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 10. Perfis de ativos

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 propósitos de correlação para ajudar a reduzir positivos falsos. Por exemplo, se uma origem tentar explorar um serviço específico em execução em um ativo, o QRadar determinará se o ativo está vulnerável a este ataque correlacionando o ataque ao perfil de ativo.

Perfis de ativos são descobertos automaticamente se tiver varreduras de avaliação de vulnerabilidades (VA) configuradas.

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 exclusivo (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 Vulnerabilidade Comum e Exposições (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*.

O QRadar Vulnerability Manager é um componente que pode ser comprado separadamente e ativado usando uma chave de licença. O QRadar Vulnerability Manager é uma plataforma de varredura de rede que fornece reconhecimento de vulnerabilidades que existem em aplicativos, sistemas ou dispositivos em sua rede. Após varreduras identificarem vulnerabilidades, será possível procurar e revisar dados de vulnerabilidade, corrigir vulnerabilidades e executar varreduras novamente para avaliar o novo nível de risco.

Quando QRadar Vulnerability Manager for ativado, será possível 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 uma área de trabalho a partir da qual é possível gerenciar seus ativos de rede e investigar as vulnerabilidades, portas, aplicativos, histórico e outras associações de um ativo.

Usando a guia **Ativos**, é possível:

- Visualizar todos os ativos descobertos.

- Incluir manualmente os perfis de ativos.
- Procurar ativos específicos.
- Visualizar informações sobre ativos descobertos.
- Editar os perfis de ativos para ativos manualmente incluídos ou descobertos.
- Ajustar vulnerabilidades de positivo falso.
- Importar ativos.
- Imprimir ou exportar perfis de ativo.
- Descobrir os ativos.
- Configurar e gerenciar varreduras de vulnerabilidade de terceiros.
- Iniciar as varreduras do Gerenciador de Vulnerabilidade do QRadar.

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

Lista da guia Ativo

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

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

Tabela 34. Parâmetros da página Perfil de ativo

Parâmetro	Descrição
ID	Exibe o número do ID de ativo do ativo. O número do ID de recurso é automaticamente gerado ao incluir um perfil de ativo manualmente ou quando os recursos forem descobertos pelas varreduras de eventos ou vulnerabilidade.
IP Address	Exibe o último endereço IP conhecido do ativo.
Asset Name	Exibe o nome fornecido, nome NetBios, nome DSN ou 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 NetBios agregado será exibido. Se o ativo for descoberto automaticamente, esse campo será preenchido automaticamente, no entanto, é possível editar o nome do ativo, se necessário.

Tabela 34. Parâmetros da página Perfil de ativo (continuação)

Parâmetro	Descrição
Risk Score	<p>Exibe uma das seguintes pontuações do Sistema de Pontuação de Vulnerabilidade Comum (CVSS):</p> <ul style="list-style-type: none"> • Pontuação do CVSS ambiental agregada unida • Agregar pontuação do CVSS temporal • Agregar pontuação base do CVSS • <p>Essas pontuações são exibidas na ordem de prioridade. Por exemplo, se a pontuação do CVSS ambiental agregada unida não estiver disponível, a pontuação do CVSS temporal agregada será exibida.</p> <p>Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras.</p> <p>A contagem do CVSS é calculada a partir dos seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> • Potencial de Danos Colaterais • Requisito de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade <p>Para obter mais informações sobre como configurar estes parâmetros, consulte “Incluindo ou editando um perfil de ativo” na página 122.</p> <p>Para obter mais informações sobre o 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 pela última vez.

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 35. Funções da barra de ferramentas da página de Perfis de Ativos

Função	Descrição
Procura	<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>Nesta caixa de listagem, é possível executar procuras salvas anteriormente. As opções serão exibidas na caixa de listagem Procuras rápidas apenas quando tiverem sido salvos os critérios de procura 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 122.</p>

Tabela 35. 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 menus 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 36. 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 DNS que são baseadas no endereço IP. • Consulta WHOIS - Procura o proprietário registrado de um endereço IP remoto. O servidor de WHOIS padrão é whois.arin.net. • Varredura de porta – Executa uma varredura do Mapeador de Rede (NMAP) do endereço IP selecionado. Essa opção estará disponível somente 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 de Vulnerabilidade	<p>Selecione esta opção para executar uma varredura do Gerenciador de Vulnerabilidades no ativo selecionado.</p> <p>Essa opção será exibida somente após o QRadar Vulnerability Manager estar instalado.</p>

Visualizando um perfil de ativos

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

Sobre Esta Tarefa

Informações do perfil de ativo são descobertas automaticamente por meio do Server Discovery ou configuradas manualmente. É possível editar informações de perfil de ativo geradas automaticamente.

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

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

Tabela 37. Funções da barra de ferramentas da página Perfil de Ativo

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 você deseja visualizar na área de janela de Perfil de Ativo. As áreas de janela Resumo de Ativo e Resumo de Interface de Rede são sempre exibidas.</p> <p>Para obter mais informações sobre os parâmetros que são exibidos em cada área de janela, consulte Ativos página parâmetros de perfil.</p>
Editar ativo	Clique nesta opção para editar o Perfil de Ativo. Consulte “Incluindo ou editando um perfil de ativo” na página 122.
Visualizar resumo de destino	Se este ativo for o destino de um crime, essa opção permitirá que você visualize informações de resumo de destino.
Histórico	<p>Clique em Histórico para visualizar informações do histórico de eventos para este ativo. Quando você clica no ícone Histórico, a janela Procura de eventos é exibida, pré-preenchida com critérios de procura de eventos:</p> <p>É possível customizar os parâmetros de procura, se necessário. Clique em Procurar para visualizar as informações do histórico de eventos.</p>
Aplicativos	<p>Clique em Aplicativos para visualizar informações do aplicativo para este ativo. Quando você clica no ícone Aplicativos, a janela Procura de Fluxo é exibida, pré-preenchida com critérios de procura do evento.</p> <p>É possível customizar os parâmetros de procura, se necessário. Clique em Procurar para visualizar as informações do aplicativo.</p>
Conexões de procura	<p>Clique em Conexões de procura para procurar por conexões. A janela Procura de conexão é exibida.</p> <p>Essa opção será exibida apenas quando o IBM Security QRadar Risk Manager estiver sendo comprado e licenciado. Para obter mais informações, consulte <i>Guia do Usuário do IBM Security QRadar Risk Manager</i>.</p>
Visualizar Topologia	Essa opção será exibida apenas quando o IBM Security QRadar Risk Manager estiver sendo comprado e licenciado. Para obter mais informações, consulte <i>Guia do Usuário do IBM Security QRadar Risk Manager</i> .
Ações	<p>Na lista Ações, selecione Histórico de vulnerabilidade.</p> <p>Essa opção será exibida apenas quando o IBM Security QRadar Risk Manager estiver sendo comprado e licenciado. Para obter mais informações, consulte <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 várias áreas de janela de informação do perfil de ativos. Consulte Editando um perfil de ativo.
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 ativo. Consulte Editando um perfil de ativo.
7. Clique em **Retornar para Lista de Ativos** para selecionar e visualizar outro ativo, se necessário.

Incluindo ou editando um perfil de ativo

Perfis de ativos são descobertos e incluídos automaticamente; no entanto, talvez seja necessário que você inclua um perfil manualmente

Sobre Esta Tarefa

Quando ativos são descobertos usando a opção de Descoberta do Servidor, alguns detalhes do perfil de ativos são preenchidos automaticamente. É possível incluir manualmente as informações para o perfil do ativo e você pode editar determinados parâmetros.

Você só pode editar os parâmetros que foram inseridos manualmente. Os parâmetros que foram gerados pelo sistema são exibidos em itálico e não são editáveis. É possível 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 digite o endereço IP ou intervalo do CIDR do ativo no campo **Novo endereço IP**.
 - Para editar um ativo, clique duas vezes no ativo que você deseja visualizar e clique em **Editar ativo**.
4. Configure os parâmetros na área de janela do Endereço IP & do MAC. Configure uma ou mais das seguintes opções:
 - Clique no ícone **Novo endereço MAC** e digite um Endereço MAC na caixa de diálogo.
 - Clique no ícone **Novo endereço IP** e digite um endereço IP na caixa de diálogo.
 - Se **NIC desconhecido** estiver listado, você poderá selecionar esse item, clicar no ícone **Editar** e digitar um novo endereço MAC na caixa de diálogo.
 - Selecione um endereço MAC ou IP da lista, clique no ícone **Editar** e digite um novo endereço MAC na caixa de diálogo.
 - Selecione um endereço MAC ou IP na lista e clique no ícone **Remover**.
5. Configure os parâmetros na área de janela Descrição de & Nomes. Configure uma ou mais das seguintes opções:

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

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 ativo.
 - 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 seguintes opções:
 - **Até a próxima varredura** – Selecione esta opção para especificar que o scanner fornece informações do sistema operacional e as informações podem ser temporariamente editadas. Se você editar os parâmetros do sistema operacional, o scanner irá restaurar as informações em sua próxima varredura.
 - **Para sempre** – Selecione esta 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 & de Peso. Configure uma ou mais das seguintes opções:

Parâmetro	Descrição
Potencial de Danos Colaterais	<p>Configure esse parâmetro para indicar o potencial de perda de vida ou ativos físicos por dano ou furto desse ativo. Você também pode usar esse parâmetro para indicar um potencial de perda econômica de produtividade ou receita. O potencial de dano colateral aumentado aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem Potencial de danos colaterais, selecione uma das seguintes opções:</p> <ul style="list-style-type: none"> • Nenhum • Baixo • Média baixa • Média alta • Alto • Não definido <p>Ao configurar o parâmetro Collateral Damage Potential, o parâmetro Weight será atualizado automaticamente.</p>
Requisito de Confidencialidade	<p>Configure esse parâmetro para indicar o impacto sobre a confidencialidade de uma vulnerabilidade explorada com êxito neste ativo. O impacto de confidencialidade aumentada aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem Requisito de confidencialidade, selecione uma das seguintes opções:</p> <ul style="list-style-type: none"> • Baixo • Médio • Alto • Não definido

Parâmetro	Descrição
Requisito de Disponibilidade	<p>Configure esse parâmetro para indicar o impacto para disponibilidade do ativo quando uma vulnerabilidade é explorada com êxito. Ataques que consomem a largura da banda da rede, ciclos do processador ou espaço em disco impactará na disponibilidade de um ativo. O impacto de disponibilidade aumentada aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem Requisito de disponibilidade, selecione uma das seguintes opções:</p> <ul style="list-style-type: none"> • Baixo • Médio • Alto • Não definido
Requisito de Integridade	<p>Configure esse parâmetro para indicar o impacto para a integridade do ativo quando uma vulnerabilidade é explorada com êxito. Integridade refere-se à fidelidade e a veracidade garantida de informações. O impacto de integridade aumentada aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem Requisito de integridade, selecione uma das seguintes opções:</p> <ul style="list-style-type: none"> • Baixo • Médio • Alto • Não definido
Peso	<p>Na caixa de listagem Peso, selecione um peso para este perfil de ativo. O intervalo é de 0 – 10.</p> <p>Ao configurar o parâmetro de Weight, o parâmetro de Collateral Damage Potential é atualizado automaticamente.</p>

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

Parâmetro	Descrição
Business Owner	digitar o nome do proprietário de negócios do ativo. Um exemplo de um proprietário de negócios é um gerente de departamento. O comprimento máximo é de 255 caracteres.
Business Owner Contact	Digite as informações de contato para o proprietário de negócios. O comprimento máximo é de 255 caracteres.

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

9. Clique em **Salvar**.

Procurando perfis de ativos

É possível 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 ativo. Consulte Grupos de procura de ativo.

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 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

É possível salvar seu critério de procura de ativo. Consulte Salvando critério de procura de ativo.

Salvando critérios de procura de ativos

Na guia **Ativos**, você pode salvar o critério de procura configurado 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 ativo.
4. Clique em **Salvar critérios**.
5. Insira os valores para os parâmetros:

Parâmetro	Descrição
Insira o nome desta procura	Digite o nome exclusivo que deseja designar a esses critérios de procura.
Gerenciar Grupos	Clique em Gerenciar grupos para gerenciar os grupos de procura. Para obter mais informações, consulte Grupos de procura de ativo. Essa opção será exibida somente se você tiver permissões administrativas.
Designar procura aos grupos	Selecione a caixa de seleção para o grupo que você deseja designar a essa procura salva. Se você não selecionar um grupo, esta procura salva será designada ao grupo Outro por padrão. Para obter mais informações, consulte Grupos de procura de ativo.
Incluir em minhas procuras rápidas	Selecione essa caixa de seleção para incluir essa procura em sua caixa de listagem Procura rápida , que está na barra de ferramentas da guia Ativos .
Configurar como Padrão	Selecione esta caixa de seleção para configurar esta procura como sua procura padrão quando você acessar a guia Recursos .
Compartilhar com todos	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, é possível criar e gerenciar grupos de procura de ativos.

Esses grupos permitem localizar facilmente critérios de procura salvos na guia **Ativos**.

Visualizando grupos de procura

Use a janela Grupos de Procura de Ativo para visualizar um grupo e subgrupos de lista.

Sobre Esta Tarefa

Na janela Grupos de procura de ativos, é possível 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 **Outro**.

A janela Grupos de Procura de Ativos exibe os seguintes parâmetros para cada grupo:

Tabela 38. Funções da barra de ferramentas da janela Grupos de Procura de Ativos

Função	Descrição
Novo grupo	Para criar um novo grupo de procura, você pode clicar em Novo grupo . Consulte Criando um novo grupo de procura.
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 em 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 você deseja remover e clique em Remover . 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 **Procurar > 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 Ativo, 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

É possível 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. Digite uma nova descrição no campo **Descrição**.
9. Clique em **OK**.

Copiando uma procura salva em outro grupo

É possível 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 item, selecione a caixa de seleção para o grupo que você deseja copiar a procura salva.
8. Clique em **Designar grupos**.

Removendo um grupo ou uma procura salva de um grupo

É possível 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, a procura salva não será excluída do sistema. A procura salva é removida do grupo e automaticamente movida para o grupo **Outros**.

Não é possível remover os seguintes grupos do sistema:

- Grupos de Procura de Ativo
- Outro

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 de ativo usando a guia **Ativos**.

Sobre Esta Tarefa

Usando a guia **Ativos**, é possível excluir, importar e exportar perfis de ativos.

Excluindo ativos

É possível excluir ativos específicos ou todos os perfis de ativo listados.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione o ativo que 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 deste ativo até 255 caracteres de comprimento. Vírgulas não são válidas neste campo e invalidam o processo de importação. Por exemplo: WebServer01 está correto.
- **Peso** – Especifica um número de 0 a 10, que indica a importância deste ativo em sua rede. Um valor de 0 denota importância baixa e 10 é muito alta.
- **Descrição** – Especifica uma descrição textual para este ativo 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 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 **Navegar** para localizar e selecionar o arquivo CSV que você deseja importar.
5. Clique em **Importar ativos** para iniciar o processo de importação.

Exportando ativos

É possível exportar Perfis de ativos listados em um arquivo Extended Markup Language (XML) ou Comma-Separated Value (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. Visualize a janela de status para o status do processo de exportação.
5. Opcional: Se você desejar usar outras guias e páginas enquanto a exportação estiver em andamento, clique no link **Notificar quando estiver pronto**.
Quando a exportação for concluída, a janela Download de Arquivo será exibida.
6. Na janela Download de Arquivo, escolha uma das seguintes opções:
 - **Abrir** – Selecione esta opção para abrir os resultados de exportação em sua opção de navegador.
 - **Salvar** – Selecione esta opção para salvar os resultados em seu desktop.
7. Clique em **OK**.

Pesquisar vulnerabilidades de ativos

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

Sobre Esta Tarefa

É possível clicar duas vezes na vulnerabilidade para exibir mais detalhes de vulnerabilidade.

A janela Pesquisar Detalhes de Vulnerabilidade fornece os seguintes detalhes:

Parâmetro	Descrição
Vulnerability ID	Especifica o ID da vulnerabilidade. O ID de Vuln é um identificador exclusivo que é gerado pelo Sistema de Informação de Vulnerabilidade (VIS).
Published Date	Especifica a data na qual os detalhes de vulnerabilidade foram publicados no OSVDB.
Name	Especifica o nome da vulnerabilidade.
Assets	Especifica o número de ativos em sua rede que possuem esta 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 CVE para a vulnerabilidade. Os identificadores CVE são fornecidos pelo NVDB. Clique no link para obter mais informações. Quando você clica no link, o site NVDB é exibido em uma nova janela do navegador.

Parâmetro	Descrição
xforce	<p>Especifica o identificador X-Force para a vulnerabilidade.</p> <p>Clique no link para obter mais informações. Quando você clica no link, o website da IBM Internet Security Systems é exibido em uma nova janela do navegador.</p>
OSVDB	<p>Especifica o identificador do OSVDB para a vulnerabilidade.</p> <p>Clique no link para obter mais informações. Quando você clica no link, o website do OSVDB é exibido em uma nova janela do navegador.</p>
Detalhes do plug-in	<p>Especifica o ID do QRadar Vulnerability Manager.</p> <p>Clique no link para visualizar as Definições ovais, as entradas de Base de conhecimento do Windows ou os consultores do UNIX para a vulnerabilidade.</p> <p>Esse recurso fornece informações sobre como o QRadar Vulnerability Manager verifica os detalhes de vulnerabilidade durante uma varredura de correção. É possível usá-lo para identificar por que uma vulnerabilidade foi aumentada em um ativo ou por que não foi.</p>
Base de pontuação do CVSS	<p>Exibe a pontuação do Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras.</p> <p>A pontuação do CVSS é calculada usando os seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> • Potencial de Danos Colaterais • Requisito de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade <p>Para obter mais informações sobre como configurar estes parâmetros, consulte "Incluindo ou editando um perfil de ativo" na página 122.</p> <p>Para obter mais informações sobre o CVSS, consulte http://www.first.org/cvss/.</p>
Impact	<p>Exibe o tipo de prejuízo ou dano que pode ser esperado se essa vulnerabilidade for explorada.</p>

Parâmetro	Descrição
Métricas Base de CVSS	Exibe as métricas usadas para calcular a pontuação CVSS de base, incluindo: <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.
Referência	Exibe uma lista de referências externas, incluindo: <ul style="list-style-type: none"> • Tipo de referência – Especifica o tipo de referência que está listada, como uma URL consultiva ou lista de postagem do correio. • URL – especifica a URL na qual você pode clicar para visualizar a referência. Clique no link para obter mais informações. Ao clicar no link, o recurso externo será exibido em uma nova janela do navegador.
Produtos	Exibe uma lista de produtos associados a essa vulnerabilidade. <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 da área de janela Resumo de ativo que é acessada a partir da página Perfil de ativo.

A área de janela Resumo de ativo na página Perfil de ativo fornece as seguintes informações:

Tabela 10-8 Parâmetros da área de janela Resumo de ativo

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.
MAC Address	Exibe o último endereço MAC conhecido do ativo.
Network	Exibe a última rede relatada associada ao ativo.
NetBIOS Name	Exibe o nome NetBIOS do ativo, se conhecido. Se o ativo tiver mais de um nome NetBIOS, este campo indicará o número de nomes NetBIOS. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de nomes NetBIOS associados.
DNS Name	Exibe o endereço IP ou nome DNS do ativo, se conhecido. Se o ativo tiver mais de um nome DNS, este campo indicará o número de nomes DNS. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de nomes DNS associados.
Nome Dado	Exibe o nome do ativo. Por padrão, este campo está vazio. Para fornecer um determinado nome para o ativo, edite o perfil de ativo.
Group Name	Exibe o grupo último grupo de usuário conhecido do ativo, se conhecido.

Parâmetro	Descrição
Último Usuário	Exibe o último usuário conhecido do ativo. As informações de usuário são derivadas de eventos de identidade. Se mais de um usuário estiver associado a este ativo, será possível clicar no link para exibir todos os usuários.
Operating System	Exibe o sistema operacional que está em execução 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. É possível editar esse parâmetro diretamente se o parâmetro Override for especificado como Até a próxima varredura ou Indefinidamente .
Weight	Exibe o nível de importância que está associado a este ativo. O intervalo é de 0 (Não Importante) a 10 (Muito Importante). Por padrão, este campo está vazio. Para fornecer uma ponderação para o ativo, edite o perfil de ativo.
Aggregate CVSS Score	Exibe a pontuação do Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras. A pontuação do CVSS é calculada usando os seguintes parâmetros definidos pelo usuário: <ul style="list-style-type: none"> • Potencial de Danos Colaterais • Requisito de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade Para obter mais informações sobre como configurar estes parâmetros, consulte “Incluindo ou editando um perfil de ativo” na página 122. Para obter mais informações sobre o CVSS, consulte http://www.first.org/cvss/ .
Business Owner	Exibe o nome do proprietário de negócios do ativo. Um exemplo de um proprietário de negócios é um gerente de departamento.
Business Owner Contact Info	Exibe as informações de contato do proprietário de negócios.

Parâmetro	Descrição
CVSS Collateral Damage Potential	Exibe o potencial que esse ativo tem para danos colaterais. Este valor é incluído na fórmula para calcular o parâmetro CVSS Score . Por padrão, esse campo não está definido. Para fornecer um local para o ativo, edite o perfil de ativo.
Technical Owner	Exibe o responsável técnico do ativo. Um exemplo de um responsável técnico é um gerenciador de TI ou diretor.
Technical Owner Contact Info	Exibe as informações de contato do responsável técnico.
CVSS Availability	Exibe o impacto de disponibilidade do ativo quando uma vulnerabilidade for explorada com sucesso.
Wireless AP	Exibe o ponto de acesso (AP) wireless deste perfil de ativo.
SSID Wireless	Exibe o Identificador de Conjunto de Serviço Wireless (SSID) deste perfil de ativo.
CVSS Confidentiality Requirements	Exibe o impacto na confidencialidade de uma vulnerabilidade explorada com sucesso neste ativo.
Switch ID	Exibe o ID do comutador deste perfil ativo.
Switch Port ID	Exibe o ID da porta do comutador deste perfil de ativo.
CVSS Integrity Requirements	Exibe o impacto à integridade do ativo quando uma vulnerabilidade for explorada de maneira bem-sucedida.
Technical User	Especifica o nome do usuário que está associado a este perfil de ativo.
Open Services	Exibe o número de aplicativos exclusivos da Camada 7 que são executados neste perfil de ativo.
Vulnerabilidades	Exibe o número de vulnerabilidades que são descobertas nesse perfil de ativo.
Location	Especifica o local físico do ativo. Por padrão, este campo está vazio. Para fornecer um local para o ativo, edite o perfil de ativo.
Asset Description	Especifica uma descrição deste ativo. Por padrão, este campo está vazio. Para fornecer uma descrição para o ativo, edite o perfil de ativo.
Extra Data	Especifica quaisquer informações estendidas que são baseadas em um evento.

Área de janela de resumo da interface de rede

É possível localizar as descrições de parâmetros para a área de janela Resumo da interface de rede acessada a partir da página Perfil de ativo.

A área de janela Resumo da interface de rede na página Perfil de ativo fornece as seguintes informações:

Tabela 1 Parâmetros de área de janela Resumo de interface de rede

Parâmetro	Descrição
MAC Address	Exibe o endereço MAC deste ativo, se conhecido.
IP Address	Exibe o endereço IP que é detectado para este endereço MAC.
Network	Exibe a rede com a qual o endereço IP está associado, se conhecido.
Last Seen	Exibe a data e hora em que o endereço IP foi detectado por último nesse endereço MAC.

Área de janela Vulnerabilidade

É possível localizar descrições de parâmetros da área de janela Vulnerabilidade acessada a partir da página Perfil de ativo.

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

Tabela 39. Parâmetros da área de janela Vulnerabilidade

Parâmetro	Descrição
ID	Exibe o ID da vulnerabilidade. O ID é um identificador exclusivo que é gerado pelo Sistema de Informação de Vulnerabilidade (VIS).
Gravidade	Exibe a severidade da Indústria de Segurança de Pagamento (PCI) que está associada à vulnerabilidade.
Risk	O 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 um serviço estiver associado, exibe o serviço. Caso contrário, exibe Vários (N) onde N indica ao número total de serviços associados a esta vulnerabilidade.
Port	Exibe o número da porta na qual esta vulnerabilidade foi descoberta. Se a vulnerabilidade for 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 da porta.

Tabela 39. Parâmetros da área de janela Vulnerabilidade (continuação)

Parâmetro	Descrição
Vulnerability	Nome ou título desta vulnerabilidade.
Details	Texto detalhado específico que está associado a essa vulnerabilidade, conforme determinado pela varredura. Se somente um detalhe estiver associado, exibe o texto desse Detalhe. Caso contrário, exibe Vários (N) onde N indica ao número total de Detalhes que estão associados a esta vulnerabilidade.
CVSS Score	<p>Exibe a pontuação do Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras.</p> <p>A pontuação do CVSS é calculada usando os seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> • Potencial de Danos Colaterais • Requisito de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade <p>Para obter mais informações sobre como configurar estes parâmetros, consulte “Incluindo ou editando um perfil de ativo” na página 122.</p> <p>Para obter mais informações sobre o CVSS, consulte http://www.first.org/cvss/.</p>
Found	Exibe a data na qual essa vulnerabilidade foi originalmente encontrada em uma varredura.
Last seen	Exibe a data na qual essa vulnerabilidade foi vista pela última vez em uma varredura.

Área de janela Serviços

É possível localizar descrições de parâmetros da área de janela Serviços acessada a partir da página Perfil de ativo.

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

Tabela 40. parâmetros da área de janela serviços

Parâmetro	Descrição
Service	Exibe o nome do serviço aberto.
Produto	Exibe o produto que executa este serviço, se conhecido.

Tabela 40. parâmetros da área de janela serviços (continuação)

Parâmetro	Descrição
Port	Exibe a porta na qual o aplicativo 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 da porta.
Protocol	Exibe uma lista separada por vírgula de protocolos que são descobertos na porta que executa o serviço aberto.
Last Seen Passive	Exibe a data e hora em que o serviço aberto foi visto pela última vez passivamente.
Last Seen Active	Exibe a data e hora em que o serviço aberto foi visto pela última vez ativamente.
Service Default Ports	Exibe uma lista separada por vírgula de portas conhecidas que o aplicativo Camada 7 é conhecido por executar.
Vulnerabilities	Exibe o número de vulnerabilidades que estão associadas a este serviço aberto.

Área de janela de Serviços do Windows

É possível localizar as descrições de parâmetros da área de janela Serviços do Windows acessada a partir da página Perfil de ativo. A área de janela Serviços do Windows será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema.

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

Tabela 41. Parâmetros da área de janela Serviços do Windows

Parâmetro	Descrição
Name	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 as descrições de parâmetros para a área de janela Pacotes acessada a partir da página Perfil de ativo.

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

Tabela 42. Parâmetros da área de janela Pacotes

Parâmetro	Descrição
Packages	Exibe o nome do pacote que é aplicado ao ativo.
Version	Exibe a versão do pacote que é aplicada ao ativo.
Revision	Exibe a revisão do pacote que é aplicada ao ativo.

Área de janela de correções do Windows

É possível localizar descrições de parâmetros para a área de janela Correções do Windows que é acessada a partir da página Perfil de ativo.

A área de janela Correções do Windows será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema. A área de janela Correções do Windows na página Perfil de ativo fornece as seguintes informações:

Tabela 43. Parâmetros da área de janela Correções do Windows

Parâmetro	Descrição
Microsoft KB Number	Exibe número da Base de Conhecimento (KB) da Microsoft da correção do Windows que é executada no ativo.
Description	Exibe a descrição da correção do Windows.
Bulletin ID	Exibe o número do ID do boletim da correção do Windows.
ID de vulnerabilidade	Exibe o ID de vulnerabilidade da correção do Windows.
CVE-ID	Exibe o ID de CVE associado à correção do Windows. Se mais de um ID de CVE for associado à correção do Windows, mova o seu mouse sobre o link Vários para exibir a lista de IDs de CVE. É possível clicar em um link do ID de CVE para acessar mais informações.
System	Exibe o sistema Windows para a correção.
Service Pack	Exibe o Service Pack da correção.

Área de janela de propriedades

É possível localizar descrições de parâmetros para a área de janela Propriedades acessada na página Perfil de ativo. A área de janela Propriedades será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema.

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

Tabela 44. Parâmetros da área de janela Propriedades

Parâmetro	Descrição
Name	Exibe o nome da propriedade de configuração que foi vista ativamente no ativo.

Tabela 44. Parâmetros da área de janela Propriedades (continuação)

Parâmetro	Descrição
Value	Exibe o valor da propriedade de configuração.

Área de janela Políticas de risco

É possível localizar descrições de parâmetros da área de janela Políticas de risco, acessada a partir da página Perfil de ativo. A área de janela Políticas de riscos será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema.

A área de janela Políticas de risco em Perfil de ativo fornece as seguintes informações:

Tabela 45. Parâmetros da área de janela Políticas de risco

Parâmetro	Descrição
Policy	Especifica o nome da política associada a esse ativo.
Pass/Fail	Indica se a política tem um status Aprovado ou Reprovado .
Last Evaluated	Exibe a data da última vez que esta política foi avaliada.

Área de janela Produtos

É possível 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 46. 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 11. 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 47. 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 47. 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 48. Opções da barra de ferramentas Relatórios

Opção	Descrição
Grupo	

Tabela 48. 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. É possível compartilhar grupos de relatórios com outros usuários.

Tabela 48. Opções da barra de ferramentas Relatórios (continuação)

Opção	Descrição
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 48. 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	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: <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

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. Será possível 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*.

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

Use o assistente de Relatório para criar e customizar 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 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

Após você criar um relatório que é gerado 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 construídos. Por exemplo, uma procura semanal requer sete dias para construir os dados. Essa procura retornará resultados após 7 dias.

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 usa 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. Na janela Bem-vindo ao assistente do Relatório! , clique em **Avançar**.
4. Selecione uma das opções a seguir:

Opção	Descrição
Manualmente	Por padrão, o relatório é gerado 1 vez. É possível gerar o relatório tantas vezes quanto você desejar.
Por hora	Planeja o relatório para ser gerado no final de cada hora. Os dados da hora anterior são usados. 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 .
Semanal	Planeja o relatório para gerar semanalmente usando os dados da semana anterior. 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.
Mensal	Planeja o relatório para gerar mensalmente usando os dados do mês anterior. Na caixa de listagem, selecione a data que você deseja gerar o relatório. O padrão é o primeiro dia do mês. Selecione um horário 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. A partir da caixa de listagem **Orientação**, selecione **Retrato** ou **Paisagem** para a orientação da página.
 - b. Selecione uma das seis opções de layout exibidas no assistente de Relatório.
 - c. Clique em **Avançar**.
7. Especifique valores para os seguintes parâmetros:

Parâmetro	Valores
Título do Relatório	O título pode ter até 100 caracteres de comprimento. Não use caracteres especiais.

Parâmetro	Valores
Logotipo	A partir da caixa de listagem, selecione um logotipo.
Opções de Paginação	A partir da caixa de listagem, selecione um local para números de página a serem exibidos no relatório. É possível escolher não ter exibição de números de página.
Classificação do Relatório	Digite uma classificação para esse relatório. É possível digitar até 75 caracteres de comprimento. É possível usar espaços iniciais, caracteres especiais e caracteres de byte duplo. A classificação do relatório é exibida no cabeçalho e no rodapé do relatório. Talvez você queira classificar o seu relatório como confidencial, altamente confidencial, sensível ou interno.

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, configure os parâmetros do gráfico.

Nota: Também é possível criar procuras salvas de ativo. A partir da caixa de listagem **Procurar para usar**, selecione a sua procura salva.

- c. Clique em **Salvar detalhes do contêiner**.
 - d. Se você selecionou mais de um contêiner, repita as etapas a até c.
 - e. Clique em **Avançar**.
9. Visualize a página de Visualização de Layout e, em seguida, clique em **Avançar**.
10. Selecione as caixas de seleção para os formatos de relatório que você deseja gerar e, em seguida, clique em **Avançar**.

Importante: 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 do Relatório	Selecione esta caixa de seleção para enviar o relatório gerado para a guia Relatórios . Console do Relatório 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.

Opção	Descrição
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.
Email	Selecione essa caixa de seleção se desejar distribuir o relatório gerado por 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 do Relatório	Essa opção é exibida somente depois que você seleciona a caixa de seleção Email . Selecione essa caixa de seleção para incluir um link para o Console do Relatório no email.

12. Na página Concluindo, insira os valores para os parâmetros a seguir.

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.
Selecione quaisquer grupos dos quais gostaria que esse relatório fosse membro	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

É possível 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.

Nota: Quando você customizar um relatório planejado para ser gerado manualmente, selecione o período de tempo **Data de Encerramento** antes de selecionar a **Data de Início**.

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 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.

Visualizando relatórios gerados

Na guia **Relatórios**, um ícone será exibido na coluna **Formatos** se um relatório possuir conteúdo gerado. É possível 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 gerado são exibidos na coluna **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).

É possível 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. É possível 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.

É possível 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

É possível customizar o relatório duplicado.

Compartilhando um relatório

É possível 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
- Outro

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 IBM Security QRadar Log Manager*.

Criando um grupo de relatórios

É possível 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 os valores para os parâmetros a seguir:
 - **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

É possível 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.

Compartilhando grupos de relatórios

É possível compartilhar grupos de relatórios com outros usuários.

Antes de Iniciar

Você deve ter permissões administrativas para compartilhar um grupo de relatórios com outros usuários.

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

Não é possível usar a Ferramenta de Gerenciamento de Conteúdo (CMT) para compartilhar grupos de relatórios.

Para obter informações adicionais sobre a CMT, consulte o *IBM Security QRadar SIEM Administration Guide*

Sobre Esta Tarefa

Na janela Grupos de Relatórios, usuários compartilhados podem ver o grupo de relatórios na lista de relatórios.

Quaisquer atualizações que o usuário fizer em um grupo de relatórios compartilhados não afetam a versão original do relatório. Somente o proprietário pode excluir ou modificar.

Uma cópia do relatório é criada quando um usuário duplica ou executa o relatório compartilhado. O usuário pode editar ou planejar relatórios dentro do grupo de relatórios copiado.

A opção de compartilhamento de grupo substitui opções de compartilhamento de relatório anterior que foram configuradas para relatórios no grupo.

Procedimento

1. Clique na guia **Relatórios**.
2. Na janela **Relatórios**, clique em **Gerenciar Grupos**.
3. Na janela **Grupos de Relatórios**, selecione o grupo de relatórios que você deseja compartilhar e clique em **Compartilhar**.
4. Na janela **Opções de Compartilhamento**, selecione uma das opções a seguir.

Opção	Descrição
Padrão (herdar do pai)	<p>O grupo de relatórios não é compartilhado.</p> <p>Qualquer grupo de relatórios copiado ou relatório gerado permanece na lista de relatórios dos usuários.</p> <p>Cada relatório no grupo é designado com qualquer opção de compartilhamento de relatório-pai que foi configurada.</p>
Compartilhar com Todos	<p>O grupo de relatórios é compartilhado com todos os usuários.</p>
Compartilhe com usuários que correspondem aos seguintes critérios...	<p>O grupo de relatórios é compartilhado com usuários específicos.</p> <p>Funções de Usuário Selecione a partir da lista de funções de usuário e pressione o ícone incluir (+).</p> <p>Perfis de Segurança Selecione a partir da lista de perfis de segurança e pressione o ícone incluir (+).</p>

5. Clique em **Salvar**.

Resultados

Na janela Grupos de Relatórios, usuários compartilhados veem o grupo de relatórios na lista de relatórios. Relatórios gerados exibem conteúdo com base na configuração do perfil de segurança.

Designar um relatório a um grupo

É possível 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 **Remover** 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 **Remover**.
6. Clique em **OK**.
7. Feche a janela Grupos de relatórios.

Avisos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos

incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

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

Marcas comerciais

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

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



e/ou em outros países.

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

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

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

Considerações sobre política de privacidade

Os produtos de Software IBM, including software as a service solutions, (“Ofertas de software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto, ajudar a melhorar a experiência do usuário final, customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação de identificação pessoal é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar na coleta de informações de identificação pessoal. Se esta Oferta de Software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

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

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

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

Glossário

Este glossário fornece termos e definições para os produtos e o software [nome do produto].

As referências cruzadas a seguir são usadas neste glossário:

- *Consulte* o encaminha de um termo não preferencial para um termo preferencial ou de forma de abreviação para uma forma integral.
- *Consulte também* o encaminha para um termo relacionado ou contrastante.

Para outros termos e definições adicionais, veja o website IBM Terminology (abre em uma nova janela).

"A" "B" "C" "D" na página 166 "E" na página 167 "F" na página 167 "G" na página 167 "H" na página 167 "I" na página 167 "L" na página 168 "M" na página 168 "N" na página 168 "O" na página 169 "P" na página 169 "R" na página 169 "S" na página 170 "T" na página 171 "V" na página 171

A

acumulador

Um registro no qual um operando de uma operação pode ser armazenada e, subsequentemente, substituído pelo resultado dessa operação.

agregação de link

O agrupamento de placas da interface de rede física, como cabos ou portas, em uma única interface de rede lógica. A agregação de link é usada para aumentar a disponibilidade da rede e da largura da banda.

Alta disponibilidade (HA)

Pertencente a um sistema em cluster, que é reconfigurado quando nó ou falhas de daemon ocorrem, para que as cargas de trabalho possam ser redistribuídos para os nós restantes no cluster.

anomalia

Um desvio do comportamento esperado da rede.

ARP Consulte Protocolo de Resolução de Endereço.

ARP (Address Resolution Protocol)

Um protocolo que mapeia dinamicamente um endereço de IP para um adaptador de rede, mapeia em uma rede local.

arquivo-chave

Em segurança de computador, um arquivo que contém chaves públicas, chaves privadas, raízes confiáveis e certificados.

arquivo de armazenamento confiável

Um arquivo de banco de dados de chave que contém as chaves públicas para uma entidade confiável.

ASN Consulte número de sistema autônomo.

assinatura de aplicativo

Um conjunto exclusivo de características que são derivadas pelo exame da carga útil do pacote e, em seguida, são usadas para identificar um aplicativo específico.

ativo Um objeto gerenciável que é implementado ou que se pretende que seja implementado em um ambiente operacional.

B

burst Um aumento súbito e nítido na taxa dos eventos ou fluxos recebidos, de forma que o limite da taxa do evento ou do fluxo licenciado seja excedido.

C

camada de rede

Na arquitetura de OSI, a camada que fornece serviços para estabelecer um caminho entre os sistemas abertos com uma qualidade de serviço previsíveis.

captura de conteúdo

Um processo que captura um valor configurável de carga útil e em seguida, armazena os dados em um log do fluxo.

CIDR Consulte Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)

Um método para incluir a classe C de endereços IP (Internet Protocol). Os endereços são oferecidos aos Provedores

de Serviço Internet (ISPs) para utilização de seus clientes. Endereços CIDR reduzem o tamanho das tabelas de roteamento e tornam disponíveis mais endereços IP nas organizações.

cliente

Um programa ou computador de software que atende os serviços a partir de um servidor.

Cluster HA

Uma configuração de alta disponibilidade que consiste em um servidor principal e um servidor secundário.

compartilhamento administrativo

Um recurso de rede que fica oculto dos usuários sem privilégios administrativos. Os compartilhamentos administrativos fornecem aos administradores acesso a todos os recursos em um sistema de rede.

comportamento

Os efeitos observáveis de uma operação ou de um evento, incluindo seus resultados.

conjunto de referência

Uma lista de elementos únicos que são derivados de eventos ou fluxos em uma rede. Por exemplo, uma lista de endereços IP de uma lista de nomes de usuários.

console

Uma estação de exibição, da qual um operador pode controlar e observar um sistema de produção.

contexto do host

Um serviço que monitora os componentes para assegurar que cada componente está operando conforme o esperado.

conversão de endereço de rede (NAT)

Em um firewall, a conversão de segurança de Internet Protocol (IP) endereça para endereços registrados externos. Isto permite comunicações com redes externas, mas mascara os endereços IP usados dentro do firewall.

credencial

Um conjunto de informações que é concedida a um usuário ou certos processos de direitos de acesso.

credibilidade

Uma classificação numérica entre 0-10 que é utilizada para determinar a integridade de um evento ou uma ofensa.

Credibilidade aumenta à medida que várias fontes relatam o mesmo evento ou ofensa.

criptografia

Na segurança do computador, o processo de transformação de dados em uma forma ininteligível, de tal maneira que os dados originais, quer não pode ser obtido ou só pode ser obtida por meio de um processo de decifração.

CVSS Veja Common Vulnerability System.

D**dados de carga útil**

os dados do aplicativo contidos em um fluxo de IP, excluindo cabeçalho e informações administrativas.

destino de encaminhamento

Um ou mais sistemas fornecedores que recebem dados brutos e normalizados a partir de fontes de log e fontes de fluxo.

destino externo

Um dispositivo que está fora do local primário que recebe fluxo de evento ou dados de um coletor de eventos.

Device Support Module (DSM)

Um arquivo de configuração que analisa eventos recebidos de múltiplas fontes de log e os converte para um formato de taxonomia padrão, que pode ser exibida como saída.

DHCP Consulte Dynamic Host Configuration Protocol.

dispositivo de varredura externo

Uma máquina que está conectada à rede para reunir informações de vulnerabilidade sobre ativos na rede.

DNS Consulte Domain Name System.

DSM Consulte Módulo de Suporte de Dispositivo.

Dynamic Host Configuration Protocol (DHCP)

Um protocolo de comunicação utilizado para gerenciar centralmente as informações de configuração. Por exemplo, o DHCP automaticamente designa endereços IP para computadores em uma rede.

E

endereço IP virtual de cluster

Um endereço IP que é compartilhado entre o host primário ou secundário e o cluster de HA.

extensão de origem de log

Um arquivo XML que inclui todos os padrões de expressão regular necessários para identificar e categorizar eventos da carga útil do evento.

F

falso positivo

Um resultado de teste classificado como positivo (indicando que o site está vulnerável ao ataque), que o usuário decide que é na realidade negativo (não uma vulnerabilidade).

Fluxo Uma única de transmissão de dados transmitidos através de um link durante uma conversa.

fluxo de log

Uma coleção de gravação de fluxo.

fluxo duplicado

Várias instâncias do mesmo fluxo de transmissão recebidos a partir de diferentes origens de dados.

folha Em uma árvore, uma entrada ou nó que não possui frutos.

fontes de fluxo

A origem na qual o fluxo é capturado. Uma fonte de fluxo é classificada como interna, quando o fluxo vem de um hardware instalado em um gerenciador de host ou é classificado como externo, quando o fluxo é enviado para um coletor de fluxo.

FQDN

Consulte nome completo do domínio.

FQNN

Consulte nome completo da rede.

funcionário público

Um componente interno que analisa o tráfego de rede e os eventos de segurança com relação a regras customizadas definidas.

G

Gateway

Um dispositivo ou programa usado para conectar redes ou sistemas com diferentes arquiteturas de rede.

H

HA Consulte alta disponibilidade.

Hash-Com Message Authentication Code (HMAC)

O código de criptografia que usa criptografia função hash e chave secreta.

hierarquia de rede

Um tipo de contêiner que constitui uma coleta hierárquica de objetos da rede.

HMAC

Consulte Código de autenticação Hash-Based Message .

host de HA primário

O computador principal que é conectada ao cluster de HA.

host de HA secundário

O computador espera que o está conectado ao cluster de HA. O host de HA secundário assume a responsabilidade do host de HA primário se o host de HA primário falhar.

I

ICMP Consulte Internet Control Message Protocol.

Identifica

Uma coleta de atributos de uma origem de dados que representa uma pessoa, organização, lugar ou item.

IDS Consulte sistema de detecção de intrusão.

Interconexão de sistemas abertos (OSI)

A interconexão de sistemas abertos em concordância com padrões do International Organization for Standardization (ISO) para a troca de informações.

Interface vinculada

Consulte agregação de link.

Internet Control Message Protocol (ICMP)

Um protocolo de Internet que é usado por um gateway para comunicar-se com um

host de origem, por exemplo, para reportar um erro em um datagrama.

intervalo de relatório

Um intervalo de tempo configurável no final do qual o processador de evento deve enviar todos os eventos capturados e fluxo de dados para o console.

intervalo de união

O intervalo no qual os eventos são empacotados. o pacote configurável de eventos ocorre em intervalos de 10s. e começa com o primeiro evento que não corresponde a nenhum evento de união atualmente. No intervalo de união, os três primeiros eventos correspondentes são empacotados e enviados para o processador de eventos.

IP Consulte Protocolo da Internet.

IP multicast

Transmissão de um datagrama protocolo de internet (IP), para configurar sistemas que formam um grupo multicast único.

IPS Consulte sistema de prevenção de intrusão.

ISP Consulte Provedor de serviços da Internet.

L

LDAP Consulte protocolo LDAP.

L2L Consulte Local para Local.

Local para Local (L2L)

Pertencente ao tráfego interno de uma rede local para outra rede local.

Local para Remoto (R2L)

O tráfego externo a partir de uma rede remota a uma rede local.

L2R Consulte Local para Remoto.

M

magnitude

Uma medida da importância relativa de uma determinada falha crítica. Magnitude é um valor calculado a partir de peso a relevância, gravidade e credibilidade.

mapa de referência

Um registro de dados de mapeamento

direto de uma chave para um valor, por exemplo, um nome de usuário para um ID global.

mapa de referência de conjuntos

Um registro de dados de uma chave mapeada para muitos valores. Por exemplo, o mapeamento de uma lista de usuários privilegiados para um host.

mapa de referência de mapas

Um registro de dados de duas chaves mapeadas para muitos valores. Por exemplo, o mapeamento do total de bytes de um aplicativo para um IP de origem.

Mapear QID

Uma taxonomia que identifica cada evento único e mapeia os eventos de categoria baixo e alto nível, para determinar como um evento deve ser correlacionado e organizado.

máscara de sub-rede

Para sub-rede da Internet, uma máscara de 32 bits usada para identificar os bits do endereço da sub-rede na parte do host de um endereço IP.

N

NAT Consulte conversão de endereço de rede.

NetFlow

Um protocolo de rede Cisco que monitora dados do fluxo do tráfego de rede. Dados NetFlow incluem informações do cliente e informações de servidores, cujas portas são usadas, e o número de bytes e pacotes que fluem através de roteadores conectados a uma rede. Os dados são enviados para os coletores NetFlow onde dados são analisados.

Nome completo da rede (FQNN)

Em uma hierarquia da rede, o nome de um objeto que inclui todos os departamentos. Um exemplo de um nome completo de rede é CompanyA.Department.Marketing.

Nome completo do domínio (FQDN)

Em comunicações da Internet, o nome de um sistema de host que inclui todos os subnomes do nome de domínio. Um exemplo de um nome de domínio completo é rchland.vnet.ibm.com.

número do 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 possibilita que algoritmos de roteamento automatizado façam distinção entre sistemas autônomos.

O

objeto rede

Um componente de uma hierarquia de rede.

ofensa Uma mensagem enviada ou um evento gerado em resposta a uma condição monitorada. Por exemplo, uma ofensa fornecerá informações sobre se uma política tiver sido infringida ou a rede está sofrendo um ataque.

O objeto folha de banco dados

Um nó ou um objeto terminal em uma hierarquia de banco de dados.

ordem de análise

Uma definição de origem de log em que o usuário pode definir a ordem de importância de origens de log que compartilham um endereço IP ou um nome de host comum.

origem do log

O equipamento de segurança ou o equipamento de rede a partir da qual uma origem de log de eventos.

origem externa

Um dispositivo que está fora do local primário que envia dados normalizados para um coletor de eventos.

o servidor whois

Um servidor que é utilizado para recuperar as informações sobre uma Internet recursos registrados, como nomes de domínio e alocações de endereço IP.

OSI Consulte interconexão de sistemas abertos.

OSVDB

Consulte Abrir Origem Vulnerabilidade de Banco de Dados.

P

Para Local (Remote L2R)

Relativo ao tráfego interno de uma rede local para outra rede remota.

para Remoto (Remote R2R)

O tráfego externo a partir de uma rede remota para outra rede remota.

peso de rede

O valor numérico aplicado para cada rede que significa a importância da rede. O peso da rede é definido pelo usuário.

ponto de dados

Um valor calculado de uma métrica em um momento.

protocolo

Um conjunto de regras que controlam a comunicação e a transferência de dados entre dois ou mais dispositivos ou sistemas em uma rede de comunicação.

Protocolo da Internet(IP)

Um protocolo que encaminha dados através de uma rede ou redes interconectadas. Este protocolo atua como um intermediário entre as camadas de protocolo superiores e a rede física. Consulte também Transmission Control Protocol.

Protocolo de Controle de Transmissões (TCP)

Um protocolo de comunicação utilizado na Internet e em todas as redes que seguem os padrões da Internet Engineering Task Force (IETF) para protocolo de interligação de redes. O TCP oferece um protocolo confiável de host a host em redes de comunicação através da comutação de pacotes e em sistemas interconectados dessas redes. Consulte também Internet Protocol.

protocolo LDAP

Um protocolo que usa TCP/IP para fornecer acesso aos diretórios que suportam um modelo X.500 que não incorra nos requisitos de recursos X.500 Directory Access Protocol (DAP) mais complexos. Por exemplo, LDAP pode ser usado para localizar pessoas, organizações, e outros recursos em um diretório intranet, ou internet.

Provedor de serviços da Internet (ISP)

Uma organização que fornece acesso à Internet.

R

recon Consulte reconhecimento.

reconhecimento (recon)

Um método pelo qual informações referentes à identidade de recursos de rede são reunidos. Varredura de rede e outras técnicas são usadas para compilar uma lista de eventos de recurso de rede que são então designados com um nível de severidade.

Rede Local

Consulte rede local.

Rede local (LAN)

Uma rede que conecta vários dispositivos em uma área limitada (tal como uma única construção ou campus) e que pode ser conectada a uma rede maior.

Redirecionamento do ARP

Um método ARP para notificar o host se 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 satisfeitos por dados do evento, uma coleta de condições e roteamento subsequente são executadas.

relatório

Em um gerenciamento de consulta, os dados formatados que resultam da execução de uma consulta e da aplicação de um formulário a ela.

relevância

Uma medida de impacto relativo de um evento, categoria ou ofensa na rede.

R2L Consulte Local para Remoto.

R2R Consulte Para Remoto Remoto.

S**scanner**

Um programa de segurança automatizado que procura vulnerabilidades de software nos aplicativos da web.

severidade

Uma medida da ameaça relativo que uma origem apresenta em um destino.

sistema ativo

Em um cluster de alta disponibilidade

(HA), o sistema que possui todos os seus serviços em execução.

Sistema de detecção de intrusão (intrusion detection system) (IDS)

Software que detecta tentativas de ataque ou ataques bem sucedidos nos recursos monitorados que são parte de uma rede ou de um host de sistema.

sistema de espera

Um sistema que automaticamente se torna ativo quando o sistema ativo falhar. Se a replicação de disco estiver ativado, replica dados do sistema ativo.

Sistema de Nomes de Domínio (DNS)

O sistema de banco de dados distribuído que mapeia nomes de domínio para endereços IP.

Sistema de Pontuação de Vulnerabilidade Comum - Common Vulnerability Scoring System (CVSS)

Um sistema de pontuação cuja severidade de vulnerabilidade é medida.

Sistema de prevenção de intrusão (IPS)

Um sistema que tenta negar a atividade potencialmente dolosa. Os mecanismos de negação podem envolver filtragem, rastreamento ou configuração de taxa limite.

SNMP

Consulte Simple Network Management Protocol.

SNMP (Simple Network Management Protocol)

Um conjunto de protocolos para sistemas de monitoramento e os dispositivos em redes complexas. As informações sobre os dispositivos gerenciados são definidas e armazenadas em uma Management Information Base (MIB).

SOAP Um protocolo leve, baseado em XML para troca de informações em um ambiente distribuído, descentralizado. SOAP pode ser utilizado para consultar e retornar informações e chamar os serviços através da Internet.

sub-procura

Uma função que permite que uma consulta de procura para ser executada dentro de um conjunto de resultados de procura concluídas.

sub-rede

Consulte sub-rede.

sub-rede (sub-rede)

Uma rede que é dividida em subgrupos independentes menores, que ainda estão interconectados.

superflow

Um único fluxo que é composto de vários fluxos com propriedades semelhantes para aumentar a capacidade de processamento reduzindo as restrições de armazenamento.

rede para a segurança da comunidade de rede, um banco de dados aberto que fornece informações técnicas em uma rede de vulnerabilidade de segurança.

T**tabela de referência**

Uma tabela em que o registro de dados mapeia chaves que têm um tipo designado para outras chaves que são, em seguida, mapeadas para um único valor.

TCP Consulte Protocolo de Controle de Transmissões.

Tempo de atualização

Um dispositivo interno que é disparado manualmente ou automaticamente em intervalos de tempo que atualiza os dados da atividade de rede atual.

terminal

O endereço de uma API ou de um serviço em um ambiente. Uma API expõe um terminal e, ao mesmo tempo, chama os terminais de outros serviços.

V**varredura em tempo real**

Uma varredura de vulnerabilidade que gera dados de relatório a partir dos resultados da varredura com base no nome da sessão.

violação

Um ato que ignora ou contrária à política corporativa.

visualização do sistema

Uma representação visual de ambos primário e os hosts gerenciados que compõem um sistema.

vulnerabilidade

Uma exposição de segurança em um sistema operacional, software do sistema ou componente de software de aplicativo.

Vulnerabilidade de Banco de Dados de Origem Aberta (OSVDB)

Criado pela comunidade de segurança de

Índice Remissivo

A

administrador da rede vii
área de janela correções do Windows 135
Área de janela de pacotes 135
área de janela interface de rede 135
Área de janela Políticas de risco 135
Área de janela Produtos 135
área de janela propriedades 135
Área de janela Serviços 135
Área de janela Vulnerabilidade 135
as funções da barra de ferramentas de detalhes do evento 41
assistente de regras customizadas 6, 16
assistente Regra de Detecção de Anomalias 101
ativar regras 103
atividade de log 9, 12, 13, 17, 21, 23, 43, 61, 63, 67, 81, 82, 85, 86, 87, 88, 89, 97
critérios de procura 73
visão geral 23
atividade de rede 12, 21, 61, 63, 67, 81
ativo 117
ativos 5, 12, 13
atualizando detalhes do usuário 11
atualizar dados 9

B

barra de ferramentas 23
barra de ferramentas da página regras 108
barra de ferramentas de detalhes do evento 41
barra de status 27
blocos de construção 97
editando 107

C

caixa de lista de exibição 33
cancelar uma procura 85
classificar resultados em tabelas 8
coluna de dados do PCAP 44, 46
compartilhando grupos de relatórios 157
compartilhar relatórios 155
configurando atividade de log 18
configurando conexões 18
configurando gráficos 63
configurando itens do painel 18
configurar e gerenciar redes, plug-ins e componentes 6
configurar e gerenciar sistemas 6
configurar e gerenciar usuários 6
configurar tamanho da página 13
controles 6
copiar procura salva 88, 130
copiar um item para um grupo 106
copiar uma regra 104
criando grupos de procura 86

criando regras customizadas 100
criando um novo grupo de procura 87
criar novo grupo de procura 129
criar relatórios 5
criar um grupo de regras 105
critérios de procura
excluindo 82
guia atividade de log 82
salvando 73
salvos disponíveis 82

D

dados de Captura de Pacotes (PCAP) 44
dados do evento bruto 31
dados do evento não analisados 31
dados do PCAP 44, 45
desativar regras 103
descrição do evento 38
designar itens para um grupo 105
detalhes da vulnerabilidade 132
detalhes do evento 41
detalhes do evento único 38
distribuir relatórios 5
Duplicar um relatório 155

E

editar ativo 122
editar blocos de construção 107
editar grupo de procura 129
editar um grupo 106, 157
editar um grupo de procura 87
endereço IP 9, 116
especificar o número de objetos de dados para visualizar 18
especificar tipo de gráfico 18
eventos 15, 42, 63, 67
eventos normalizados 28
excluindo ativos 131
excluindo uma procura 86
excluir painel 20
excluir perfil de ativo 130
excluir uma regra 104
executando uma subprocura 81
executar dados 9
exibir em uma nova janela 20
exibir itens 15
exportando ativos 132
exportando eventos 46
exportar perfil de ativo 130

F

fazer download do arquivo PCAP 46
fazer o download do arquivo de dados do PCAP 45
filtro rápido 67
fluxo de eventos 28
fluxos 63, 67, 74

funções 97
fuso horário 144

G

gerar um relatório manualmente 154
Gerenciador de Vulnerabilidade QRadar 115
gerenciamento de grupo de regras 104
gerenciamento de painel 13
gerenciamento de regras 97, 103
gerenciando grupos de procura 86
Gerenciar grupos 130
gerenciar rede 115
gerenciar relatórios 5, 145
gerenciar resultados da procura 85, 86
Glossário 165
gráfico de série temporal 61
grupo
copiando um item 106
designando itens 105
editando 106
excluindo 107
excluindo um item 106
removendo 88
grupo de procura
criando 87
editando 87
grupo de procura de eventos 87
grupo de regras
criando 105
visualizando 105
grupos de procura
gerenciando 86
visualizando 86
grupos de procura de ativos 128
grupos de relatórios 157
Guia Administração 6
guia atividade de log 4, 8, 23, 27, 28, 31, 33, 42, 44, 46, 67, 83
guia atividade de rede 8, 67
guia ativo 115, 116, 119, 128
guia ativos 122, 128, 131
Guia Ativos 5, 115, 117, 120, 129, 130, 131
guia ofensas 8
guia padrão 4
guia painel 4, 6, 13, 17, 19, 20
Guia Painel 4, 13
guia relatório 144, 145
guia relatórios 8, 144
Guia Relatórios 5
guias 4
guias da interface com o usuário 4, 6

H

hosts 5

I

- IBM Security QRadar Vulnerability Manager 5
- ícone Remover 130
- ID 116
- imagem
 - relatórios
 - atribuição de marca 156
 - upload 156
- importar ativos 131
- importar perfil de ativo 130
- imprimir perfil de ativo 115
- incluindo itens de eventos 21
- incluindo itens de procura de fluxo 21
- incluir ativo 115, 122
- incluir filtro 81
- incluir itens 17, 21
- informações de login 4
- informações de login padrão 4
- informações do filtro de eventos 119
- informações sobre o usuário 11
- interface com o usuário 4
- introdução vii
- investigando eventos 13
- investigar a atividade de log 23
- investigar ativo 115
- investigar os logs de eventos 4
- item de painel notificação do sistema 16
- item de painel resumo do sistema 15
- item do painel 21
- itens do painel atividade de log 13

J

- janela grupos de procura 86

L

- Layout de relatório 148
- legendas do gráfico 63
- lista de eventos 38

M

- manter a regra customizada 97
- manter regras customizadas 97
- mapear evento 43
- mensagem de notificação 16
- menu ativado pelo botão direito 27
- menu de mensagens 6
- modificar mapeamento de evento 43
- modo de documento
 - Navegador da Web Internet Explorer 3
- modo de navegador
 - Navegador da Web Internet Explorer 3
- monitorando eventos 13
- mostrar painel 19, 20

N

- navegador da Web
 - versões suportadas 3
- navegar no QRadar 3

- nome de usuário 4
- nome do ativo 116
- nomes de usuários 11
- notificação do sistema 21
- notificações do sistema 6
- nova procura 129
- novos recursos
 - visão geral do guia do usuário 1

O

- o que há de novo 1
- objetos do gráfico 63
- ofensa 42
- ofensas 13, 67, 87
- ofensas atualizadas 15
- opções de eventos agrupados 33
- opções de menu ativado pelo botão direito 119
- ordem de classificação 145
- organizar os itens do painel 13
- origem do log 31

P

- página de detalhes do evento 38
- página de procura de ativo 126
- página perfil de ativo 132, 135, 138, 139, 140, 141, 142
- página perfis de ativo 116
- painel 21
- painel gerenciador de vulnerabilidade 15
- parâmetros da área de janela correções do Windows 141
- parâmetros da área de janela de produtos 142
- Parâmetros da área de janela Pacotes 140
- parâmetros da área de janela políticas de risco 142
- Parâmetros da área de janela Propriedades 141
- Parâmetros da área de janela Resumo da interface de rede 138
- parâmetros da área de janela resumo de ativo 135
- parâmetros da área de janela serviços 139
- parâmetros da área de janela serviços do Windows 140
- Parâmetros da área de janela Vulnerabilidade 138
- parâmetros da guia relatório 144
- parâmetros da página perfil de ativo 135
- parâmetros de eventos agrupados 33
- parâmetros de regra 107
- pausar dados 9
- perfil do ativo 120, 122
- perfis de ativos 115, 127, 128, 131, 132
- Perfis de ativos 117, 129, 130
- permissão de regra 97
- permissões 144
 - propriedades customizadas 89
- pontuação do CVSS agregado 116

- positivos falsos 115
- procura 129
 - copiando para um grupo 88
- procura planejada
 - eventos 74
 - procura 74
 - procura salva 74
- procurando 67
- procurando perfis de ativos 126
- procurar por ativo 115
- procuras de dados 67
- propriedade
 - copiando customizada 95
 - modificando customizada 94
- propriedade customizada 96
- propriedade de cálculo 92
- propriedade regex 90
- propriedades de evento customizado 89

Q

- QID 43

R

- redimensionar colunas 12
- regra
 - copiando 104
 - editar 103
 - respostas 98
- regra de detecção de anomalias 101
- regra de evento 97
- regras 97
 - ativando 103
 - desativando 103
 - visualizando 99
- relatório
 - editando 153
- relatórios 12, 13
 - visualizando 153
- Relatórios gerados mais recentemente 15
- relatórios personalizados 149
- remover grupo 88, 130
- remover item do painel 19
- remover procura salva 130
- remover procura salva de um grupo 88
- remover um item do painel 20
- renomear painel 20
- Resposta de Regra 110
- resultados da procura
 - cancelar 85
 - excluindo 86
 - salvando 83
 - visualizando gerenciado 83
- resultados do processador de evento 27
- resumo de atividade nas últimas 24 horas 15

S

- salvando critérios de procura de evento e de fluxo 28
- salvando resultados da procura 83
- salvar critérios 127
- salvar critérios de procura de ativo 127
- scanners de terceiros 115

senha 4
serviços 116
servidores 5
Sinalizador 16
sincronizar tempo 144

T

tabelas 13
tempo do console 11
tempo do sistema 11
tempo real 28
tempo real (fluxo) 9
testes 97
tipo de propriedade calculada 89

tipo de propriedade regex 89
tipos de diagrama 149
tipos de gráfico 148
tipos de propriedade 89

U

último minuto (atualização automática) 9

V

vários painéis 13
visão geral de gráficos 61
visualização de dados do PCAP 45

visualização de eventos agrupados 33
visualização do grupo de regra 105
visualizando eventos de fluxo 28
visualizando grupos de procura 86, 128
visualizando mensagens 6
visualizando ofensas associadas a eventos 42
visualizando resultados da procura gerenciada 83
visualizar ativos 115
visualizar notificações do sistema 21
visualizar perfil de ativo 120
visualizar regras customizadas 97
vulnerabilidades 115
Vulnerabilidades 116
vulnerabilidades de ativo 132