IBM Security Intelligence on Cloud:

Guia de Administração

Nota

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 67.

Informações do produto

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

Índice

Introdução à administração do produto QRadar

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

Público-Alvo

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

Documentação técnica

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

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

Entrando em contato com o suporte ao cliente

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

Declaração de boas práticas de segurança

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

Observação:

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

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

Capítulo 1. Gerenciamento do usuário

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

Usuário função de acesso e permissões

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

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

Tabela 1. Descrição da janela Gerenciamento de Função de Usuário parâmetros

Parâmetro	Descrição
Nome da função do usuário	Um nome exclusivo para a função.
Admin	Concede acesso administrativo para a interface com o usuário. Você pode conceder permissões: Admin específico **Gerenciador do Administrador** Concede acesso administrativo para a interface com o usuário. Você concede permissões específicas de Administrador. **Configuração de Redes e Serviços Remotos** Concede permissão para configurar redes remotas e serviços na guia **Admin** . **Administrador do Sistema** Concede permissão para acessar todos os domínios da interface com o usuário. Os usuários que têm esse acesso não pode editar outras contas do administrador.
Ofensas	Concede o acesso a todas as funções na guia **Ofensas** . Você pode conceder permissões específicas : **Designar Crimes a Usuários** Concede permissão para designar ofensas a outros usuários. **Manter Regras Customizadas** Concede permissão para criar e editar regras customizadas. **Gerenciar Motivos de Encerramento de Crime** Concede permissão para gerenciar ofensas de razões de fechamento. **Visualizar Regras Customizadas** Concede permissão para visualizar regras customizadas. Se concedidas a uma função de usuário que não terá também a permissão **Manter regras customizadas** , a função do usuário não pode criar ou editar regras customizadas.

Tabela 1. Descrição da janela Gerenciamento de Função de Usuário parâmetros (continuação)

Parâmetro	Descrição
Atividade do Log	Concede acesso a funções na guia **Atividade de Log** . Você também pode conceder permissões específicas : **Manter Regras Customizadas** Concede permissão para criar ou editar regras que são exibidos na guia **Atividade de Log** . **Gerenciar Série Temporal** Concede permissão para configurar e visualizar gráficos de dados série temporal. **Propriedades de Eventos Definidas pelo Usuário** Concede permissão para criar propriedades de evento customizado. Para obter informações adicionais sobre propriedades de eventos customizados, consulte a *Guia do Usuário* para seu produto. **Visualizar Regras Customizadas** Concede permissão para visualizar regras customizadas. Se concedidas a uma função de usuário que não terá também a permissão **Manter regras customizadas** , a função do usuário não pode criar ou editar regras customizadas.
Recursos	**Nota:** Esta permissão é exibida somente se IBM Security QRadar Vulnerability Manager for instalado em seu sistema. Concede acesso à função na guia **Ativos** . Você pode conceder permissões específicas : **Desempenhe VA Varreduras** Concede permissão para concluir varreduras de avaliação de vulnerabilidades. Para obter informações adicionais sobre de avaliação de vulnerabilidades, consulte a guia *Gerenciando Avaliação de Vulnerabilidades*. **Remover Vulnerabilidades** Concede permissão para remover as vulnerabilidades de ativos. **Servidor Discovery** Concede permissão para descobrir servidores. **Visualização VA Data** Concede permissão aos dados de avaliação de vulnerabilidades. Para obter informações adicionais sobre de avaliação de vulnerabilidades, consulte o *Gerenciando guia Avaliação de Vulnerabilidades*.
Atividade da Rede	Concede acesso a todas as funções na guia **Atividade de Rede** . Você pode conceder acesso específico para as seguintes permissões: **Manter Regras Customizadas** Concede permissão para criar ou editar regras que são exibidos na guia **Atividade de Rede** . **Gerenciar Série Temporal** Concede permissão para configurar e visualizar gráficos de dados série temporal. **Visualizar Regras Customizadas** Concede permissão para visualizar regras customizadas. Se a função do usuário não terá também a permissão **Manter regras customizadas** , a função do usuário não pode criar ou editar regras customizadas.
Relatórios	Concede permissão para acesso a todas as funções no guia **Relatórios** . Você pode conceder aos usuários permissões específicas : **Distribuir Relatórios por E-mail** Concede permissão para distribuírem relatórios por meio de email. **Manter Gabaritos** Concede permissão para editar os modelos de relatório.
Gerenciador de Vulnerabilidade	Concede permissão para QRadar Vulnerability Manager função. IBM Security QRadar Vulnerability Manager deve ser ativada. Para obter informações adicionais, consulte *IBM Security QRadar Vulnerability Manager User Guide*.

Tabela 1. Descrição da janela Gerenciamento de Função de Usuário parâmetros (continuação)

Parâmetro	Descrição
Forense	Concede permissões para os recursos do QRadar Incident Forensics. **Crie casos no Resposta a Insidentes** Concede permissões para criar casos para coleções de documentos importados e arquivos pcap.
Clique com o botão direiro em extensões IP	Concede permissão para opções incluídas no menu de atalho.
Configuração de plataforma	Concede permissão para serviços **Configuração de Plataforma** .

Parâmetros de perfil de segurança

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

Tabela 2. Parâmetros da janela Gerenciamento de perfil de segurança

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

Parâmetros da janela de gerenciamento do usuário

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

Tabela 3. Parâmetros da janela de gerenciamento do usuário

Parâmetro	Descrição
Nome de usuário	Exibe o nome do usuário desta conta do usuário.
Descrição	Exibe a descrição da conta do usuário.
e-mail	Exibe o endereço de e-mail desta conta do usuário.
Função de usuário	Exibe a função do usuário que está designada a esta conta de usuário. Funções do usuário definem quais ações o usuário tem permissão para executar.
Perfil de Segurança	Exibe o perfil de segurança que é designado a esta conta de usuário. Perfis de Segurança definem quais dados o usuário tem permissão para acessar.

Parâmetros da janela Detalhes do Usuário

parâmetros da janela Detalhes do Usuário

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

Tabela 4. Parâmetros da janela Detalhes do Usuário

Parâmetro	Descrição
Nome de usuário	Digite um nome de usuário exclusivo para o novo usuário. O nome de usuário deve conter no máximo 30 caracteres.
e-mail	Digite o endereço de e-mail do usuário. O endereço de e-mail deve atender aos seguintes requisitos: • Deve ser um endereço de e-mail válido • Mínimo de 10 caracteres • Máximo de 255 caracteres
Senha	Digite uma senha para o usuário para obter acesso. A senha deve atender aos seguintes critérios: • Mínimo de 5 caracteres • Máximo de 255 caracteres

Tabela 4. Parâmetros da janela Detalhes do Usuário (continuação)

Parâmetro	Descrição
Confirme a senha	Digite a senha novamente para confirmação.
Descrição	`Opcional.` Digite uma descrição para a conta do usuário. O número máximo de caracteres é 2.048.
Função de usuário	Na caixa de listagem, selecione a função do usuário que você deseja designar para este usuário.
Perfil de Segurança	Na caixa de listagem, selecione o perfil de segurança que você quer designar para este usuário.

Capítulo 2. Configurar QRadar

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

É possível configurar sua hierarquia de rede, as atualizações automáticas, as configurações do sistema, os depósitos de retenção de eventos, as , as configurações do console, os motivos do fechamento de ofensas e o gerenciamento de índice.

Hierarquia de Rede

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

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

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

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

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

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

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

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

Tabela 5. Exemplo de CIDRs múltiplos e sub-redes em um único grupo de rede

Grupo	Descrição	endereços IP
1	Marketing	10.10.5.0/24
2	Venda	10.10.8.0/21

Tabela 5. Exemplo de CIDRs múltiplos e sub-redes em um único grupo de rede (continuação)

Grupo	Descrição	endereços IP
3	Cluster do banco de dados	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32

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

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

Tabela 6. Exemplo de um grupo global

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

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

Valores CIDR aceitáveis

QRadaraceita valores CIDR específicos.

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

Tabela 7. Valores CIDR aceitáveis

Comprimento CIDR	máscara	Número de Redes	Hosts
/1	128.0.0.0	128 A	2.147.483.392
/2	192.0.0.0	64 A	1.073.741.696
/3	224.0.0.0	32 A	536.870.848
/4	240.0.0.0	16 A	268.435.424
/5	248.0.0.0	8 A	134.217.712
/6	252.0.0.0	4 A	67.108.856
/7	254.0.0.0	2 A	33.554.428
/8	255.0.0.0	1 A	16.777.214
/9	255.128.0.0	128 B	8.388.352
/10	255.192.0.0	64 B	4.194.176
/11	255.224.0.0	32 B	2.097.088
/12	255.240.0.0	16 B	1.048.544
/13	255.248.0.0	8 B	524.272
/14	255.252.0.0	4 B	262.136
/15	255.254.0.0	2 B	131.068
/16	255.255.0.0	1 B	65.534
/17	255.255.128.0	128 C	32.512
/18	255.255.192.0	64 C	16.256
/19	255.255.224.0	32 C	8.128
/20	255.255.240.0	16 C	4.064
/21	255.255.248.0	8 C	2.032
/22	255.255.252.0	4 C	1.016
/23	255.255.254.0	2 C	508
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 sub-redes	124
/26	255.255.255.192	4 sub-redes	62
/27	255.255.255.224	sub-8	30

Tabela 7. Valores CIDR aceitáveis (continuação)

Comprimento CIDR	máscara	Número de Redes	Hosts
/28	255.255.255.240	sub-16	14
/29	255.255.255.248	sub-32	6
/30	255.255.255.252	sub-64	2
/31	255.255.255.254	nenhum	nenhum
/32	255.255.255.255	1/256 C	1

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

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

  Intervalo do Host de sub-rede

  0 192.0.0.1-192.0.0.126

  1 192.0.0.129-192.0.0.254
- /26 192.0.0.0

  Intervalo do Host de sub-rede

  0 192.0.0.1 – 192.0.0.62

  1 192.0.0.65 – 192.0.0.126

  2 192.0.0.129 – 192.0.0.190

  3 192.0.0.193 – 192.0.0.254
- 192.0.0.0 /27

  Intervalo do Host de sub-rede

  0 192.0.0.1 – 192.0.0.30

  1 192.0.0.33 - 192.0.0.62

  2 192.0.0.65 – 192.0.0.94

  3 192.0.0.97 – 192.0.0.126

  4 192.0.0.129 – 192.0.0.158

  5 192.0.0.161 – 192.0.0.190

  6 192.0.0.193 – 192.0.0.222

  7 192.0.0.225 – 192.0.0.254

Tarefas relacionadas:

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

Definindo sua Hierarquia de Rede

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

Sobre Esta Tarefa

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

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

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

Procedimento

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

Conceitos relacionados:

"Valores CIDR aceitáveis" na página 6
QRadaraceita valores CIDR específicos.

Endereçamento IPv6 em implementações de QRadar

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

Revise os detalhes a seguir sobre endereçamento IPv6.

"Componentes do QRadar que suportam endereçamento IPv6" na página 9

"Implementando QRadar em ambientes IPv6 ou mistos" na página 9

“Limitações de endereçamento IPv6 ” na página 10

Componentes do QRadar que suportam endereçamento IPv6

Os componentes do QRadar a seguir suportam endereçamento IPv6:

Guia Atividade de Rede

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

Para economizar espaço e indexar em um ambiente de origem IPv4 ou IPv6, campos de endereço IP extra não são armazenadas ou exibidos.

Guia Atividade de Log

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

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

Procurando, agrupamento e relatando campos IPv6

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

Regras Customizadas

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

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

Editor de implementação

O editor de implementação suporta endereços IPv6.

Módulos de suporte de dispositivos (DSMs)

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

Implementando QRadar em ambientes IPv6 ou mistos

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

```
https://[<Endereço IP>]
```

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

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

Limitações de endereçamento IPv6

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

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

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

Instalando um host gerenciado somente IPv4 em um ambiente misto

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

Procedimento

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

Retenção de Dados

Configure o período de retenção customizada para datas específicas.

depósitos de retenção define as políticas de retenção para eventos que correspondem aos requisitos do filtro customizado. Como QRadar recebe eventos, cada evento é comparado com os critérios de filtragem depósito de retenção. Quando um evento corresponder a um filtro de depósito de retenção, o mesmo será armazenado no depósito de retenção até que o período da política de retenção seja alcançado. Esse recurso permite a configuração de múltiplos depósitos de retenção.

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

Configurando depósitos de retenção

Por padrão, a janela Retenção de Evento fornece um depósito de retenção padrão e 10 depósitos de retenção não configurados. Até que se configure um depósito de retenção, todos os eventos são armazenados no depósito de retenção padrão.

Sobre Esta Tarefa

A janela Retenção de Evento fornece as informações a seguir para cada depósito de retenção :

Tabela 8. janela parâmetros de retenção

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

A barra de ferramentas fornece as seguintes funções:

Tabela 9. Barra de ferramentas da janela Retenção

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

Procedimento

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

Parâmetro	*Descrição*
Nome	Digite um nome exclusivo para o depósito de retenção.
Mantenha dados colocados nesse depósito para	Selecione um período de retenção. Quando o período de retenção for atingido, os dados são excluídos de acordo com o parâmetro *Excluir dados neste depósito*.

Parâmetro	*Descrição*
Permite que dados neste depósito sejam compactados.	Selecione a caixa de opção para ativar a compactação de dados e, em seguida, selecione um intervalo de tempo na caixa de listagem. Quando o quadro de tempo for atingido, todos os dados no depósito de retenção são elegíveis para serem compactadas. Isso aumenta a performance do sistema pela garantia que não há compressão de dados dentro do período específico. A compactação ocorre apenas quando o espaço em disco utilizado atingir 83% para cargas úteis e 85% para registros.
Excluir dados neste depósito	Selecione uma política de exclusão. Selecione **Quando o espaço de armazenamento é necessário** se você desejar dados que correspondam ao parâmetro *Mantenha dados colocados no depósito para esta* para permanecer no armazenamento até que o sistema de monitoramento detecte que o armazenamento em disco é necessário. Se o espaço em disco utilizado atingir 85% para registros e 83% para cargas úteis, os dados serão excluídos. A exclusão continua até que o espaço em disco utilizado atingir 82% para registros e 81% para cargas úteis. Selecione **Imediatamente após o período de retenção ter expirado** se você deseja que os dados sejam excluídos imediatamente na correspondência do **Mantenha dados colocados no depósito para este parâmetro**. Os dados são excluídos no processo de manutenção do disco próxima planejada, independentemente do espaço livre em disco e requisitos de compactação. Quando de armazenamento é necessário, apenas os dados que corresponde ao **Mantenha dados colocados no depósito** para este parâmetro ser excluído.
Descrição	Digite uma descrição para o depósito de retenção.
Filtros Atuais	Configure seus filtros. Na primeira lista, selecione um parâmetro que você deseja filtrar. Por exemplo, Dispositivo, Porta de Origem, ou Nome do Evento. Na segunda lista, selecione o modificador que deseja utilizar para o filtro. A lista de modificadores depende do atributo selecionado na primeira lista. No campo de texto, digite informações específicas relacionadas a seu filtro e, em seguida, clique em **Incluir Filtro**. Os filtros são exibidos na caixa de texto **Filtros atuais**. Você pode selecionar um filtro e clicar em **Remover Filtro** para remover um filtro da caixa de texto **Filtrar Atual**.

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

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

Gerenciando Sequência de Depósito de Retenção

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

Sobre Esta Tarefa

depósitos de retenção serão colocados em ordem de prioridade a partir da fileira de cima a linha inferior na janela de Retenção de Evento. Um registro é armazenado no primeiro depósito de retenção que corresponde aos parâmetros de registro.

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

Procedimento

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

Editando um Depósito de Retenção

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

Sobre Esta Tarefa

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

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados**.
3. Escolha uma das seguintes opções:
4. Clique no ícone **Retenção de Evento**.
5. Selecione o depósito de retenção que você deseja editar e, em seguida, clique em **Editar**.
6. Edite os parâmetros. Para obter informações adicionais, consulte “Configurando depósitos de retenção” na página 11.
7. Clique em **Salvar**.

Ativando e Desativando um Depósito de Retenção

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

Sobre Esta Tarefa

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

Procedimento

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

Excluindo um Depósito de Retenção

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

Procedimento

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

Razões customizadas para encerramento de ofensas

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

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

- Ajuste falso-positivo
- Sem problema
- Violação de Política

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

Incluindo um motivo de ofensa customizada

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

Sobre Esta Tarefa

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

Tabela 10. Parâmetros customizados de janelas motivos para encerramento.

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

Procedimento

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

Editando Motivo Fechamento da Ofensa Customizado

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

Procedimento

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

Excluindo um Motivo de Fechamento de Ofensa Customizado

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

Procedimento

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

Configurando uma propriedade de recurso customizado

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

Procedimento

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

Gerenciando Visualizações de Dados Agregados

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

Sobre Esta Tarefa

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

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

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

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

Procedimento

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

Tabela 11. Visualização Gerenciamento de Dados Agregados descrições de colunas

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

Capítulo 3. Gerenciamento de conjuntos de referência

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

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

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

Incluindo um conjunto de referência

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

Sobre Esta Tarefa

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

Procedimento

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

Tabela 12. Parâmetros do Conjunto de Referência

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

3. Clique em **Criar**.

Editando um Conjunto de Referência

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

Procedimento

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

Tabela 13. Parâmetros do Conjunto de Referência

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

4. Clique em **Enviar**.

Excluindo Conjuntos de Referência

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

Sobre Esta Tarefa

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

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

Procedimento

Escolha uma das seguintes opções:

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

Visualizando o Conteúdo em um Conjunto de Referência

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

Procedimento

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

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

Tabela 14. Parâmetros da Guia Conteúdo

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

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

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

Tabela 15. Parâmetros da Guia Conteúdo

Parâmetro	Descrição
Nome da Regra	O nome desta regra.
Grupo	O nome do grupo ao qual esta regra pertence.
Categoria	A categoria da regra. As opções incluem **Regra Customizada** ou **Regra de Detecção de Anomalia**.
Tipo	O tipo desta regra.
Ativado	Indica se a regra está ativada ou desativada.
Resposta	As respostas que estão configuradas para esta regra.
Origem	**Sistema** indica uma regra padrão. **Modificado** indica que uma regra padrão foi customizada. **Usuário** indica uma regra criada pelo usuário.

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

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

Incluindo um Elemento em um conjunto de referência

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

Procedimento

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

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

6. Clique em **Incluir**.

Excluindo Elementos de um Conjunto de Referência

É possível excluir elementos de um conjunto de referência.

Procedimento

1. Na janela Gerenciamento do Conjunto de Referência, selecione um conjunto de referência.
2. Clique em **Visualizar Conteúdo**.
3. Clique na guia **Conteúdo**.
4. Escolha uma das seguintes opções:
   - Selecione um elemento e, em seguida, clique em **Excluir**.
   - Utilize a caixa de texto **Procura Rápida** para exibir apenas os elementos que você deseja excluir e, em seguida, clique em **Excluir Listados**.
5. Clique em **Excluir**.

Importando Elementos em um Conjunto de Referência

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

Antes de Iniciar

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

Procedimento

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

Exportando Elementos a Partir de um Conjunto de Referência

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

Procedimento

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

Capítulo 4. Coleções dos dados de referência

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

É possivel criar os segiuntes tipos de dados de referências:

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

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

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

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

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

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

Os requisitos do arquivo CSV para coletas de dados de referência

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

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

Exemplo 1: mapa de Referência

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

Exemplo 2: mapa de conjuntos de Referência

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

Exemplo 3: Mapa de referencia de mapas

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

Example 3: Reference table

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

Criando uma Coleção de Dados de Referência

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

Procedimento

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

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

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

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

Exemplo

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

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

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

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

O que Fazer Depois

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

Referência de comando ReferenceDataUtil.sh

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

criar

Cria uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

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

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

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

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

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

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

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

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

update

Cria uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

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

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

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

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

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

adicionar

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

name
O nome da coleta de dados de referência.

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

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

excluir

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

name
O nome da coleta de dados de referência.

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

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

remover

Remove uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

limpar

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

name
O nome da coleta de dados de referência.

list

Lista elementos em uma coleta de dados de referência.

name
O nome da coleta de dados de referência.

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

listall

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

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

carregamento

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

name
O nome da coleta de dados de referência.

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

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

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

Capítulo 5. Descoberta do servidor

A função **Descoberta do Servidor** usa o ativo banco de dados do perfil para descobrir deferentes tipos de servidores que são baseados em definições de portas. Assim, é possível selecionar os servidores para adicionar um servidor-tipo building blocks para regras.

A função **Descobrindo Servidores**é baseada em servidores-tipo building block. Portas são usadas para definir o tipo de servidor. Desta forma, o servidor tipo building block trabalha como filtro port-based quando você busca pelo banco de dados perfil de recurso.

Para mais informações sobre building blocks, consulte o *IBM Security QRadar SIEM Users Guide*.

Descobrindo Servidores

Utilize a guia **Ativos** para descobrir servidores em sua rede.

Procedimento

1. Clique na guia **Ativos**
2. No menu de navegação, clique em **Descoberta do Servidor**.
3. Na lista **Tipo de Servidor**, selecione o tipo de servidor que você deseja descobrir.
4. Selecione uma das seguintes opções para determinar os servidores que você deseja descobrir:
   - Para utilizar o **Tipo de Servidor** atualmente selecionado para procurar todos os servidores em sua implementação, selecione **Todos**.
   - Para procurar servidores em sua implementação que foram designados para o **Tipo de Servidor** atualmente selecionado, selecione **Designados**.
   - Para procurar servidores em sua implementação que não estão designados, selecione **Não Designados**.
5. A partir da lista **Rede**, selecione a rede que você deseja procurar.
6. Clique em **Descobrir Servidores**.
7. Na tabela **Servidores Correspondentes**, selecione as caixas de seleção de todos os servidores que você deseja designar à função de servidor.
8. Clique em **Aprovar Servidores Selecionados**.

Capítulo 6. Categorias de Evento

Categorias de eventos são usadas para agrupar eventos de recebimento para processamento pelo IBM Security QRadar. As categorias de eventos são pesquisáveis e ajudam a monitorar sua rede.

Eventos que ocorrem em sua rede são agregados em categorias de alto nível e de baixo nível. Cada categoria de alto nível contém categorias de baixo nível e um nível de severidade associado. É possível rever os níveis de severidade que são designados para eventos e ajustá-los às suas necessidades de política corporativa.

Categorias de eventos de alto nível

Eventos em QRadar origens de log são agrupados em categorias de alto nível. Cada evento é atribuído a uma categoria de alto nível específico.

Categorizando os eventos de entrada assegura que você pode procurar facilmente os dados.

A tabela a seguir descreve as opções de comando.

Tabela 16. Categorias de eventos de alto nível

Categoria	Descrição
"Recon" na página 34	Eventos que são relacionados à varredura e outras técnicas que são utilizados para identificar os recursos de rede, por exemplo, rede ou host varreduras de porta.
"DoS" na página 34	Eventos que são relacionados ao serviço (DoS) ou ataques de negação distribuído (DDoS) em relação a serviços ou hosts, por exemplo, força bruta rede contra ataques DoS.
"Autenticação" na página 36	Eventos que são relacionadas a controles de autenticação, grupo ou alterar privilégio, por exemplo, efetuar login ou logout.
"Acesso" na página 39	Eventos resultante de uma tentativa para acessar os recursos de rede, por exemplo, aceitar ou negar firewall.
"Explorar" na página 40	Events that are related to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.
"Malware" na página 41	Eventos que são relacionados ao vírus, Tróia, atentados a porta traseira, ou outras formas de software hostil. Eventos malware pode incluir um vírus, Tróia, software mal-intencionado, ou spyware.
"Atividade Suspeita" na página 42	A natureza da ameaça é desconhecida, mas o comportamento é suspeito. A ameaça potencialmente anomalias protocolo pode indicar evasivo técnicas que incluem, por exemplo, pacote ou técnicas de fragmentação sonegação sistema de detecção de intrusão conhecido (IDS).
"Sistema" na página 44	Os eventos que são relacionados a alterações do sistema, instalação de software, ou mensagens de status.
"Política" na página 46	Eventos corporativo ou uso indevido sobre violações de política.
"Desconhecido" na página 47	Os eventos que estão relacionados com a actividade desconhecido em seu sistema.
"CRE" na página 47	Os eventos que são gerados a partir de um ou ofensa evento de regra.
"Exploração Potencial" na página 48	Eventos relacionados ao aplicativo explora potencial e as tentativas de estouro de buffer.
"Usuário definido" na página 48	Eventos que são relacionados aos objetos definido pelo usuário.
"SIM de auditoria" na página 50	Eventos que são relacionadas à interação do usuário com o Console e as funções administrativas.
"Descoberta do Host VIS" na página 50	Eventos que são relacionados ao host, portas, ou as vulnerabilidades que o componente VIS descobre.
"Aplicação" na página 50	Os eventos que estão relacionados com a actividade de auditoria.
"Auditoria" na página 62	Os eventos que estão relacionados com a actividade de auditoria.
"Risco" na página 62	Eventos que são relacionados com a actividade risco em IBM Security QRadar Risk Manager.

Tabela 16. Categorias de eventos de alto nível (continuação)

Categoria	Descrição
"Gerenciador de risco de auditoria" na página 63	Eventos que são relacionados com a actividade de auditoria em IBM Security QRadar Risk Manager.
"Controle" na página 63	Eventos que são relacionados ao seu hardware do sistema.
"Gerenciadores de perfis ativos" na página 64	Eventos que são relacionados aos perfis de ativos.

Recon

A categoria Recon contém eventos que estão relacionados à varredura e outras técnicas que são utilizados para identificar os recursos de rede.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados a categoria recon.

Tabela 17. categorias de baixo nível e níveis de gravidade para a categoria de eventos Recon

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Forma Desconhecida de Recon	Uma forma de reconhecimento desconhecido.	2
Consulta do Aplicativo	Reconhecimento de aplicativos em seu sistema.	3
Consulta de Host	Reconhecimento para um host em sua rede.	3
Tempo de Acesso da Rede	Reconhecimento em sua rede.	4
Reconhecimento de Correio	Reconhecimento em seu sistema de correio.	3
Windows Reconhecimento	Reconhecimento para o sistema operacional Windows.	3
Portmap / RPC r\Request	Reconhecimento em sua solicitação de RPC ou portmap.	3
Varredura de Porta do Host	Indica que uma varredura ocorreu nas portas do host.	4
Dump do RPC	Indica que as informações RPC (Remote Procedure Call) é removido.	3
Reconhecimento do DNS	Reconhecimento nos servidores DNS.	3
Reconhecimento de Eventos Diversoa	Diversos eventos de reconhecimento.	2
Reconhecimento da Web	reconhecimento da Web em sua rede.	3
Reconhecimento do Banco de Dados	reconhecimento do Banco de Dados em sua rede.	3
Reconhecimento do ICMP	Reconhecimento no tráfego ICMP.	3
Reconhecimento do UDP	Reconhecimento no tráfego UDP.	3
Reconhecimento do SNMP	Reconhecimento sobre o tráfego SNMP.	3
Consulta do Host ICMP	Indica uma consulta do host ICMP.	3
Consulta do Host UDP	Indica uma consulta do host UDP.	3
Reconhecimento do NMAP	Indica de reconhecimento do NMAP.	3
Reconhecimento do TCP	Indica de reconhecimento TCP em sua rede.	3
Reconhecimento do UNIX	Reconhecimento em sua rede UNIX.	3
Reconhecimento do FTP	Indica de reconhecimento de FTP.	3

DoS

A categoria contém eventos que estão relacionados aos ataques DoS de serviço (DoS) em relação a serviços ou hosts.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de gravidade associado para a categoria DoS.

Tabela 18. categorias de baixo nível e níveis de severidade para a categoria DoS eventos

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ataque DoS Desconhecido	Indica um ataque DoS desconhecido.	8
DoS do ICMP	Indica um ataque de ICMP DoS.	9
DoS do TCP	Indica um ataque DoS banco de dados.	9

Tabela 18. categorias de baixo nível e níveis de severidade para a categoria DoS eventos (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
DoS do UDP	Indica um ataque DoS do UDP.	9
DoS do Serviço DNS	Indica um ataque DoS do serviço DNS.	8
DoS do Serviço da Web	Indica um ataque DoS do serviço da Web.	8
DoS do Serviço de Correio	Indica um ataque DoS do servidor de correio.	8
DoS Distribuído	Indica um ataque DoS distribuído.	9
DoS Diverso	Indica um ataque diversos DoS.	8
UNIX DoS	Indica um ataque UNIX DoS.	8
Windows DoS	Indica um ataque Windows DoS.	8
DoS do Banco de Dados	Indica um ataque DoS banco de dados.	8
DoS do FTP	Indica um ataque DoS do FTP.	8
DoS de Infraestrutura	Indica um ataque DoS na infra-estrutura.	8
DoS do Telnet	Indica um ataque DoS do Telnet.	8
Força bruta Login	Indica acesso ao seu sistema por meio de métodos não autorizados.	8
Taxa Alta TCP DoS	Indica uma alta taxa de TCP DoS do ataque.	8
Taxa Alta de DoS do UDP	Indica uma alta taxa de DoS do UDP ataque.	8
Taxa Alta DoS do ICMP	Indica uma alta taxa de ataque distribuído DoS do ICMP.	8
Taxa Alta DoS	Indica um ataque DoS taxa alta.	8
DoS do TCP Taxa média	Indica um ataque TCP taxa média.	8
DoS do UDP Taxa média	Indica um ataque UDP taxa média.	8
Taxa de DoS do ICMP Médio	Indica um ataque de ICMP taxa média.	8
DoS Taxa Média	Indica um ataque DoS taxa média distribuído.	8
DoS Taxa Média	Indica um ataque DoS taxa média distribuído.	8
Baixa Taxa de DoS do TCP	Indica uma baixa taxa TCP DoS ataque.	8
Baixa Taxa de DoS do UDP	Indica uma baixa taxa UDP DoS ataque.	8
Baixa Taxa de DoS do ICMP	Indica uma baixa taxa de ataque DoS do ICMP.	8
Baixa Taxa de DoS	Indica um ataque DoS taxa baixa.	8
Taxa Alta Distribuída DoS TCP	Indica uma taxa alta DoS do TCP ataque distribuído.	8
Distributed High Rate UDP DoS	Indica uma alta taxa de DoS do UDP ataque distribuído.	8
Distributed High Rate ICMP DoS	Indica uma alta taxa de ataque distribuído DoS do ICMP.	8
Taxa Alta DoS Distribuído	Indica um ataque distribuído de alta taxa de DoS.	8
Taxa DoS Distribuído Medium TCP	Indica uma taxa média TCP DoS do ataque distribuído.	8
Taxa DoS Distribuído Medium UDP	Indica uma taxa média UDP DoS ataque distribuído.	8
Taxa Média ICMP DoS Distribuído	Indica uma taxa baixa DoS do ICMP ataque distribuído.	8
Taxa Média DoS Distribuído	Indica um ataque DoS taxa média distribuído.	8
Baixa Taxa TCP DoS Distribuído	Indica uma baixa taxa de DoS do TCP ataque distribuído.	8
Baixa Taxa UDP DoS Distribuído	Indica uma baixa taxa de DoS do UDP ataque distribuído.	8
Baixa Taxa ICMP DoS Distribuído	Indica uma baixa taxa de ataque ICMP DoS distribuída.	8
Baixa Taxa de DoS Distribuído	Indica uma baixa taxa de DoS distribuída.	8
Taxa Alta de varredura TCP	Indica uma taxa alta de varredura TCP.	8
Taxa Média Varredura UDP	Indica uma varredura de UDP taxa alta.	8
Taxa Alta de varredura ICMP	Indica uma taxa alta de varredura ICMP.	8
Taxa Alta Varredura	Indica uma taxa alta de varredura.	8
Taxa média de varredura TCP	Indica que uma varredura de TCP taxa média.	8
Taxa Média Varredura UDP	Indica uma varredura de UDP taxa média.	8

Tabela 18. categorias de baixo nível e níveis de severidade para a categoria DoS eventos (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Taxa média de varredura ICMP	Indica que uma varredura de ICMP taxa média.	8
Taxa média de Varredura	Indica que uma varredura de taxa média.	8
Low Rate TCP Scan	Indica que uma varredura de TCP taxa baixa.	8
Baixa Taxa de UDP de Varredura	Indica uma varredura de UDP taxa baixa.	8
Baixa Taxa de ICMP de Varredura	Indica que uma varredura de ICMP taxa baixa.	8
Baixa Taxa de Varredura	Indica uma baixa taxa de varredura.	8
DoS VoIP	Indica um ataque VoIP DoS.	8
Estouro	Indica um ataque inundação.	8
TCP Inundação	Indica um ataque TCP Inundação.	8
UDP Flood	Indica um ataque flood UDP.	8
ICMP Flood	Indica um ataque ICMP flood.	8
SYN Flood	Indica um ataque SYN flood.	8
URG Flood	Indica um ataque flood com a urgência (URG) sinalizada.	8
SYN Flood URG	Indica um ataque flood com urgência (URG) sinalizada.	8
SYN Flood FIN	Indica um ataque flood SYN FIN.	8
SYN Flood ACK	Indica um ataque flood SYN ACK.	8

Autenticação

A acrtegoria autenticação contêm eventos que estão relacionados a autenticação, sessões e controles de acesso que monitora usuários na rede.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de autenticação.

Tabela 19. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Autenticação Desconhecida	Indica de autenticação desconhecida.	1
Login do Host Bem-sucedido	Indica um login do host bem-sucedido.	1
Login do Host com Falha	Indica que o login do host falhou.	3
Login Diverso Bem-sucedido	Indica que a sequência de login foi bem-sucedida.	1
Login Diverso com Falha	Indica que a sequência de login falhou.	3
Escalação de Privilégio com Falha	Indica que a escalação privilegiada falhou.	3
Escalação de Privilégio Bem-sucedida	Indica que a escalação de privilégio ocorreu com êxito.	1
Login de Serviço de Correio Bem-sucedido	Indica que o serviço de correio de login foi bem-sucedida.	1
Login de Serviço de Correio com Falha	Indica que o login de serviço de correio falhou.	3
Login de Servidor de Autenticação com Falha	Indica que o login do servidor de autenticação falhou.	3
Login de Servidor de Autenticação Bem-sucedido	Indica que o servidor de autenticação de login obteve êxito.	1
Login de Serviço da Web Bem-sucedido	Indica que o serviço da Web de login obteve êxito.	1
Login de Serviço da Web com Falha	Indica que o login de serviço da web falhou.	3
Login de Administrador Bem-sucedido	Indica que um login administrativo foi bem-sucedido.	1
Login de Administrador com Falha	Indica que o login do SSH falhou.	3
Nome de Usuário Suspeito	Indica que um usuário tentou acessar a rede utilizando um nome de usuário incorreto.	4
Login com padrões de nome/ senha bem-sucedidos	Indica que um usuário acessou a rede utilizando o nome de usuário e senha padrão.	4

Tabela 19. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Login com padrões de nome de usuário/ senha falhou	Indica que um usuário foi mal-sucedido ao acessar a rede utilizando o nome de usuário e senha padrão.	4
Login de FTP Bem-sucedido	Indica que o login de FTP foi bem-sucedido.	1
Login de FTP com Falha	Indica que o login de FTP falhou.	3
Login de SSH Bem-sucedido	Indica que o login do SSH foi bem-sucedido.	1
Falha de Login de SSH	Indica que o login do SSH falhou.	2
Direito de Usuário Designado	Indica que o acesso do usuário a recursos de rede foi concedido com êxito.	1
Direito de Usuário Removido	Indica que o acesso do usuário a recursos de rede foi removido com êxito.	1
Domínio Confiável Incluído	Indica que um domínio confiável foi adicionado com êxito à sua implementação.	1
Domínio Confiável Removido	Indica que um domínio confiável foi removida de sua implementação.	1
Acesso de Segurança do Sistema Concedido	Indica que o acesso de segurança do sistema foi concedido com êxito.	1
Acesso de Segurança do Sistema Removido	Indica que o acesso de segurança do sistema foi removido com êxito.	1
Política Incluída	Indica que uma política foi incluída com êxito.	1
Mudança de Política	Indica que uma política foi alterada com êxito.	1
Conta do Usuário Incluída	Indica que uma conta de usuário foi incluída com êxito.	1
Conta do Usuário Alterada	Indica uma alteração em uma conta de usuário existente.	1
Mudança de Senha com Falha	Indica que uma tentativa de alterar uma senha existente falhou.	3
Mudança de Senha Bem-sucedida	Indica que uma mudança de senha foi bem-sucedida.	1
Conta do Usuário Removida	Indica que uma conta do usuário foi removida com êxito.	1
Membro do Grupo Incluído	Indica que um membro do grupo foi incluído com êxito.	1
Membro do Grupo Removido	Indica que um membro do grupo foi removido.	1
Grupo Incluído	Indica que um grupo foi incluído com êxito.	1
Grupo Alterado	Indica uma alteração em um grupo existente.	1
Grupo Removido	Indica que um grupo foi removido.	1
Conta do Computador Incluída	Indica que uma conta do computador foi incluída com êxito.	1
Conta do Computador Alterada	Indica uma alteração em uma conta do computador existente.	1
Conta do Computador Removida	Indica que uma conta do computador foi removida com êxito.	1
Login de Acesso Remoto Bem-sucedido	Indica que o acesso a rede usando um login remoto foi concluído com sucesso.	1
Login de Acesso Remoto com Falha	Indica que uma tentativa de acessar a rede usando um login remoto falhou.	3
Autenticação Geral Bem-sucedida	Indica que o processo de autenticação foi bem-sucedida.	1
Autenticação Geral com Falha	Indica que o processo de autenticação falhou.	3
Login do Telnet Bem-sucedido	Indica que o login de telnet foi bem-sucedida.	1
Login do Telnet com Falha	Indica que o login de Telnet falhou.	3
Senha Suspeita	Indica que um usuário tentou efetuar login utilizando uma senha suspeita.	4
Login de Administrador Bem-sucedido	Indica que um usuário efetuou login com êxito no utilizando o Samba.	1
Login do Samba com falha	Indica um usuário falhou ao efetuar login utilizando Samba.	3
Sessão do Servidor de Autenticação Aberta	Indica que uma sessão de comunicação com o servidor de autenticação foi iniciado.	1

Tabela 19. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão do Servidor de Autenticação Encerrada	Indica que uma sessão de comunicação com o servidor de autenticação foi fechada.	1
Sessão de Firewall Encerrada	Indica que uma sessão de firewall foi fechada.	1
Logout do Host	Indica que um host efetuou logout com êxito.	1
Logout Diverso	Indica que um usuário efetuou logout com êxito.	1
Logout do Servidor de Autenticação	Indica que o processo para efetuar logout do servidor de autenticação foi bem-sucedido.	1
Logout do Serviço da Web	oIndica que o processo para efetuar logout do serviço da Web foi bem-sucedido.	1
Logout Admin	Indica que o usuário administrativo efetuou logout com êxito.	1
Logout do FTP	Indica que o processo para efetuar logout do serviço de FTP foi bem-sucedido.	1
Logout do SSH	Indica que o processo para efetuar logout da sessão SSH foi bem-sucedido.	1
Logout de Acesso Remoto	Indica que o processo para efetuar logout do servidor de autenticação foi bem-sucedido.	1
Logout do Telnet	Indica que o processo para efetuar logout da sessão Telnet foi bem-sucedido.	1
Logout do Samba	Indica que o processo para efetuar logout do Samba foi bem-sucedido.	1
Início da Sessão SSH	Indica que a sessão de login do SSH foi iniciado em um host.	1
Conclusão de Sessão de Administrador	Indica o término de uma sessão de login do SSH em um host.	1
Sessão Admin Iniciada	Indica que uma sessão de login foi iniciada em um host, por um usuário administrativo, ou com privilégios de administrador.	1
Conclusão de Sessão de Administrador	Indica o término de uma sessão de administrador ou de usuários privilegiados em um host.	1
Login VoIP bem-sucedido	Indica um serviço de login de VoIP bem-sucedido	1
Falha de Login de VoIP	Indica uma tentativa mal-sucedida de acessar o serviço VoIP.	1
Logout de VoIP	Indica um logout do usuário,	1
Início de sessão de VoIP	Indica o início de uma sessão de VoIP.	1
Sessão VoIP finalizada	Indica o fim de uma sessão de VoIP.	1
Login Bem-sucedido banco de dados	Indica um login do banco de dados bem-sucedido.	1
Falha de Login do Banco	Indica que uma tentativa de login do banco de dados falhou.	3
Falha de Autenticação IKE	Indica que uma falha de autenticação Internet Key Exchange (IKE) foi detectada.	3
Aautenticação IKE Bem-sucedida	Indica que uma autenticação de IKE bem sucedida foi detectado.	1
Sessão Iniciada IKE	Indica que uma sessão do IKE foi iniciada.	1
Sessão IKE finalizada	Indica que uma sessão do IKE foi finalizada.	1
Erro de IKE	Indica uma mensagem de erro de IKE.	1
Status do IKE	Indica mensagem de status IKE.	1
Sessão Iniciada RADIUS	Indica que uma sessão RADIUS foi iniciada.	1
Sessão RADIUS finalizada	Indica uma sessão RADIUS foi finalizada.	1
Sessão RADIUS Negado	Indica que uma sessão RADIUS foi negada.	1
Status da Sessão RADIUS	Indica uma mensagem de status da sessão RADIUS.	1
Falha na Autenticação do RADIUS	Indica uma falha de autenticação RADIUS.	3
Autenticação RADIUS bem-sucedida	Indica uma autenticação RADIUS foi bem-sucedido.	1
Sessão TACACS iniciada	Indica uma sessão TACACS foi iniciada.	1
Sessão TACACS finalizada	Indica uma sessão TACACS foi finalizada.	1

Tabela 19. categorias de baixo nível e níveis de gravidade para a categoria de eventos de autenticação (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão TACACS negada	Indica que uma sessão TACACS foi negada.	1
Status da Sessão do TACACS	Indica uma mensagem de status da sessão TACACS.	1
Autenticação do TACACS bem-sucedida	Indica uma autenticação TACACS foi bem-sucedida.	1
Falha de autenticação do TACACS	Indica uma falha de autenticação TACACS.	1
Re-autenticação de host bem-sucedida	Indica que a re-autenticação de um host foi bem-sucedida.	1
Re-autenticação do Host com falha	Indica que a re-autenticação de um host falhou.	3
Estação de autenticação Bem-sucedido	Indica que o reassociação estação foi bem-sucedida.	1
Falha de autenticação da Estação	Indica que a estação de um host falhou.	3
Estação de associação de Bem-sucedido	Indica que a associação estação foi bem-sucedida.	1
Falha estação de associação	Indica que a associação estação falhou.	3
Estação de Autenticação Bem-sucedido	Indica que o reassociação de estação foi bem-sucedida.	1
Estação de Re-associação com falha	Indica que a associação estação falhou.	3
Desassociando do Host Bem-sucedido	Indica que o desassociando um host foi bem-sucedida.	1
Falha ao dessasociar o host	Indica que a desassociação de um host falhou	3
Erro SA	Indica mensagem de erro uma Associação de Segurança (SA).	5
Falha de Criação de SA	Indica falha na criação de uma Associação de Segurança (SA).	3
Estabelecida SA	Indica que a conexão uma Associação de Segurança (SA) estabelecido.	1
SA Rejeitado	Indica mensagem de erro uma Associação de Segurança (SA).	3
Deletando SA	Indica a exclusão de uma Associação de Segurança (SA).	1
A SA	Indica a criação de uma Associação de Segurança (SA).	1
Incompatibilidade de Certificado	Indica uma incompatibilidade de certificados.	3
Incompatibilidade de Credenciais	Indica uma incompatibilidade credenciais.	3
Tentativa de Login de Administrador	Indica uma tentativa de login admin.	2
Tentativa de Login do Usuário	Indica que uma tentativa de login do usuário.	2
Usuário de Login Bem-sucedido	Indica um login de usuário bem-sucedido.	1
Falha de Login do Usuário	Indica um login de usuário falhou.	3
Login SFTP Bem-sucedido	Indica uma com êxito o SSH File Transfer Protocol (SFTP) de login.	1
Falha de Login SFTP	Indica uma falha o SSH File Transfer Protocol (SFTP) de login.	3
Logout SFTP	Indica um logout o SSH File Transfer Protocol (SFTP).	1

Acesso

A categoria de acesso contém autenticação e controles de acesso que são utilizados para monitorar eventos de rede.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de acesso.

Tabela 20. Categorias de baixo nível e níveis de severidade para a categoria de eventos de acesso

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento de comunicação de rede desconhecida	Indica um evento de comunicação de rede desconhecida.	3

Tabela 20. Categorias de baixo nível e níveis de severidade para a categoria de eventos de acesso (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Permissão de firewall	Indica que o acesso ao firewall foi permitido.	0
Negação de firewall	Indica que o acesso ao firewall foi negado.	4
Evento de comunicação de rede diversa	Indica um evento de comunicações diversas.	3
Negação de IPS	Indica que o sistema de prevenção de instrusão (IPS) negou o tráfego.	4
Sessão de firewall aberta	Indica que a sessão firewall foi aberta.	0
Sessão de Firewall Encerrada	Indica que a sessão de firewall foi encerrada.	0
Conversão de endereço dinâmico bem-sucedida	Indica que a conversão de endereço dinâmico foi bem-sucedida.	0
Grupo de conversão não localizado	Indica que nenhum grupo de conversão foi localizado.	2
Autorização diversa	Indica que o acesso foi concedido a uma autenticação de diversos servidores.	2
Permissão de ACL	Indica que uma lista de controle de acesso (ACL) permitiu o acesso.	0
Negação de ACL	Indica que uma lista de controle de acesso negou o acesso.	4
Acesso permitido	Indica que o acesso foi permitido.	0
Acesso negado	Indica que o acesso foi negado.	4
Sessão aberta	Indica que uma sessão foi aberta.	1
Sessão fechada.	Indica que uma sessão foi fechada.	1
Sessão reconfigurada	Indica que uma sessão foi reconfigurada.	3
Seção encerrada	Indica que uma sessão foi permitida.	4
Sessão negada	Indica que uma sessão foi negada.	5
Sessão em andamento	Indica que uma sessão está em andamento.	1
Sessão atrasada	Indica que uma sessão está em atraso.	3
Sessão em fila	Indica que uma sessão estava em fila.	1
Entrada da sessão	Indica que uma sessão é de entrada.	1
Sessão de saída	Indica que uma sessão é de saída.	1
Tentativa de acesso não autorizado	Indica que uma tentativa de acesso não autorizado foi detectada.	6
Ação de aplicação diversa permitida	Indica que uma ação do aplicativo foi permitida.	1
Ação de aplicação diversa negada.	Indica que uma ação do aplicativo foi negada.	3
Ação do banco de dados permitida.	Indica que uma ação do banco de dados foi permitida.	1
Ação do banco de dados negada.	Indica que uma ação do banco de dados foi negada.	3
Ação de FTP permitida	Indica que uma ação de FTP foi permitida.	1
Ação de FTP negada	Indica que uma ação de FTP foi negeda.	3
Objeto em cache	Indica que um objeto foi armazenado em cache.	1
Objeto não armazenado em cache	Indica que um objeto não foi armazenado em cache.	1
Limite de taxa	Indica que o trafego de rede está em sua taxa limite.	4
Sem limite de taxa	Indica que a rede está sem taxa de tráfego limite.	0

Explorar

A categoria explorar contém eventos onde uma comunicação ou um acesso explorar ocorreu.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associado para explorar categoria.

Tabela 21. categorias de baixo nível e níveis de severidade para o explorar categoria de eventos

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ataque de Exploração Desconhecido	Indica um ataque exploit desconhecido.	9
Estouro de Buffer	Indica um estouro de buffer.	9
Exploração de DNS	Indica um DNS explorar.	9
Exploração de Telnet	Indica uma Telnet explorar.	9
Linux Explorar	Indica um explorar Linux.	9
UNIX Explorar	Indica um explorar UNIX.	9
Windows Explorar	Indica um Microsoft Windows explorar.	9
Exploração do Correio	Indica um servidor de correio explorar.	9
Exploração da Infraestrutura	Indica uma infra-estrutura de explorar.	9
Exploração Diversa	Indica uma exploração mista.	9
Exploração da Web	Indica uma explorador da web.	9
Interceptação de Sessão	Indica que uma sessão em sua rede foi extraordinário.	9
Worm Ativo	Indica um vírus ativo.	10
Dedução/Recuperação de Senha	Indica que um usuário solicitou acesso às suas informações de senha do banco de dados.	9
Exploração do FTP	Indica um servidor FTP explorar.	9
Exploração do RPC	Indica um RPC explorar.	9
Exploração do SNMP	Indica um SNMP explorar.	9
Exploração do NOOP	Indica um NOOP explorar.	9
Exploração do Samba	Indica um explorador Samba.	9
Exploração do Banco de Dados	Indica um explorador banco.	9
Exploração do SSH	Indica um SSH explorar.	9
Exploração do ICMP	Indica um ICMP explorar.	9
Exploração do UDP	Indica uma UDP explorar.	9
Exploração do Navegador	Indica uma exploração em seu navegador.	9
Exploração do DHCP	Indica um DHCP explorar.	9
Exploração de Acesso Remoto	Indicates a remote access exploit	9
Exploração do ActiveX	Indicates an exploit through an ActiveX application.	9
SQL Injection	Indica que uma injeção de SQL.	9
Cross-Site Scripting	Indica uma vulnerabilidade de script entre sites.	9
Vulnerabilidade de Sequência de Formatação	Indica uma vulnerabilidade da cadeia de formatação.	9
Exploração de Validação de Entrada	Indica que uma tentativa de explorar a validação de entrada foi detectado.	9
Remote Code Execution	Indica que uma tentativa de execução de código remota foi detectado.	9
Memória Distorção	Indica que um dano de memória explorar foi detectado.	9
Execução do Comando	Indicates that a remote command execution attempt was detected.	9

Malware

O software de categoria mal-intencionado a (malware) contém eventos que estão relacionados ao aplicativo e explora tentativas de estouro de buffer.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria malware.

Tabela 22. Categorias de baixo nível e níveis de severidade para categorias de eventos de malware.

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Malware Desconhecido	Indica um vírus desconhecido.	4
Porta dos Fundos Detectada	Indica que uma porta de volta para o sistema foi detectado.	9
Anexo de Correio Hostil	Indica um anexo de correio hostil.	6

Tabela 22. Categorias de baixo nível e níveis de severidade para categorias de eventos de malware. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Software Malicioso	Indica um vírus.	6
Download de Software Hostil	Indica um download de software hostil à sua rede.	6
Vírus Detectado	Indica que um vírus foi detectado.	8
Malware Diverso	Indica softwares maldosos diversos.	4
Cavalo de Troia Detectado	Indica que um trojam foi detectado.	7
Spyware Detectado	Indica que spyware foi detectado em seu sistema.	6
Varredura de conteúdo	Indica que uma tentativa de varredura de seu conteúdo foi detectado.	3
Falha de Varredura de Conteúdo	Indica que uma varredura de seu conteúdo falhou.	8
Varredura de conteúdo	Indica que uma varredura de seu conteúdo foi bem-sucedida.	3
Varredura de conteúdo em Andamento	Indica que uma varredura de seu conteúdo está em andamento.	3
Keylogger	Indica que um keylogger foi detectado.	7
Adware Detectado	Indica que Adware foi detectado.	4
Quarentena Bem-sucedida	Indicates that a quarantine action successfully completed.	3
Falha da Quarentena	Indica que uma ação de quarentena falhou.	8

Atividade Suspeita

categoria categoria suspeita contem eventos que estão relacionados a vírus, trojans, ataque as portas dos fundos, e outras formas de softwares hostis.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associadas à categoria da atividade suspeita.

Tabela 23. categorias de baixo nível e níveis de severidade para a categoria de eventos de atividades suspeitas

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento Suspeito Desconhecido	Indica um evento suspeito desconhecido.	3
Padrão Suspeito Detectado	Indica que um padrão suspeito foi detectado.	3
Conteúdo Modificado por Firewall	Indica que o conteúdo foi modificado pelo firewall.	3
Comando ou Dados Inválidos	Indica um comando ou dados inválidos.	3
Pacote Suspeito	Indica um pacote suspeito.	3
Atividade Suspeita	Indica atividade suspeita.	3
Nome do Arquivo Suspeito	Indica um nome de arquivo suspeito.	3
Atividade da Porta Suspeita	Indica atividade suspeita.	3
Roteamento Suspeito	Indica de roteamento suspeito.	3
Vulnerabilidade da Web Potencial	Indica da web vulnerabilidade em potencial.	3
Evento de Evasão Desconhecido	Indica um evento evasão desconhecido.	5
Spoof de IP	Indica um endereço IP. fraudam	5
Fragmentação de IP	Indica fragmentação de IP.	3
Sobrepondo Fragmentos de IP	Indica de sobreposição fragmentos IP.	5
Evasão do IDS	Indica uma evasão IDS.	5
Anomalia do Protocolo DNS	Indica um protocolo DNS anomalia.	3
Anomalia do Protocolo FTP	Indica um protocolo FTP anomalia.	3
Anomalia do Protocolo de Correio	Indica um protocolo de correio anomalia.	3
Anomalia do Protocolo de Roteamento	Indica um protocolo de roteamento anomalia.	3
Web Protocol Anomaly	Indica um protocolo da web anomalia.	3
Anomalia do Protocolo SQL	Indica um protocolo SQL anomalia.	3
Código Executável Detectado	Indica que um código executável foi detectado.	5

Tabela 23. categorias de baixo nível e níveis de severidade para a categoria de eventos de atividades suspeitas (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento Suspeito Diverso	Indica um evento suspeito diversos.	3
Fuga de Informações	Indicates an information leak.	1
Vulnerabilidade de Correio Potencial	Indica uma vulnerabilidade em potencial no servidor mail.	4
Vulnerabilidade de Versão Potencial	Indica uma vulnerabilidade em potencial na versão IBM Security QRadar SIEM.	4
Vulnerabilidade de FTP Potencial	Indica uma vulnerabilidade em potencial FTP.	4
Vulnerabilidade de SSH Potencial	Indica uma vulnerabilidade em potencial SSH.	4
Vulnerabilidade de DNS Potencial	Indica uma vulnerabilidade em potencial no servidor DNS.	4
Vulnerabilidade de SMB Potencial	Indica um potencial SMB (Samba) vulnerabilidade.	4
Vulnerabilidade de Banco de Dados Potencial	Indica uma vulnerabilidade em potencial no banco de dados.	4
Anomalia do Protocolo IP	Indica uma anomalia protocolo IP potencial	3
Endereço IP Suspeito	Indica que um endereço IP suspeita foi detectado.	2
Uso do Protocolo IP Inválido	Indica um protocolo IP inválido.	2
Protocolo Inválido	Indica um protocolo inválido.	4
Janela de eventos suspeitos	Indica um evento suspeito com uma tela em seu desktop.	2
Atividade suspeita de ICMP	Indica atividade suspeita ICMP.	2
Vulnerabilidade de NFS Potencial	Indica um sistema de arquivos de rede em potencial (NFS) vulnerabilidade.	4
Vulnerabilidade Potencial de NTTP	Indica uma potencial vulnerabilidade NNTP (Network News Transfer Protocol).	4
Potencial Vulnerabilidade de RPC	Indica uma potencial vulnerabilidade RPC.	4
Vulnerabilidade potencial de Telnet	Indica uma vulnerabilidade potencial de Telnet em seu sistema.	4
Vulnerabilidade potencial de SNMP	Indica uma vulnerabilidade em potencial SNMP.	4
Combinação de Sinalizador TCP Ilegal	Indica que uma combinação inválida de sinalizador TCP foi detectada.	5
Combinação de Sinalizador TCP Suspeita	Indica que uma combinação de sinalizador TCP potencialmente inválida foi detectada.	4
Uso de Protocolo ICMP Ilegal	Indica que um uso inválido do protocolo ICMP foi detectado.	5
Uso de Protocolo ICMP Suspeito	Indica que o uso do protocolo potencialmente inválido ICMP foi detectado.	4
Tipo de ICMP Ilegal	Indica que um tipo ICMP inválido foi detectado.	5
Código de ICMP Ilegal	Indica que um tipo ICMP inválido foi detectado.	5
Tipo de ICMP Suspeito	Indica que um tipo ICMP potencialmente inválido foi detectado.	4
Código de ICMP Suspeito	Indica que um código ICMP potencialmente inválido foi detectado.	4
porta TCP 0	Indica um pacote TCP utiliza uma porta reservada (0) para origem ou para destino.	4
Porta UDP 0	Indica um pacote UDP usa uma porta reservada (0) para orígem ou destino.	4
IP Hostil	Indica a utilização de um endereço IP hostil conhecido.	4
Lista de observação IP	Indica o uso de um endereço IP de uma lista de observação de endereços de IP.	4
IP ofensor conhecido	Indica a utilização de um endereço IP de um ofensor conhecido.	4
IP do RFC 1918 (privado)	Indica a utilização de um endereço IP a partir de um intervalo de endereços IP particulares.	4
Vulnerabilidade potencial de NTTP	Indica uma vulnerabilidade potencial VoIP.	4
Lista de bloqueio de endereços	Indica que um endereço IP está na lista de bloqueio.	8
Endereço de lista de observação	Indica que o endereço IP está na lista de endereços IP que estão sendo monitorados.	7

Tabela 23. categorias de baixo nível e níveis de severidade para a categoria de eventos de atividades suspeitas (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Darknet Endereço	Indica que o endereço IP faz parte de um darknet.	5
Endereço Botnet	Indica que o endereço é parte de uma bootnet.	7
Endereço suspeito	Indica que o endereço IP deverá ser monitorado.	5
Conteúdo inválido	Indica que conteúdo inválido foi detectado.	7
Certificado Inválido	Indica que um certificado inválido foi detectado.	7
Atividade do Usuário	Indica que a atividade do usuário foi detectado.	7
Uso de Protocolo Suspeito	Indica que um padrão suspeito foi detectado.	5
Atividade Suspeita BGP	Indica de uso suspeito do protocolo de roteamento de borda - BGP (Border Gateway Protocol) foi detectado.	5
Rotear Envenenamento	Indica que a corrupção de roteamento foi detectada.	5
Envenenamento ARP	Indica que envenenamento ARP-cache foi detectado.	5
Dispositivo Rogue Detectado	Indica que um dispositivo rouge foi detectado.	5

Sistema

A categoria do sistema contém eventos que estão relacionados a alterações do sistema, instalação de software, ou mensagens de status.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria do sistema.

Tabela 24. categorias de baixo nível e níveis de severidade para a categoria de eventos do sistema

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento do Sistema Desconhecido	Indica um evento do sistema desconhecido.	1
Inicialização do Sistema	Indica um reinício do sistema.	1
Configuração do sistema	Indica uma alteração na configuração do sistema.	1
Interrupção do Sistema	Indica que o sistema foi interrompida.	1
Falha do Sistema	Indica uma falha do sistema.	6
Status do Sistema	Indica qualquer evento de informações.	1
Erro de Sistema	Indica um erro do sistema.	3
Evento do Sistema Diverso	Indica um evento de sistema diversificadas.	1
Serviço Iniciado	Indica que os serviços do sistema foi iniciado.	1
Serviço Parado	Indica que os serviços do sistema parou.	1
Falha no Serviço	Indica uma falha do sistema.	6
Modificação de Registro Bem-sucedida	Indica que uma modificação no registro foi bem-sucedida.	1
Modificação de Política do Host Bem-sucedida	Indica que uma modificação na política de host foi bem-sucedida.	1
Modificação de Arquivo Bem-sucedida	Indica que uma modificação de um arquivo foi bem-sucedida.	1
Modificação de Pilha Bem-sucedida	Indica que uma modificação para a pilha foi bem-sucedida.	1
Modificação de Aplicativo Bem-sucedida	Indica que uma modificação no aplicativo foi bem-sucedida.	1
Modificação de Configuração Bem-sucedida	Indica que uma modificação na configuração foi bem-sucedida.	1
Modificação de Serviço Bem-sucedida	Indica que uma modificação de um serviço foi bem-sucedida.	1
Modificação de Registro com Falha	Indica que uma modificação no registro falhou.	1

Tabela 24. categorias de baixo nível e níveis de severidade para a categoria de eventos do sistema (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Modificação de Política do Host com Falha	Indica que uma modificação na política do host falhou.	1
Modificação de Arquivo com Falha	Indica que uma modificação em um arquivo falhou.	1
Modificação de Pilha com Falha	Indica que uma modificação para a pilha falhou.	1
Modificação de Aplicativo com Falha	Indica que uma modificação de um aplicativo falhou.	1
Modificação de Configuração com Falha	Indica que uma modificação na configuração falhou.	1
Modificação de Serviço com Falha	Indica que uma modificação para o serviço falhou.	1
Adição de Registro	Indica que um novo item foi incluído no registro.	1
Política do Host Criada	Indica que um novo entry foi incluído no registro.	1
Arquivo Criado	Indica que um novo foi criado no sistema.	1
Aplicativo Instalado	Indica que um novo aplicativo foi instalado no sistema.	1
Serviço Instalado	Indica que um novo serviço foi instalado no sistema.	1
Exclusão de Registro	Indica que uma entrada de registro foi excluído.	1
Política do Host Excluída	Indica que uma entrada de política de host foi excluído.	1
Arquivo Excluído	Indica que um arquivo foi excluído.	1
Aplicativo Desinstalado	Indica que um aplicativo foi desinstalado.	1
Serviço Desinstalado	Indica que um serviço foi desinstalado.	1
Informativo do Sistema	Indica informações do sistema.	3
Permissão de Ação do Sistema	Indica que uma ação tentada no sistema foi autorizado.	3
Negação de Ação do Sistema	Indica que uma ação tentada no sistema foi negado.	4
Cron	Indica uma mensagem de crontab.	1
Status do Cron	Indica uma mensagem de status crontab.	1
Falha Cron	Indica uma mensagem de falha crontab.	4
Cron Bem-sucedido	Indica uma mensagem de êxito crontab.	1
Daemon	Indica uma mensagem de daemon.	1
Status do Daemon	Indica uma mensagem de status do daemon.	1
Falha do Daemon	Indicates a daemon failure message.	4
Daemon de Bem-sucedida	Indica uma mensagem de êxito do daemon.	1
Kernel	Indica uma mensagem de kernel.	1
Status do Kernel	Indica uma mensagem de status do kernel.	1
Falha Kernel	Indica uma mensagem de falha do kernel.	
Kernel Bem-sucedido	Indica uma mensagem de êxito do kernel.	1
Autenticação	Indica uma mensagem de autenticação.	1
- Informações	Indica uma mensagem informativa.	2
Nota	Indica uma mensagem de aviso.	3
Aviso	Indica uma mensagem de aviso.	5
Erro	Indica uma mensagem de erro.	7
Critical	Indica uma mensagem crítica.	9
Depurar	Indica uma mensagem de depuração.	1
Mensagens	Indica uma mensagem genérica.	1
Privilégio de Acesso	Indica que o acesso privilégio foi tentado.	3
Alerta	Indica uma mensagem de alerta.	9
Emergência	Indica uma mensagem de emergência.	9
Status de SNMP	Indica uma mensagem de status SNMP.	1
Status do FTP	Indica uma mensagem de status do FTP.	1
Status do NTP	Indica uma mensagem de status do NTP.	1
A Rádio Access Point	Indica uma falha de ponto de acesso.	3
Incompatibilidade de Configuração de Protocolo de Criptografia	Indica uma incompatibilidade de configuração do protocolo de criptografia.	3

Tabela 24. categorias de baixo nível e níveis de severidade para a categoria de eventos do sistema (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Dispositivo ou Client Authentication Server Malconfigurado	Indica que um dispositivo cliente ou servidor de autenticação não foi configurado adequadamente.	5
Espera Ativa Falha Ativar	Indica uma falha ativar hot standby.	5
Espera Ativa Falha Desativar	Indicates a hot standby disable failure.	5
Espera Ativa Ativado com êxito	Indica que um grupo foi incluído com êxito.	1
Espera Ativa Associação Perdida	Indica que uma associação hot standby foi perdida.	5
Falha de iniciação no Modo principal	falha de iniciação no modo principal.	5
MainMode Initiation Bem-sucedido	Indica que o início MainMode foi bem-sucedida.	1
MainMode de Status	Indica uma mensagem de status MainMode foi relatado.	1
QuickMode Falha Initiation	Indica que o início QuickMode falhou.	5
Quickmode Initiation Bem-sucedido	Indica que o início QuickMode foi bem-sucedida.	1
Quickmode de Status	Indica uma mensagem de status QuickMode foi relatado.	1
Licença Inválida	Indica um protocolo inválido.	3
Licença Expirada	Indica uma licença expirou.	3
New License Applied	Indica uma nova licença aplicado.	1
Erro de licença	Indica um erro de licença.	5
Status da Licença	Indica uma mensagem de status da licença.	1
Erro de configuração	Indica que foi detectado um erro de configuração.	5
Interrupção de Serviço	Indica que uma interrupção do serviço foi detectado.	5
Licença Excedido	Indica que o recursos de licença foram excedidos.	3
Status do Desempenho	Indica que o reassociação estação foi bem-sucedida.	1
Degradação do Desempenho	Indica que o desempenho estiver sendo prejudicado.	4
Configuração incorreta	Indica que uma configuração incorreta foi detectado.	5

Política

A categoria de política contém eventos que estão relacionados à administração da política de rede e ao monitoramento de recursos da rede quanto a violações de política.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de política.

Tabela 25. Categorias de baixo nível e níveis de severidade para a categoria de política

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Violação de política desconhecida	Indica uma violação de política desconhecida.	2
Violação de política da web	Indica uma violação de política da web.	2
Violação de política de acesso remoto	Indica uma violação de política de acesso remoto.	2
Violação de política de IRC/IM	Indica uma violação de política de mensagens instantâneas.	2
Violação de política de P2P	Indica uma violação de política ponto a ponto (P2P).	2
Violação de política de acesso de IP	Indica uma violação de política de acesso de IP.	2
Violação de política de aplicativo	Indica uma violação de política de aplicativo.	2
Violação de política de banco de dados	Indica uma violação de política de banco de dados.	2

Tabela 25. Categorias de baixo nível e níveis de severidade para a categoria de política (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Violação de política de limite de rede	Indica uma violação de política de limite de rede.	2
Violação de política de pornografia	Indica uma violação de política de pornografia.	2
Violação de política de jogos	Indica uma violação de política de jogos.	2
Violação de política diversa	Indica uma violação de política diversa.	2
Violação de política de conformidade	Indica uma violação de política de conformidade.	2
Violação de política de correio	Indica uma violação de política de correio.	2
Violação de política de IRC	Indica uma violação de política de IRC	2
Violação de política de IM	Indica uma violação de política que está relacionada a atividades de mensagens instantâneas (IM).	2
Violação de política de VoIP	Indica uma violação de política de VoIP	2
Com êxito	Indica uma mensagem de êxito da política.	1
Com falha	Indica uma mensagem de erro da política.	4

Desconhecido

A categoria desconhecido contém eventos que não são analisados e, portanto, não podem ser categorizados.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria desconhecido.

Tabela 26. Categorias de baixo nível e níveis de severidade para categorias desconhecidas.

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Desconhecido	Indica um evento de limite desconhecido.	3
Evento desconhecido de Snort	Indica um evento desconhecido. Snort	3
Evento do Dragon Desconhecido	Indica um evento desconhecido. Dragon	3
Evento do Pix Firewall Desconhecido	Indica um evento desconhecido. Cisco Private Internet Exchange (PIX) Firewall	3
Evento de Ponto de Mudança Desconhecido	Indica um evento desconhecido. HP TippingPoint	3
Evento do Servidor de Autenticação do Windows	Indica um evento desconhecido. Windows Auth Server	3
Evento do Nortel Desconhecido	Indica um evento desconhecido. Nortel	3
Armazenado	Indica um evento armazenado desconhecido.	3
Comportamental	Indica um evento comportamental desconhecido.	3
Limite	Indica um evento de limite desconhecido.	3
Anomalia	Indica um evento anomal desconhecido.	3

CRE

A categoria de evento de regra customizada contêm eventos que são gerados de uma ofensa customizada ou de uma regra de evento.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria do CRE.

Tabela 27. Categorias de baixo nível

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento do CRE Desconhecido	Indica um mecanismo de regras customizadas de evento desconhecido.	5
Correspondência de Regra de Evento Único	Indica uma cruzada ofensa de eventos da regra de seqüência de correspondência.	5

Tabela 27. Categorias de baixo nível (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Correspondência de Regra de Sequência de Eventos	Indica uma correspondência de regra de sequência de eventos.	5
Correspondência de Regra de Sequência de Eventos de Ofensa Cruzado	Indica uma cruzada ofensa de eventos da regra de seqüência de correspondência.	5
Correspondência de Regra de Ofensa	Indica uma correspondência de regra de ofensa.	5

Exploração Potencial

A categoria de exploração potencial contém eventos que são relacionados a explorações potenciais de aplicativos ou tentativas de estouro de buffer.

A guia a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a categoria de exploração potencial.

Tabela 28. Categorias de baixo nível e níveis de severidade para a categoria de exploração potencial.

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ataque potencial de exploração desconhecido	Indica que um ataque potencial de exploração foi detectado.	7
Estouro potencial de buffer	Indica que estouro potencial de buffer foi detectado.	7
Exploração potencial por meio do DNS	Indica que foi detectado um ataque potencial de exploração por meio do servidor DNS	7
Exploração potencial pelo Telnet	Indica que foi detectado um ataque de exploração potencial por meio do Telnet.	7
Exploração potencial pelo Linux	Indica que foi detectado um ataque de exploração potencial por meio do Linux	7
Exploração potencial pelo UNIX	Indica que foi detectado um ataque de exploração potencial por meio do UNIX.	7
Exploração potencial pelo Windows	Indica que foi detectado um ataque de exploração potencial por meio do Windows.	7
Exploração potencial por e-mail	Indica que foi detectado um ataque de exploração potencial por e-mail.	7
Exploração potencial de infraestrutura	Indica que foi detectado um ataque de exploração potencial na infra-estrutura do sistema.	7
Exploração potencial diversa	Indica que um ataque potencial de exploração foi detectado.	7
Exploração potencial pela web	Indica que foi detectado um ataque de exploração potencial pela web.	7
Conexão potencial de Botnet	Indica que foi detectado um ataque de exploração potencial que usa botnet.	6
Atividade potencial de Worm	Indica que foi detectado um ataque de exploração potencial atividade de worm.	6

Usuário definido

A categoria Usuário definido contêm eventos que estão relacionados a objetos definidos pelo usuário

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria Usuário definido.

Tabela 29. Categorias de baixo nível e níveis de severidade da categoria Usuário definido

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sentry baixo customizado	Indica um evento com anormalidade customizado de baixa severidade.	3
Sentry médio customizado	Indica um evento com anormalidade customizado de média severidade.	5
Sentry alto customizado	Indica um evento com anormalidade customizado de alta severidade.	7

Tabela 29. Categorias de baixo nível e níveis de severidade da categoria Usuário definido (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sentry 1 customizado	Indica um evento com anormalidade customizado com um nível de severidade 1.	1
Sentry 2 customizado	Indica um evento com anormalidade customizado com um nível de severidade 2.	2
Sentry 3 customizado	Indica um evento com anormalidade customizado com um nível de severidade 3.	3
Sentry 4 customizado	Indica um evento com anormalidade customizado com um nível de severidade 4.	4
Sentry 5 customizado	Indica um evento com anormalidade customizado com um nível de severidade 5.	5
Sentry 6 customizado	Indica um evento com anormalidade customizado com um nível de severidade 6.	6
Sentry 7 customizado	Indica um evento com anormalidade customizado com um nível de severidade 7.	7
Sentry 8 Customizado	Indica um evento com anormalidade customizado com um nível de severidade 8.	8
Sentry 9 customizado	Indica um evento com anormalidade customizado com um nível de severidade 9.	9
Política baixa customizada	Indica um evento de política customizada com um nível de severidade baixo.	3
Política média customizada	Indica um evento de política customizada com um nível de severidade médio.	5
Política alta customizada	Indica um evento de política customizada com um nível de severidade alto.	7
Política 1 customizada	Indica um evento de política customizada com um nível de severidade 1.	1
Política 2 customizada	Indica um evento de política customizada com um nível de severidade 2.	2
Política 3 customizada	Indica um evento de política customizada com um nível de severidade 3.	3
Política 4 customizada	Indica um evento de política customizada com severidade de nível 4.	4
Política 5 customizada	Indica um evento de política customizada com um nível de severidade 5.	5
Política 6 customizada	Indica um evento de política customizada com um nível de severidade 6.	6
Política 7 customizada	Indica um evento de política customizada com um nível de severidade 7.	7
Política 8 customizada	Indica um evento de política customizada com um nível de severidade 8.	8
Política 9 customizada	Indica um evento de política customizada com um nível de severidade 9.	9
Usuário baixo customizado	Indica um evento do usuário customizado com um nível de severidade baixa.	3
Usuário médio customizado	Indica um evento do usuário customizado com um nível de severidade média.	5
Usuário alto customizado	Indica um evento do usuário customizado com um nível de severidade alta.	7
Usuário 1 customizado	Indica um evento do usuário customizado com um nível de severidade 1.	1
Usuário 2 customizado	Indica um evento do usuário customizado com um nível de severidade 2.	2
Usuário 3 customizado	Indica um evento do usuário customizado com um nível de severidade 3.	3
Usuário 4 customizado	Indica um evento do usuário customizado com um nível de severidade 4.	4
Usuário 5 customizado	Indica um evento do usuário customizado com um nível de severidade 5.	5
Usuário 6 customizado	Indica um evento do usuário customizado com um nível de severidade 6.	6
Usuário 7 customizado	Indica um evento do usuário customizado com um nível de severidade 7.	7
Usuário 8 customizado	Indica um evento do usuário customizado com um nível de severidade 8.	8
Usuário 9 customizado	Indica um evento do usuário customizado com um nível de severidade 9.	9

SIM de auditoria

A categoria Auditoria SIM contém eventos que estão relacionadas à interação do usuário com o QRadar Console e recursos administrativos.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de gravidade associado para a categoria SIM de auditoria.

Tabela 30. categorias de baixo nível e níveis de gravidade para a categoria Auditoria SIM

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Autenticação do Usuário SIM	Indica um login de usuário ou logout no Console.	5
Alteração de Configuração SIM	Indica que um usuário alterou a configuração ou a implementação SIM.	3
Autenticação do Usuário SIM	Indica que um usuário iniciou um processo, como iniciar um backup ou gerar um relatório, no módulo SIM.	3
Sessão Criada	Indica que uma sessão do usuário foi criada.	3
Sessão Destruído	Indica que uma sessão do usuário foi destruída.	3
Sessão Admin Criada	Indica que uma sessão admin foi criado.	
Sessão de Administrador Destruídas	Indica que uma sessão do administrador foi destruída.	3
Sessão de Autenticação Inválida	Indica uma autenticação de sessão inválida.	5
Autenticação da Sessão Expirado	Indica que uma autenticação de sessão expirou.	3
Configuração de gerenciador de risco	Indica que um usuário alterou a configuração IBM Security QRadar Risk Manager.	3

Descoberta do Host VIS

Quando o componente VIS descobre e armazena novos hosts, portas, ou as vulnerabilidades que são detectados na rede, o componente VIS gera eventos. Esses eventos são enviados para o Coletor de eventos para ser correlato a outro evento de segurança.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados para a VIS categoria de descoberta de host.

Tabela 31. categorias de baixo nível e níveis de severidade para o VIS de host de descoberta da categoria

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Descoberta do Novo Host	Indica que o componente VIS detectou um novo host.	3
Nova porta descoberta	Indica que o componente VIS detectou uma nova porta aberta.	3
Nova descoberta vulnerabilidade	Indica que o componente VIS detecta uma nova vulnerabilidade.	3
Descoberta do novo do S.O.	Indica que o componente VIS detectou um novo sistema operacional em um host.	3
Massa do host descoberto	Indica que o componente VIS detectou muitos novos hosts em um curto período.	3

Aplicação

A categoria de aplicação contêm eventos que estão relacionados a atividade de aplicação, tais como email ou atividade de FTP.

A tabela abaixo descreve as categorias de evento de nível inferior associadas a níveis de severidade para categoria do aplicativo.

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo.

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Correio aberto	Indica que uma conexão de email foi estabilizada.	1
Email encerrado.	Indica que uma conexão de email foi encerrada.	1
Email reconfigurado	Indica que um email foi reconfigurado.	3
Email finalizado	Indica que uma conexão de email foi finalizada.	4
Email negado	Indica que uma conexão de email foi negada.	4
Email em andamento	Indica que uma conexão de email está sendo tentada.	1
Email atrasado	Indica que uma conexão de email foi atrasada.	4
Email na fila	Indica que uma conexão de email estava na fila.	3
Email redirecionado	Indica que uma conexão de email foi redirecionada.	1
FTP aberto	Indica que uma conexão FTP foi aberta.	1
FTP fechado	Indica que uma conexão FTP foi fechada.	1
FTP reconfigurado	Indica que uma conexão FTP foi recuperada.	3
FTP Finalizado	Indica que uma conexão FTP foi finalizada.	4
FTP Negado	Indicates that an FTP connection was denied.	4
FTP em andamento	Indica que uma conexão FTP está em progresso.	1
FTP redirecionado	Indica que uma conexão FTP foi redirecionada.	3
HTTP aberto	Indica que uma conexão HTTP foi estabelecida.	1
HTTP fechado	Indica que uma conexão HTTP foi fechada.	1
Reconfiguração de HTTP	Indica que uma conexão HTTP foi reconfigurada.	3
HTTP finalizado	Indica que uma conexão HTTP foi finalizada.	4
HTTP Negado	Indica que uma conexão HTTP foi negada.	4
HTTP em andamento	Indica que uma conexão HTTP está em progresso.	1
HTTP em atraso	Indica que uma conexão HTTP está em atraso.	3
HTTP em fila	Indica que uma conexão HTTP estava em fila.	1
Redirecionamento do HTTP	Indica que que uma conexão HTTP foi redirecionada.	1
Proxy HTTP	Indica que uma conexão HTTP está entrando no servidor proxy.	1
HTTPS aberto	Indica que uma conexão HTTPS foi estabelecida.	1
HTTPS Closed	dica que uma conexão HTTPS foi encerrada.	1
HTTPS reconfigurada	Indica que uma conexão HTTPS foi reconfigurada.	3
HTTPS finalizada.	Indica que uma conexão HTTPS foi finalizada.	4
HTTPS negado	Indica que uma conexão HTTPS foi negada.	4
HTTPS em progresso	Indica que uma conexão HTTPS está em progresso.	1
HTTPS em atraso.	Indica que uma conexão HTTPS está em atraso.	3
HTTPS em fila.	Indica que uma conexão HTTPS foi enfileirada.	3
HTTPS redirecionada.	Indica que uma conexão HTTPS foi redirecionada.	3
Proxy HTTPS	Indica que uma conexão HTTPS está entrando no servidor proxy.	1
SSH aberto	Indica que uma conexão SSH foi estabilizada.	1
SSH fechada	Indica que uma conexão SSH foi fechada.	1

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
SSH reconfigurada	Indica que uma conexão SSH foi reconfigurada.	3
SSH finalizada	Indica que uma conexão SSH foi finalizada.	4
SSH negada	Indica que uma conexão SSH foi negda.	4
SSH em progresso	Indica que uma sessão SSH está em progresso.	1
Acesso remoto aberto	Indica que uma conexão de acesso remoto foi estabelecida.	1
Acesso remoto fechado	Indica que uma conexão de acesso remoto foi fechada.	1
Reconfiguração de acesso remoto	Indica que uma conexão de acesso remoto foi reconfigurada.	3
Acesso remoto finalizado.	Indica que uma conexão de acesso remoto foi finalizada.	4
Acesso remoto negado	Indica que um acesso remoto foi negado.	4
Acesso remoto em progresso	Indica que um acesso remoto está em progresso.	1
Acesso remoto em atraso	Indica que um acesso remoto está em atraso.	3
Acesso remoto redirecionado	Indica que um acesso remoto foi redirecionado.	3
VPN aberto	Indica que uma conexão VPN foi aberta.	1
VPN fechada	Indica que uma conexão VPN foi fechada.	1
VPN reconfigurada	Indica que uma conexão VPN foi reconfigurada.	3
VPN finalizado	Indica que uma conexão VPN foi finalizada.	4
VPN negado	Indica que uma conexão VPN foi negada.	4
VPN em andamento	Indica que uma conexão VPN está em andamento.	1
VPN em atraso	Indica que uma conexão VPN está em atraso.	3
VPN em fila	Indica que uma conexão VPN está em fila	3
VPN redirecionada	Indica que uma conexão VPN foi redirecionada	3
RDP aberto	Indica que uma conexão RDP foi estabelecida.	1
RDP fechado	Indica que uma conexão RDP foi fechada.	1
RDP reconfigurada	Indica que uma conexão RDP foi fechada.	3
RDP finalizada	Indica que uma conexão RDP foi finalizada.	4
RDP negada	Indica que uma conexão RDP foi negada.	4
RDP em andamento	Indica que uma conexão RDP está em andamento.	1
RDP redirecionada	Indica que uma conexão RDP foi redirecionada.	3
Transferência de arquivo aberta	Indica que conexão de transferência de arquivos foi estabelecida.	1
Transferência de arquivos encerrada	Indica que conexão de transferência de arquivos foi encerrada.	1
Transferência de arquivos reconfigurada	Indica que uma transferência de arquivos foi reconfigurada.	3
Transferência de arquivos finalizada	Indica que uma conexão de transferência de arquivos foi finalizada.	4
Transferência de arquivos Negado	Indica que conexão de transferência de arquivos foi negada.	4
Transferência de arquivos em andamento	Indica que uma conexão de transferência de arquivos está em andamento.	1
Transferência de arquivos em atraso	Indica que uma conexão de transferência de arquivos foi adiado.	3
Fila de transferência de arquivos	Indica que uma conexão de transferência de arquivos foi enfileirada.	3
Transferência de arquivos redirecionada	Indica que uma conexão de transferência de arquivo foi redirecionado.	3
Aberto de DNS	Indica que uma conexão de DNS foi estabelecida.	1
DNS fechado	Indica que uma conexão de DNS foi fechado.	1

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Reconfigurar DNS	Indica que uma conexão de DNS foi reconfigurada.	5
DNS Terminated	Indica que uma conexão de DNS foi terminada.	5
DNS Negado	Indica que uma conexão de DNS foi negada.	5
DNS Em Andamento	Indica que uma conexão de DNS está em andamento.	1
DNS Atrasado	Indica que uma conexão de DNS foi adiado.	5
DNS redirecionado	Indica que uma conexão de DNS foi redirecionada.	4
Bate-papo (chat) aberto	Indica que uma conexão de bate-papo foi aberta.	1
Bate-papo Encerrado	Indica que uma conexão de bate-papo foi encerrado.	1
Bate-Papo Reconfigurado	Indica que uma conexão de bate-papo foi reconfigurada.	3
Bate-papo Terminado	Indica que uma conexão de bate-papo foi finalizada.	3
Bate-papo Negado	Indica que uma conexão de bate-papo foi negado.	3
Bate-papo em andamento	Indica que uma conexão de bate-papo está em andamento.	1
Bate-papo redirecionado	Indica que uma conexão de bate-papo foi redirecionada.	1
Banco de dados aberto	Indica que uma conexão com o banco de dados foi estabelecida.	1
Banco de dados encerrado	Indica que uma conexão com o banco de dados foi encerrada.	1
Reconfiguração do Banco de Dados	Indica que uma conexão com o banco de dados foi reconfigurado.	5
Banco de dados finalizado	Indica que um banco de dados foi finalizado.	5
Banco de dados negado	Indica que um banco de dados foi negado.	5
Banco de dados em progresso	Indica que um banco de dados está em progresso.	1
Banco de dados redirecionado	Indica que um banco de dados foi redirecionado.	3
SMTP aberta	Indica que uma conexão SMTP foi aberta.	1
SMTP fechada	Indica que uma conexão SMTP foi fechada.	1
SMTP reconfigurada	Indica que uma conexão SMTP foi reconfigurada.	3
SMTP finalizado	Indica que uma conexão SMTP foi finalizada.	5
SMTP Negado	Indica que uma conexão SMTP foi negada.	5
SMTP em andamento	Indica que uma conexão SMTP está em andamento.	1
SMTP em atraso	Indica que uma conexão SMTP está em atraso.	3
SMTP em fila	Indica que uma conexão SMTP está em fila.	3
SMTP redirecionada	Indica que uma conexão SMTP foi redirecionada.	3
Autenticação Aberta	Indica que uma conexão do servidor de autorização foi estabelecida.	1
Autenticação Encerrada	I ndica que uma conexão do servidor de autorização foi encerrada.	1
Autenticação reconfigurada	Indica que uma conexão do servidor de autorização foi reconfigurada.	3
Autenticação finalizada	Indica que uma conexão do servidor de autorização foi finializada.	4
Autenticação negada	Indica que uma conexão do servidor de autorização foi negada.	4
Autenticação em andamento	Indica que uma conexão do servidor de autorização está em andamento.	1
Autenticação em atraso	Indica que uma conexão do servidor de autorização foi atrasada.	3
Autenticação Enfileirada	Indica que uma conexão do servidor de autorizações foi enfileirada.	3

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Autenticação Redirecionada	Indica que uma conexão do servidor de autorização foi redirecionada.	2
P2P Aberta	Indioca que uma conerxão ponto-a-ponto foi estabelecida.	1
P2P encerrada	Indica que uma conexão P2P foi encerrada.	1
P2P reconfigurada	Indica que uma conexão P2P foi reconfigurada.	4
P2P finalizada	Indica que uma conexão P2P foi finalizada.	4
P2P negada	Indica que uma conexão P2P foi negada.	3
P2P em progresso	Indica que uma conexão P2P está em progresso.	1
Web aberta	Indica que uma conexão da Web foi estabelecida.	1
Web encerrada	Indica que uma conexão da Web foi encerrda.	1
Web reconfigurada	Indica que uma conexão da Web foi reconfigurada.	4
Web encerrada	Indica que uma conexão da Web foi encerrada.	4
Web negada	Indica que uma conexão da Web foi negado.	4
Web em Andamento	Indica que uma conexão da Web está em andamento.	1
Atrasado da Web	Indica que uma conexão da Web foi atrasado.	3
Fila Web	Indica que uma conexão da Web foi enfileirada.	1
Web redirecionada	Indica que uma conexão da Web foi redirecionada.	1
Proxy da Web	Indica que uma conexão da Web entrou em proxy	1
Aberto VoIP	Indica que uma conexão de Voz sobre IP (VoIP) foi estabelecida.	1
Fechado VoIP	Indica que uma conexão VoIP foi fechado.	1
Reconfigurar VoIP	Indica que uma conexão VoIP foi reconfigurado.	3
VoIP finalizada	Indica que uma conexão VoIP foi finalizado.	3
VoIP negado	I ndica que uma conexão VoIP foi negada.	3
VoIP em andamento	Indica que uma conexão VoIP está em progresso.	1
VoIP Atrasado	Indica que uma conexão VoIP foi atrasado.	3
VoIP redirecionado	Indica que uma conexão VoIP foi redirecionado.	3
Sessão LDAP Iniciado	Indica uma sessão LDAP iniciada.	1
Sessão LDAP Finalizado	Indica uma sessão LDAP terminou.	1
Sessão LDAP Negado	Indica que uma sessão LDAP foi negado.	3
Status da Sessão do LDAP	Indica que uma mensagem de status de sessão LDAP foi relatado.	1
Falha de Autenticação LDAP	Indica que uma autenticação LDAP falhou.	4
Autenticação LDAP Bem-sucedido	Indica que uma autenticação LDAP foi bem-sucedida.	1
Sessão AAA Iniciada	iIndica que uma Autenticação, Autorização e sessão Contabilidade (AAA) iniciou.	1
Sessão AAA Encerrada	Indica que uma sessão AAA foi encerrada.	1
Sessão AAA Negada	Indica que uma sessão AAA foi negado.	3
Status da Sessão AAA	Indica que uma mensagem de status da sessão AAA foi relatado.	1
Falha de Autenticação AAA	Indica que uma autenticação AAA falhou.	4
Autenticação Bem-sucedido AAA	Indica que uma autenticação AAA foi bem-sucedida.	1
Falha de Autenticação IPSEC	Indica que uma autenticação da Internet Protocol Security (IPSEC) falhou.	4
IPSEC Autenticação Bem-sucedido	Indica que uma IPSEC de autenticação foi bem-sucedida.	1
Sessão Iniciada IPSEC	Indica que uma sessão IPSEC iniciado.	1
Sessão Encerrada IPSEC	Indica que uma sessão IPSEC terminou.	1

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Erro IPSEC	Indica que uma mensagem de erro IPSEC foi relatado.	5
Status do IPSEC	Indica que uma mensagem de status da sessão IPSEC foi relatada.	1
Sessão Aberta IM	Indica que uma sessão Instant Messenger (IM) foi estabelecida.	1
O IM Fechado Sessão	Indica que uma sessão de MI foi fechada.	1
Reconfigurar Sessão IM	Indica que uma sessão de MI foi redefinido.	3
Sessão IM Terminada	Indica que uma sessão de MI foi finalizado.	3
Sessão IM negada	Indica que uma sessão do IM foi negado.	3
Sessão IM em andamento	Indica que uma sessão de MI está em andamento.	1
Sessão IM Atrasada	Indica que uma sessão IM foi atrasada	3
Sessão IM direcionada	Indica que uma sessão de MI foi redirecionada.	3
Sessão Aberta WHOIS	Indica que uma sessão WHOIS foi estabelecida.	1
Sessão Fechado WHOIS	Indica que uma sessão WHOIS foi fechado.	1
Reconfigurar Descartar Sessão	Indica que um WHOIS sessão foi redefinido.	3
Sessão Terminada WHOIS	Indica que uma sessão WHOIS foi finalizada.	3
Sessão Negado WHOIS	Indica que uma sessão WHOIS foi negado.	3
Sessão WHOIS em andamento	Indica que uma sessão do WHOIS está em andamento.	1
Sessão WHOIS finalizada	Indica que uma sessão WHOIS foi finalizada.	3
Sessão de rastreio de rotas aberta	Indica que uma sessão de rastreio de rotas foi estabelecida.	1
Sessão de rastreio de rotas fechada	Indica que uma sessão de rastreio de rotas foi fechada.	1
Sessão de rastrio de rotas fechado	Indica que uma sessão de rastreio de rotas foi negada.	3
Sessão rastreio de rotas em andamento	Indica que uma sessão de rastrio de rotas está em andamento.	1
Sessão TN3270 aberta	O TN3270 é um programa de emulação de terminal, que é usado para conectar a um IBM terminal 3270. Essa categoria indica que uma sessão TN3270 foi estabelecida.	1
Sessão TN3270 Fechada	Indica que uma sessão TN3270 foi fechada.	1
Reconfigurar Sessão TN3270	Indica que uma sessão TN3270 foi reconfigurada.	3
Sessão TN3270 terminada	Indica que uma sessão TN3270 foi finalizada.	3
Sessão TN3270 Negada	Indica que uma sessão TN3270 foi negada.	3
Sessão TN3270 em andamento	Indica que uma sessão do TN3270 está em andamento.	1
Sessão TFTP aberta	Indica que uma sessão de TFTP foi estabelecida.	1
Sessão TFTP de Fechada	Indica que uma sessão de TFTP estava fechada.	1
Reconfigurar sessão TFTP	Indica que uma sessão TFTP foi reconfigurada.	3
Sessão TFTP terminada	Indica que uma sessão TFTP foi finalizada.	3
Sessão TFTP negada	Indica que uma sessão TFTP foi negada.	3
Sessão TFTP em progresso	Indica que uma sessão de TFTP está em andamento.	1
Sessão Aberta Telnet	Indica que uma sessão Telnet foi estabelecida.	1
Sessão Telnet fechada	Indica que uma sessão Telnet foi fechada.	1
Reconfigurar Sessão Telnet	Indica que uma sessão Telnet foi reconfigurada.	3
Telnet Sessão Terminada	Indica que uma sessão Telnet foi finalizado.	3
Sessão Telnet negada	Indica que uma sessão Telnet foi negada.	3
Sessão Telnet em progresso	Indica que uma sessão Telnet está em progresso.	1

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão syslog aberta	Indica que uma sessão syslog foi estabelecida.	1
Sessão syslog encerrada	Indica que uma sessão do syslog foi fechada.	1
Sessão Syslog negada	Indica que uma sessão syslog foi negada.	3
Sessão syslog em progresso	Indica que uma sessão do syslog está em progresso.	1
Sessão SSL Aberta	Indica que uma sessão da Camada Soquete Seguro(Secure Socket Layer - SSL) foi estabelecida.	1
Sessão SSL Fechada	Indica que uma sessão SSL foi fechada.	1
Reconfigurar de Sessão SSL	Indicates that an SSL session was reset.	3
Sessão SSL Terminada	Indica que uma sessão SSL foi finalizada.	3
Sessão SSL Negada	Indica que uma sessão SSL foi negada.	3
Sessão SSL em andamento	Indica que uma sessão SSL está em andamento.	1
Sessão SNMP Aberta	Indica que uma sessão SNMP (Simple Network Management Protocol) foi estabelecida.	1
Sessão SNMP fechada	Indica que uma sessão SNMP foi fechada.	1
Sessão SNMP negada	Indica que uma sessão SNMP foi negada.	3
Sessão SNMP em andamento	Indica que uma sessão SNMP está em andamento.	1
Sessão SMB aberta	Indica que uma sessão SMB (Server Message Block) foi estabelecida.	1
Sessão SMB fechada	Indica que uma sessão SMB foi fechada.	1
Sessão SMB reconfigurada	Indica que uma sessão SMB foi redefinida.	3
Sessão SMB terminada	Indica que uma sessão SMB foi finalizada.	3
Sessão SMB negado	Indica que uma sessão SMB foi negado.	3
Sessão SMB em andamento	Indica que uma sessão SMB está em andamento.	1
Sessão de fluxo de mídia em aberto	Indica que uma sessão de fluxo de mídia está em aberto foi estabelecida.	1
Sessão de fluxo de mídia fechada	Indica que uma sessão de fluxo de mídia foi fechado.	1
Sessão de reconfiguração de fluxo de mídia	Indica que uma sessão de fluxo de mídia foi redefinida.	3
Sessão de fluxo de mídia finalizada	Indica que uma sessão de fluxo de mídia foi finalizada.	3
Sessão de fluxo de mídia negada	Indica que uma sessão de fluxo de mídia foi negada.	3
Sessão de fluxo de mídia em andamento	Indica que uma sessão de fluxo de midia está em andamento.	1
Sessão RUSERS Aberta	Indica que uma sessão RUSERS foi estabelecida.	1
Sessão RUSERS fechada	Indica que uma sessão RUSERS foi fechada.	1
Sessão RUSERS negado	Indica que uma sessão RUSERS foi negada.	3
Sessão RUSERS em andamento	Indica que uma sessão RUSERS está em andamento.	1
Sessão rsh em aberto	Indica que a sessão(rsh) foi estabelecida.	1
Sessão Rsh encerrada	Indica que uma sessão rsh foi fechada.	1
Sessão Rsh reconfigurarada	Indica que uma sessão rsh foi reconfigurada.	3
Sessão Rsh terminada	Indica que uma sessão rsh foi finalizada.	3
Sessão Rsh negada	Indica que uma sessão rsh foi negada.	3
Sessão Rsh em andamento	Indica que uma sessão rsh está em andamento.	1
Sessão RLOGIN em aberto	Indica que uma sessão (RLOGIN) foi estabelecida.	1
Sessão RLOGIN encerrada	Indica que uma sessão RLOGIN foi encerrada.	1
Sessão RLOGIN reconfigurada	Indica que uma sessão RLOGIN foi reconfigurada.	3
Sessão RLOGIN finalizada	Indica que uma sessão RLOGIN foi finalizada.	3
Sessão RLOGIN negada	Indica que uma sessão RLOGIN foi negada.	3

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão RLOGIN em andamento	Indica que uma sessão RLOGIN está em andamento.	1
Sessão REXEC em aberto	Indica que uma sessão (Remote Execution) REXEC foi estabelecida.	1
Sessão REXEC fechada	Indica que uma sessão REXEC foi fechada.	1
Reconfigurar Sessão REXEC	Indica que uma sessão foi REXEC redefinida.	3
Sessão REXEC finalizada	Indica que uma sessão REXEC foi finalizada.	3
Sessão REXEC Negada	Indica que uma sessão REXEC foi negada.	3
Sessão REXEC em andamento	Indica que uma sessão REXEC está em andamento.	1
Sessão RPC em aberto	Indica que a Chanmada de Procedimento Remoto foi estabelecida.	1
Sessão RPC fechada	Indica que uma sessão RPC foi fechada.	1
Sessão RPC recuperada	Indica que uma sessão RPC foi redefinida.	3
Sessão RPC finalizada	Indica que uma sessão RPC foi finalizada.	3
Sessão RPC negada	Indica que uma sessão RPC foi negada.	3
Sessão RPC em andamento	Indica que uma sessão RPC está em andamento.	1
Sessão NTP em aberto	Indica que uma sessão Network Time Protocol (NTP) foi estabelecida.	1
Sessão NTP fechado	Indica que uma sessão NTP foi fechada.	1
Reconfigurar sessão NTP	Indica que uma sessão NTP foi reconfigurada.	3
Sessão NTP finalizada	Indica que uma sessão NTP foi finalizado.	3
Sessão NTP negado	Indica que uma sessão NTP foi negada.	3
Sessão NTP em andamento	Indica que uma sessão de NTP está em andamento.	1
Sessão NNTP em aberto	Indica que uma sessão Network News Transfer Protocol (NNTP) foi estabelecida.	1
Sessão NNTP fechado	Indica que uma sessão NNTP foi fechada.	1
Reconfigurar sessão NNTP	Indica que uma sessão NNTP foi reconfigurada.	3
Sessão NNTP finalizada	Indica que uma sessão NNTP foi finalizada.	3
Sessão NNTP negado	Indica que uma sessão NNTP foi negado.	3
Sessão NNTP em andamento	Indica que uma sessão NNTP está em andamento.	1
Sessão NFS emm aberto	Indica que uma sessão NFS (Network File System) foi estabelecida.	1
Sessão NFS fechada	Indica que uma sessão NFS foi fechada.	1
Sessão NFS reconfigurada	Indica que uma sessão NFS foi reconfigurada.	3
Sessão NFS finalizada	Indica que uma sessão NFS foi finalizada.	3
Sessão NFS negada	Indica que uma sessão do NFS foi negada.	3
Sessão NFS em andamento	Indica que uma sessão de NFS está em andamento.	1
Sessão NPC em aberto	Indica que uma sessão o Network Control Program (NCP) foi estabelecida.	1
Sessão NPC fechada	Indica que uma sessão do NCP foi fechada.	1
Sessão NCP reconfigurada	Indica que uma sessão do NCP foi reconfigurada.	3
Sessão NPC finalizada	Indica que uma sessão do NCP foi finalizada.	3
Sessão NCP negada	Indica que uma sessão do NCP foi negada.	3
Sessão NCP em andamento	Indica que uma sessão do NCP está em andamento.	1
Sessão NetBIOS em aberto	Indica que uma sessão NetBIOS foi estabelecida.	1
Sessão NetBIOS fechada	Indica que uma sessão NetBIOS foi fechada.	1
Sessão NetBIOS Reconfigurada	Indica que uma sessão NetBIOS foi reconfigurada.	3
Sessão NetBIOS finalizada	Indica que uma sessão NetBIOS foi finalizada.	3
Sessão NetBIOS negada	Indica que uma sessão NetBIOS foi negada.	3

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão NetBIOS Em Andamento	Indica que uma sessão NetBIOS está em andamento.	1
Sessão MODBUS em aberto	Indica que uma sessão MODBUS foi estabelecida.	1
Sessão MODBUS fechado	Indica que uma sessão MODBUS foi fechada.	1
Sessão MODBUS reconfigurada	Indica que uma sessão MODBUS foi redefinida.	3
Sessão MODBUS finalizada	Indica que uma sessão MODBUS foi finalizada.	3
MODBUS Sessão negada	Indica que uma sessão MODBUS foi negada.	3
Sessão MODBUS em andamento	Indica que uma sessão MODBUS está em andamento.	1
Sessão LPD em aberto	Indica que uma sessão Line Printer Daemon (LPD) foi estabelecida.	1
Sessão LPD fechada	Indica que uma sessão LPD foi fechada.	1
Sessão LPD resetada	Indica que uma sessão LPD foi reconfigurada.	3
Sessão LPD finalizada	Indica que uma sessão LPD foi finalizada.	3
Sessão LPD negada	Indica que uma sessão LPD foi negada.	3
Sessão LPD em andamento	Indica que uma sessão LPD está em andamento.	1
Lotus Notes Sessão Aberta	Indica que uma sessão Lotus Notes foi estabelecida.	1
Lotus Notes Sessão encerrada	Indica que uma sessão Lotus Notes foi fechada.	1
Lotus Notes Sessão reconfigurada	Indica que uma sessão Lotus Notes foi reconfigurada.	3
Lotus Notes Sessão Terminada	Indica que uma sessão Lotus Notes foi encerrada.	3
Lotus Notes Sessão Negada	Indica que uma sessão Lotus Notes foi negada.	3
Lotus Notes Sessão negada	Indica que uma sessão Lotus Notes está em andamento.	1
Sessão Aberta Kerberos	Indica que uma sessão Kerberos foi estabelecida.	1
Sessão Kerberos fechada	Indica que uma sessão Kerberos foi fechada.	1
Sessão Keberos reconfigurada	Indica que uma sessão do Kerberos foi reconfigurado.	3
Sessão Kerberos finalizada	Indica que uma sessão Kerberos foi finalizada.	3
Sessão Kerberos negada	Indica que uma sessão Kerberos foi negada.	3
Sessão Kerberos em andamento	Indica que uma sessão do Kerberos está em andamento.	1
Sessão IRC Aberta	Indica que uma sessão Internet Relay Chat (IRC) foi estabelecida.	1
Sessão IRC fechada	Indica que uma sessão IRC foi fechado.	1
Reconfigurar sessão IRC	Indica que uma sessão IRC foi reconfigurada	3
Sessão IRC finalizada	Indica que uma sessão IRC foi finalizada.	3
Sessão IRC negada	Indica que uma sessão IRC foi negada.	3
Sessão IRC em andamento	Indica que uma sessão IRC está em andamento.	1
Sessão IEC 104 aberta	Indica que uma sessão IEC 104 foi estabelecida.	1
Sessão IEC 104 fechada	Indica que uma sessão IEC 104 foi fechado.	1
Reconfigurar sessão IEC 104	Indica que uma sessão IEC 104 foi reconfigurada.	3
Sessão IEC 104 finalizada	Indica que uma sessão IEC 104 foi finalizado.	3
Sessão IEC 104 negada	Indica que uma sessão IEC 104 foi negada.	3
Sessão IEC 104 em andamento	Indica que uma sessão IEC 104 está em andamento.	1
Sessão Ident em aberto	Indica que uma sessão de protocolo de identidade de cliente (Ident) foi estabelecida.	1

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão Ident fechada	Indica que uma sessão Ident foi fechada.	1
Reconfigurar sessão Ident	Indica que uma sessão Ident foi reconfigurada	3
Sessão Ident finalizada	Indica que uma sessão Ident foi finalizada.	3
Sessão Ident negada	Indica que uma sessão Ident foi negada.	3
Sessão Ident em andamento.	Indica que uma sessão Ident está em andamento.	1
Sessão ICCP aberta	Indica que uma sessão Inter-Centro de Controle de Comunicações Protocol (ICCP) foi estabelecida.	1
Sessão ICCP fechada	Indica que uma sessão ICCP foi fechada.	1
Reconfigurar Sessão ICCP	Indica que uma sessão ICCP foi reconfigurada.	3
Sessão ICCP finalizada	Indica que uma sessão ICCP foi finalizada.	3
Sessão ICCP negada	Indica que uma sessão ICCP foi negada.	3
Sessão ICCP em andamento	Indica que uma sessão ICCP está em andamento.	1
GroupWiseSessão Aberta	Indica que uma sessão GroupWise foi estabelecida.	1
GroupWiseSessão fechada	Indica que uma sessão GroupWise foi encerrada.	1
GroupWiseSessão reconfigurada	Indica que uma sessão GroupWisefoi redefinida.	3
GroupWiseSessão finalizada	Indica que uma sessão GroupWisefoi encerrada.	3
GroupWiseSessão negada	Indica que uma sessão foi GroupWise negada.	3
GroupWiseSessão em andamento	Indica que uma sessão GroupWise está em andamento.	1
Sessão Gopher aberta	Indica que uma sessão Gopher foi estabelecida.	1
Sessão Gopher fechada	Indica que uma sessão Gopher foi fechada.	1
Reconfigurar sessão Gopher	Indica que uma sessão Gopher foi redefinido.	3
Sessão Gopher finalizada	Indica que uma sessão Gopher foi finalizada.	3
Sessão Gopher negada	Indica que uma sessão Gopher foi negada.	3
Sessão Gopher em andamento	Indica que uma sessão Gopher está em andamento.	1
Sessão GIOP em aberto	Indica que uma sessão GIOP (General Inter-ORB Protocol) foi estabelecida.	1
Sessão GIOP encerrada	Indica que uma sessão GIOP foi encerrada.	1
Sessão GIOP reconfigurada	Indica que uma sessão GIOP foi reconfigurada	3
Sessão GIOP finalizada	Indica que uma sessão GIOP foi finalizado.	3
Sessão GIOP negada	Indica que uma sessão GIOP foi negada.	3
Sessão GIOP em andamento	Indica que uma sessão GIOP está em andamento.	1
Sessão finger aberta	Indica que um Dedo sessão foi estabelecida.	1
Sessão Finger fechado	Indica que uma sessão Finger foi fechada.	1
Reconfigurar Sessão Finger	Indica que uma sessão Finger foi reconfigurada.	3
Sessão finger encerrada	Indica que uma sessão finger foi finalizada.	3
Sessão Finger negada	Indica que uma sessão finger foi negado.	3
Sessão finger em andamento	Indica que a sessão finger está em andamento.	1
Sessão Echo Aberta	Indica que uma sessão echo foi estabelecida.	1
Sessão Echo fechada	Indica que uma sessão Echo foi fechada.	1
Sessão Echo negada	Indica que uma sessão echo foi negada.	3
Sessão Eco em andamento	Indica que uma sessão de eco está em andamento.	1
Sessão Net remota aberta	Indica que uma sessão .NET remoto foi reconfigurada.	1
Sessão NET remota aberta	Indica que uma sessão NET remota foi fechada.	1

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Sessão .NET remota fechada	Indica que uma sessão .NET remota foi reconfigurada.	3
Sessão.NET Remota encerrada.	Indica que uma sessão .NET remoto foi encerrada.	3
Sessão remota .NET negada	Indica que uma sessão .NET remota foi negada.	3
Sessão .NET remota em andamento	Indica que uma sessão .NET remota está em andamento.	1
DNP3 Sessão Aberta	Indica que uma sessão Network Distribuído Proctologic (DNP3) foi estabelecida.	1
Sessão DNP3 encerrada	Indica que uma sessão DNP3 foi encerrada.	1
Sessão DNP3 reconfigurada	Indica que uma sessão DNP3 foi reconfigurada.	3
DNP3 Sessão finalizada	Indica que uma sessão DNP3 foi finalizado.	3
Sessão DNP3 Negada	Indica que uma sessão DNP3 foi negada.	3
Sessão DNP3 Em Andamento	Indica que uma sessão DNP3 está em andamento.	1
Sessão descartar aberta	Indica que uma sessão Descartar foi estabelecida.	1
Sessão Descartar fechada	Indica que uma sessão Descartar foi fechada.	1
Reconfigurar sessão descartar	Indica que uma sessão descartar foi redefinida.	3
Sessaão descartar finalizada	Indica que uma sessão descartar foi finalizada.	3
Sessão Descartar negada	Indica que uma sessão Descartar foi negado.	3
Sessão Descartar em andamento	Indica que uma sessão Descartar está em andamento.	1
Sessão DHCP aberta	Indica que um Protocolo de Configuração de Host Dinâmico (DHCP) foi estabelecido.	1
Sessão DHCP encerrada	Indica que uma sessão DHCP foi fechada.	1
Sessão DHCP negada.	Indica que uma sessão DHCP foi negada.	3
Sessão DHCP em andamento	Indica que uma sessão do DHCP está em andamento.	1
DHCP OK	Indica que um lease DHCP foi obtido com êxito	1
Falha DHCP	Indica que um lease DHCP não pode ser obtido.	3
Sessão Aberta CVS	Indica que um Concurrent Versions System (CVS) sessão foi estabelecida.	1
Sessão CVS fechada	Indica que uma sessão do CVS foi fechado.	1
Sessão Reconfigurar CVS	Indica que uma sessão foi redefinido CVS.	3
Sessão Terminada CVS	Indica que uma sessão CVS era finalizada.	3
Sessão Negado CVS	Indica que uma sessão do CVS foi negado.	3
Sessão CVS em andamento	Indica que uma sessão do CVS está em andamento.	1
Sessão Aberta CUPS	Indica que uma sessão comum UNIX Printing System (CUPS) foi estabelecida.	1
Sessão CUPS encerradca	Indica que uma sessão CUPS foi fechado.	1
Reconfigurar sessão CUPS	Indica que uma sessão CUPS foi redefinido.	3
Sessão CUPS finalizada	Indica que uma sessão CUPS foi finalizada.	3
Sessão CUPS negada	Indica que uma sessão CUPS foi negada.	3
Sessão CUPS em andamento	Indica que uma sessão CUPS está em andamento.	1
Sessão Chargen inicidada	Indica que a sessão Gerador de Caracteres (Chargen) foi iniciado.	1
Sessão Chargen fechada	Indica que uma sessão Chargen foi fechado.	1
Reconfigurar Chargen Sessão	Indica que uma sessão foi redefinido Chargen.	3
Sessão crhargem Terminada	Indica que uma sessão Chargen foi finalizada.	3
Sessão Negado Chargen	Indica que uma sessão Chargen foi negado.	3
Sessão Chargen	Indica que uma sessão Chargen está em andamento.	1

Tabela 32. Categorias de nível inferior e níveis de severidade para categoria do aplicativo. (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Diversa VPN	Indica que uma sessão de VPN mista foi detectada	1
Sessão Iniciada DAP	Indica que uma sessão DAP foi estabelecida.	1
Sessão Encerrada DAP	Indica que uma sessão DAP foi encerrada.	1
Sessão DAP Negado	Indica que uma sessão DAP foi negado.	3
Status da Sessão do DAP	Indica que um pedido de status da sessão DAP foi feita.	1
Sessão DAP em Andamento	Indica que uma sessão DAP está em andamento.	1
Falha de Autenticação DAP	Indica que um DAP autenticação falhou.	4
Autenticação Bem-sucedido DAP	Indica que a autenticação bem-sucedida. DAP	1
Sessão Iniciada TOR	Indica que uma sessão TOR foi estabelecida.	1
Sessão TOR fechada	Indica que uma sessão TOR foi fechado.	1
Reconfigurar Sessão TOR	Indica que uma sessão TOR foi redefinido.	3
Sessão Terminada TOR	Indica que uma sessão TOR foi finalizado.	3
Sessão TOR negada.	Indica que uma sessão TOR foi negado.	3
Sessão TOR Em Andamento	Indica que uma sessão TOR está em andamento.	1
Jogo de Sessão Iniciada	Indica que uma sessão jogo foi iniciado.	1
Jogo de Sessão fechada	Indica que uma sessão jogo foi fechado.	1
Sessão Reconfigurar Jogo	Indica que um jogo de sessão foi redefinido.	3
Sessão Terminada Jogo	Indica que uma sessão game foi finalizado.	3
Jogo Sessão Negado	Indica que um jogo de sessão foi negado.	3
Em Andamento Sessão Jogo	Indica que uma sessão jogo está em andamento.	1
Tentativa de Login de Administrador	Indica que uma tentativa de efetuar login como um usuário administrativo foi detectado.	2
Tentativa de Login do Usuário	Indica que uma tentativa de efetuar login como um usuário não administrativo foi detectado.	2
Servidor do Cliente	Indica atividade cliente / servidor.	1
Entrega de Conteúdo	Indica atividade de entrega de conteúdo.	1
Transferência de Dados	Indica uma transferência de dados.	3
Armazenamento de Dados	Indica atividade de data warehousing.	3
Serviços de Diretório	Indica fluxo de atividade.	2
Arquivo Imprimir	Indica atividade de impressão do arquivo.	1
Transferência de Arquivos	Indica transferência de arquivos.	2
Jogos	Indica atividade de jogo.	4
Saúde	Indica atividade de saúde.	1
Sistema Interna	Indica atividade do sistema interno.	1
protocolo da Internet	Indica atividade de protocolo Internet	1
Preexistente	Indica atividade de saúde.	1
Enviar Correio	Indica atividade de correio.	1
Div.	Indica atividade mista.	2
Multimídia	Indica atividade multimídia.	2
Gerenciamento de Rede	Indica atividade de gerenciamento de rede.	
P2P	Indica-to-Peer (P2P) a atividade.	4
Acesso Remoto	Indica atividade de Acesso Remoto.	3
Protocolos Routing	Indica atividade de roteamento de protocolo.	1
Protocolos de Segurança	Indica atividade de protocolo de segurança.	2
Fluxo	Indica fluxo de atividade.	2
Protocolo desconhecido	Indica atividade incomum protocolo.	3
VoIP	Indica atividade VoIP.	1
Web	Indica atividade da web.	1
ICMP	Indica atividade ICMP	1

Auditoria

A categoria auditoria contêm eventos que estão relacionados a atividade de auditoria, tais como emails ou atividades FTP.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de auditoria.

Tabela 33. categorias de baixo nível e níveis de severidade para a categoria de auditoria

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Evento de Auditoria Geral	Indica que um evento de auditoria general foi iniciado.	1
O de execução	Indica que uma tarefa de auditoria interna foi executado.	1
Cópia em massa	Indica que uma cópia em massa foi detectada.	1
Dados do Dump	Indica que um dump de dados foi detectado.	1
Importar Dados	Indica que uma importação de dados foi detectada.	1
Seleção de Dados	Indica que um processo de seleção de dados foi detectado.	1
Truncamento de Dados	Indica que o processo truncamento de dados foi detectado.	1
Atualização de Dados	Indica que o processo de atualização de dados foi detectado.	1
Execução do procedimento / disparador	Indica que o procedimento ou disparo de execução do banco de dados foi detectado.	1
Alteração de Esquema	Indica que o esquema para uma execução de procedimento ou de disparo foi alterada.	1

Risco

A categoria de risco contém eventos que estão relacionados a IBM Security QRadar Risk Manager.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados à categoria de risco.

Tabela 34. categorias de baixo nível e níveis de severidade para a categoria de auditoria

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Exposição de Política	Indica que uma exposição política foi detectada.	5
Violação de Conformidade	Indica que uma violação de conformidade foi detectado.	5
Exposição de vulnerabilidades	Indica que a rede ou dispositivo tiveram uma vulnerabilidade exposta.	9
Vulnerabilidade de Acesso Remoto	Indica que a rede ou dispositivo têm uma vulnerabilidade de acesso remoto.	9
Vulnerabilidade de Acesso Local	Indica que a rede ou dispositivo têm vulnerabilidade de acesso local.	7
Asbra o acesso wireless	Indica que a rede ou dispositivo abriram o acesso wireless.	5
Criptografia fraca	Indica que o host ou dispositivo tem a criptografia fraca.	5
Transferência de dados não criptografada	Indica que um host ou dispositivo é transmissão de dados que não está criptografada.	3
Armazenamento de dados não criptografado	Indica que o armazém de dados não está criptografada.	3
Incompatibilidade de Regra-Configurada	Indica que uma regra não está configurada corretamente.	3
Incompatibilidade de Dispositivo-Configurado	Indica que um dispositivo na rede não está configurado corretamente.	3
Os Hosts-Configurados	Indica que um host de rede não está sendo configurado corretamente.	3

Tabela 34. categorias de baixo nível e níveis de severidade para a categoria de auditoria (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Possível perda de dados	Indica que a possibilidade de perda de dados foi detectado.	5
Autenticação fraca	Indica que um host ou dispositivo está suscetível a fraude.	5
Sem senha	Indica que não existe senha.	7
Fraude	Indica que um host ou dispositivo está suscetível a fraude.	7
Possívesis destinos DoS	Indica um host ou dispositivo é um destino possível DoS.	3
Possíveis fraquezas DoS	Indica um host ou dispositivo tiver um ponto fraco DoS possível.	3
Perda de Confidencialidade	Indica que uma perda de confidencialidade foi detectado.	5
Política monitor de pontuação de risco de pontuação.	Indica que uma acumulação pontuação de risco da política de monitor foi detectado.	1

Gerenciador de risco de auditoria

A categoria de risco contém eventos que estão relacionados a IBM Security QRadar Risk Manager eventos de auditoria.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de gravidade associado para a categoria de auditoria Risk Manager.

Tabela 35. categorias de baixo nível e níveis de gravidade para a categoria de auditoria Risk Manager

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Política de Monitor	Indica que um monitor de política foi modificada.	3
Topologia	Indica que uma topologia foi modificado.	3
Simulações	Indica que uma topologia foi modificado.	3
Administração	Indica que as alterações administrativas foram feitas.	3

Controle

A categoria de controle contém eventos que estão relacionados ao seu hardware do sistema.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associado para a categoria de controle.

Tabela 36. categorias de baixo nível e níveis de severidade para a categoria de controle

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Leitura de Dispositivo	Indica que um dispositivo foi lido.	1
dispositivo de comunicação	Indica comunicação com um dispositivo.	1
Dispositivo de auditoria	Indica que um dispositivo de auditoria ocorreu.	1
Evento do Dispositivo	Indica que um evento de dispositivo.	1
Dispositivo Ping	Indica uma ação de ping para um dispositivo.	1
Configuração de Dispositivo	Indica que um dispositivo foi lido.	1
Rota de dispositivo	Indica que uma ação rotear dispositivo ocorreu.	1
Importação de dispositivo	Indica que uma importação de dispositivo ocorreu.	1
Informações sobre o Dispositivo	Indica que uma ação de informações sobre o dispositivo.	1
Aviso de Dispositivo	Indica que um aviso foi gerado em um dispositivo.	1

Tabela 36. categorias de baixo nível e níveis de severidade para a categoria de controle (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Erro do Dispositivo	Indica que um erro foi gerado em um dispositivo.	1
Retransmissão de evento	Indica um evento de retransmissão.	1
Evento NIC	Indica um potencial Interface (NIC) vulnerabilidade.	1
Evento UIQ	Indica um evento em um dispositivo móvel.	1
Eventos IMU	Indica um evento em um unidade de gerenciamento integrado (Unidade de Gerenciamento IMU).	1
Evento Faturamento	Indica um evento faturamento.	1
Evento DBMS	Indica um evento no Sistema de Gerenciamento de Banco de Dados (DBMS).	1
Importar evento	Indica que uma importação.	1
Local Importar	Indica que um local de importação.	1
Importação da Rota	Indica que uma importação de rota.	1
Exportar Evento	Indica que uma exportação ocorreu.	1
Sinal Remote	Indica um sinal remoto.	1
Status do Gateway	Indica o status do gateway.	1
Evento da Tarefa	Indica que uma tarefa ocorreu.	1
Evento de Segurança	Indica que um evento de segurança ocorreu.	1
Dispositivo de Detecção de violação	Indica que o sistema detectou uma ação de violação.	1
Evento de Tempo	Indica que um evento de tempo.	1
Comportamento suspeito	Indica que ocorreu um comportamento suspeito.	1
Interrupções de Energia	Indica que uma interrupção de disponibilidade de energia ocorreu.	1
Recuperação de Energia	Indica que a energia foi restaurada.	1
Pulsações	Indica que um ping de pulsação ocorreu.	1
Conexão Remota de Eventos	Indica uma conexão remota com o sistema.	1

Gerenciadores de perfis ativos

A categoria gerenciador de perfil ativo contêm eventos que estão relacionados aos gerenciadores de perfis ativos.

A tabela a seguir descreve as categorias de eventos de baixo nível e níveis de severidade associados ao recurso categoria do gerenciador de perfis.

Tabela 37. Categorias de baixo nível e níveis de severidade para a categoria do gerenciador de perfis

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ativo Criado	Indica que um recurso foi criado.	1
Ativo Atualizado	Indica que um ativo foi atualizado.	1
Ativo Observado	Indica que um ativo foi observado.	1
Ativo Movido	Indica que um ativo foi movido.	1
Ativo Excluído	Indica que um recurso foi excluído.	1
Ativo do host de acesso limpo	Indica que um ativo foi limpo.	1
Nome Ativo Criado	Indica que um nome de host foi criado.	1
Nome do Ativo Atualizado	Indica que um nome do host foi atualizado.	1
Nome Ativo Observado	Indica que um nome de host foi observado.	1
Nome do Ativo Movido	Indica que um nome de host foi movido.	1
Ativo do Host Excluído	Indica que um nome de host foi excluído.	1
Porta de ativos limpa	Indica que uma porta foi limpa.	1
Ativo de porta criada	Indica que uma porta foi criada.	1
Ativo de porta atualizada	Indica que uma porta foi atualizada.	1
Ativo de porta observada	Indica que uma porta foi observada.	1
Ativo porta movida	Indica que uma porta foi movida.	1

Tabela 37. Categorias de baixo nível e níveis de severidade para a categoria do gerenciador de perfis (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ativo porta excluída	Indica que uma porta foi excluída.	1
Ativo de instância de vulnerabilidade limpa	Indica que uma instância da vulnerabilidade foi limpa.	1
Ativo de instância de vulnerabilidade criado	Indica que uma instância da vulnerabilidade foi criada.	1
Ativo de instância de vulnerabilidade atualizado	Indica que um ativo de instância de vulnerabilidade afoi atualizado	1
Ativo de instância de vulnerabilidade observado	Indica que um ativo de instância de vulnerabilidade foi observado.	1
Ativo de instância de vulnerabilidade movido	Indica que um ativo de instância de vulnerabilidade foi movido	1
Ativo de instância de vulnerabilidade excluída	Indica que uma instância da vulnerabilidade foi excluída.	1
Ativo OS limpos	Indica que um sistema operacional foi limpo.	1
Ativo OS Criado	Indica que um sistema operacional foi criado.	1
Ativo propriedade atualizado	Indica que um sistema operacional foi atualizado.	1
Ativo OS observado	Indica que um sistema operacional foi observado.	1
Ativo OS movido	Indica que um sistema operacional foi movido.	1
Ativo OS excluído	Indica que um sistema operacional foi excluído.	1
Ativo de Propriedade Limpas	Indica que uma propriedade foi limpa.	1
Ativo de propriedade criado	Indica que uma propriedade foi criada.	1
Ativo de propriedades atualizado	Indica que uma propriedade foi atualizado.	1
Ativo de propriedade observado	Indica que uma propriedade foi observado.	1
Ativo de propriedade movido	Indica que uma propriedade foi movida.	1
Ativo de propriedade excluído	Indica que uma propriedade foi movida.	1
Endereço IP ativo limpo	Indica que um endereço IP foi limpo.	1
Endereço IP Ativo Criado	Indica que um endereço IP foi criado.	1
Endereço IP Ativo Atualizado	Indica que um endereço IP foi atualizado.	1
Endereço IP Ativo Observado	Indica que um endereço IP foi observado.	1
Endereço IP Ativo Movido	Indica que um endereço IP foi movido.	1
Endereço IP Ativo Excluído	Indica que um endereço IP foi excluído.	1
Ativo de Propriedade Limpas	Indica que uma interface foi limpa.	1
Ativo de interface criado	Indica que uma interface foi criada.	1
Ativo de interface atualizado	Indica que uma interface foi atualizado.	1
Ativo de interface Observado	Indica que uma interface foi observado.	1
Ativode interface Movido	Indica que uma interface foi movido.	1
Ativo de Interface Mesclados	Indica que uma interface foi mesclada.	1
Ativo de Interface Excluído	Indica que uma interface foi excluída.	1
Usuário do ativo limpo	Indica que um usuário foi limpo.	1
Usuário do ativo observado	Indica que um usuário foi observado.	1
Usuário de ativo movido	Indica que um usuário foi movido.	1
Usuário do Ativo Excluído	Indica que um usuário foi excluído.	1
Ativo de política digitalizada limpo	Indica que um ativo de política digitalizada foi limpa.	1
Ativo de política digitalizada observado	Indica que um ativo de política digitalizado foi observado.	1
Ativo de política digitalizada movido	Indica que um ativo de política digitalizado foi limpo.	1
Política de ativos digitalizados excluídos	Indica que uma política de ativos digitalizados foi excluída.	1
Aplicações de ativos Windows limpas	Indica que um aplicativo Windows foi limpo.	1
Ativo Aplicativo Windows Observado	Indica que um aplicativoWindows foi observado.	1
Aplicativo ativo em Windows movido	Indica que um aplicativo Windows foi movido.	1
Ativo aplicativo Windows excluído.	Indica que um aplicativoWindows foi excluído.	1

Tabela 37. Categorias de baixo nível e níveis de severidade para a categoria do gerenciador de perfis (continuação)

Categoria de evento de baixo nível	Descrição	Nível de severidade (0 - 10)
Ativos de serviços digitalizados limpos	Indica que ativos de serviços digitalizados foram limpos.	1
Ativos de serviços digitalizados observados	Indica que um serviço digitalizadoo foi movido.	1
Ativos de serviços digitalizados movido	Indica que um ativo de serviços digitalizados foi movido.	1
Ativos de serviços digitalizados excluídos	Indica que Ativos de serviços digitalizados foram excluídos.	1
Caminho de ativos Windows limpos.	Indica que uma correção Windows foi limpa.	1
Ativo Windows Patch Observado	Indica que um Windows correção foi observado.	1
Caminho de ativo Windows movido	Indica que ua correção Windows foi movido.	1
Patch de Ativo Windows Excluído.	Indica que uma correção Windows excluída.	1
Ativo de caminho UNIXLimpas	Indica que uma correção foi limpo UNIX.	1
Ativo UNIX Patch Observado	Indica que uma correção UNIX foi observada.	1
Asset UNIX Patch Moved	Indica que um UNIX correção foi movido.	1
Ativo de correção UNIX excluído	Indica que uma correção UNIX foi excluído.	1
Ativo correção de varredura limpo	Indica que o ativo correção de varredura foi limpo.	1
Ativo correção de varredura criado	Indica que o ativo correção de varredura foi observado.	1
Ativo correção de varredura movido	Indica que uma varredura de correção foi movida.	1
Ativo correção de varredura excluído	Indica que uma varredura de correção foi excluída.	1
Ativo correção de varredura limpo	Indica que um ativo de correção de varredura foi limpo.	1
Ativo correção de varredura criado	Indica que um ativo de correção de varredura foi limpo.	1
Ativo correção de varredura movido	Indica que uma varredura de correção foi movida.	1
Varredura de Porta ativa Excluída	Indica que uma varredura de correção foi excluída.	1
O Application Client Limpas	Indica que um aplicativo cliente foi limpo.	1
O Aplicativo Cliente Observado	Indica que um aplicativo cliente foi observado.	1
Ativo Movido Application Client	Indica que um aplicativo cliente foi movido.	1
O Aplicativo Cliente Excluído	Indica que um aplicativo cliente foi excluído.	1
Ativo Observado de Varredura de Correção	Indica que uma varredura de correção foi observado.	1
Ativo Criado de Varredura de Porta	Indica que uma varredura de correção foi observado.	1

Avisos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Marcas comerciais

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

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

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

Considerações sobre Política de Privacidade

Os produtos de Software IBM, incluindo soluções de software como serviço, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações sobre o uso do produto, para ajudar a melhorar a experiência do usuário final, ajustar as interações com o usuário final ou para outros propósitos. Em muitas casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoalmente identificáveis. Se esta Oferta de Software usar cookies para coletar informações pessoais identificáveis, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

Dependendo das configurações implementadas, essa Oferta de Software poderá usar cookies de sessão que coletam o ID da sessão de cada usuário para fins de gerenciamento de sessões e autenticação. Estes cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas para esta Oferta de Software fornecerem a capacidade de coletar, como cliente, informações pessoalmente identificáveis dos usuários finais por meio de cookies e outras tecnologias, deve-se consultar seu próprio conselho jurídico a respeito das leis aplicáveis ⌂a essa coleta de dados, incluindo quaisquer requisitos de aviso e consentimento.

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

Índice Remissivo

V