IBM Security QRadar

Guia do Usuário do Log Sources

Versão 7.2.5

IBM Security QRadar

Guia do Usuário do Log Sources

Versão 7.2.5

Nota

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 61.

Informações do produto

Este documento aplica-se ao IBM QRadar Security Intelligence Platform V7.2.4 e às liberações subsequentes, a não ser que seja substituído por uma versão atualizada.

Índice

Sobre este guia

Fontes de log são dispositivos de terceiros que enviam eventos para o IBM® Security QRadar para coleta, armazenamento, análise e processamento.

Público-alvo

Os administradores devem ter acesso ao QRadar e conhecimento da rede corporativa e das tecnologias de rede.

Documentação técnica

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

Para obter informações sobre como acessar mais documentações técnicas na biblioteca do produto 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. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que envolverá necessariamente procedimentos operacionais adicionais e podem requerer que outros sistemas, produtos ou serviços sejam mais efetivos. 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.

Capítulo 1. Introdução ao gerenciamento de fonte de log

É possível configurar o IBM Security QRadar para aceitar logs de eventos a partir de origens de log que estão em sua rede. Uma *fonte de log* é uma origem de dados que cria um log de eventos.

Por exemplo, um firewall ou eventos baseados em segurança de logs do sistema de prevenção de intrusão (IPS) e eventos baseados em rede de logs de comutadores ou roteadores.

Para receber eventos brutos de origens de log, o QRadar suporta muitos protocolos. Os *Protocolos passivos* atendem eventos em portas específicas. Os *Protocolos Ativos* utilizam APIs ou outros métodos de comunicação para conexão com sistemas externos que pesquisam e recuperam eventos.

Dependendo de seus limites de licença, o QRadar pode ler e interpretar eventos a partir de mais de 300 origens de log.

Para configurar uma fonte de log para QRadar, deve-se executar as tarefas a seguir:

1. Faça download e instale um módulo de suporte de dispositivo (DSM) que suporte a fonte de log. Um *DSM* é um aplicativo de software que contém os padrões de evento que são necessários para identificar e analisar eventos a partir do formato original do log de eventos para o formato que o QRadar pode usar. Para obter mais informações sobre DSMs e as origens de log suportadas, consulte o *Guia de Configuração de DSM.*
2. Se a descoberta automática é suportada para o DSM, aguarde QRadar para incluir automaticamente a fonte de log para sua lista de fontes de log configuradas.
3. Se a descoberta automática não for suportada para o DSM, crie manualmente a configuração da fonte de log.

Incluindo uma fonte de log

Se uma fonte de log não é descoberta automaticamente, será possível incluir manualmente uma fonte de log para receber eventos de seus dispositivos ou dispositivos de rede.

Sobre Esta Tarefa

A tabela a seguir descreve os parâmetros de fonte de log comum para todos os tipos de fonte de log:

Tabela 1. Parâmetros de fonte de log

Parâmetro	Descrição
Identificador de Origem de Log	O endereço IPv4 ou o nome do host que identificam a fonte de log. Se a sua rede contiver diversos dispositivos conectados a um console de gerenciamento único, especifique o endereço IP do dispositivo individual que criou o evento. Um identificador exclusivo para cada um deles, como um endereço IP, evita que procuras de eventos identifiquem o console de gerenciamento como a origem de todos os eventos.
Ativado	Quando esta opção não estiver ativada, a fonte de log não coletará eventos e nem será contada no limite de licença.
Credibilidade	A credibilidade é uma representação da integridade ou da validade dos eventos que são criados por uma fonte de log. O valor da credibilidade que é designado a uma fonte de log pode aumentar ou diminuir com base nos eventos recebidos ou ajustados como uma resposta às regras de eventos criadas pelo usuário. A credibilidade dos eventos das origens de log contribui com o cálculo da magnitude do crime e pode aumentar ou diminuir o valor da magnitude de um crime.
Coletor de Eventos de Destino	Especifica o QRadar Event Collector que pesquisa a origem de log remoto. Use esse parâmetro em uma implementação distribuída para melhorar o desempenho do sistema do Console ao mover a tarefa de pesquisa para um Coletor de eventos.
Unindo Eventos	Aumenta a contagem de eventos quando o mesmo evento ocorrer diversas vezes dentro de um curto intervalo de tempo. Eventos unidos permitem uma maneira de visualizar e determinar a frequência com que um tipo de evento único ocorre na guia **Atividade do Log**. Quando essa caixa de seleção estiver desmarcada, os eventos são visualizados individualmente e não são empacotados. Origens de log novas e descobertas herdam automaticamente o valor dessa caixa de seleção da configuração **Configurações do Sistema** na guia **Administrador**. É possível utilizar esta caixa de seleção para substituir o comportamento padrão das configurações do sistema para uma origem de log individual.

Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Origens de Log**.
3. Clique em **Incluir**.
4. Configure os parâmetros comuns para sua fonte de log.
5. Configure os parâmetros específicos de protocolo para sua fonte de log.
6. Clique em **Salvar**.
7. Na guia **Administrador**, clique em **Implementar Mudanças**.

Opções de configuração de protocolo JDBC

O QRadar utiliza o protocolo JDBC para coletar informações de tabelas ou visualizações que contiverem dados do evento a partir de vários tipos de banco de dados.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo JDBC:

Tabela 2. Parâmetros do protocolo JDBC

Parâmetro	Descrição
Tipo do Banco de Dados	Na caixa de listagem, selecione o tipo de banco de dados que contém os eventos.
Nome do Banco de Dados	O nome do banco de dados deve corresponder ao nome do banco de dados que é especificado no campo **Identificador de Origem de Log**.
Porta	A porta JDBC deve corresponder à porta de atendimento que está configurada no banco de dados remoto. O banco de dados deve permitir conexões TCP recebidas. Se uma **Instância de Banco de Dados** for usada com o tipo de banco de dados MSDE, o administrador deverá deixar o parâmetro de **Porta** em branco na configuração da fonte de log.
Nome do Usuário	Uma conta do usuário para o QRadar no banco de dados.
Domínio de Autenticação	Um domínio deve estar configurado para os bancos de dados MSDE que estiverem em um domínio do Windows. Se a rede não usar um domínio, deixe este campo em branco.
Instância de Banco de Dados	A instância do banco de dados, se necessário. Os bancos de dados MSDE podem incluir diversas instâncias do servidor SQL em um servidor. Quando uma porta não padrão é utilizada para o banco de dados ou o acesso é bloqueado para a porta 1434 para a resolução do banco de dados SQL, o parâmetro **Instância do Banco de Dados** deverá estar em branco na configuração da fonte de log.
Consulta Predefinida	Opcional.
Nome da tabela	O nome da tabela ou visualização que incluem os registros de eventos. O nome da tabela pode incluir os seguintes caracteres especiais: cifrão ($), sinal de número (#), sublinhado (_), traço (–) e ponto(.).

Tabela 2. Parâmetros do protocolo JDBC (continuação)

Parâmetro	Descrição
Selecionar Lista	A lista de campos a serem incluídos quando a tabela for pesquisada em busca de eventos. É possível utilizar uma lista separada por vírgulas ou digitar * para selecionar todos os campos da tabela ou visualização. Se uma lista separada por vírgulas for definida, a lista deverá conter o campo que está definido em **Comparar Campo**.
Comparar Campo	Um valor numérico ou campo de registro de data e hora da tabela ou visualização que identifica novos eventos que são incluídos na tabela entre as consultas. Permite que o protocolo identifique eventos que foram pesquisados anteriormente pelo protocolo para assegurar que eventos duplicados não sejam criados.
Usar Instruções Preparadas	Instruções preparadas permitem que a origem do protocolo JDBC configure a instrução SQL e, em seguida, execute a instrução SQL várias vezes com parâmetros diferentes. Por motivos de segurança e desempenho, a maioria das configurações do protocolo JDBC pode usar as instruções preparadas.
Data e Horário de Início	Se um horário de início não estiver definido, o protocolo tentará pesquisar eventos após a configuração de fonte de log ser salva e implementada.
Intervalo de Pesquisa	O intervalo de pesquisa padrão é de 10 segundos.
Regulador de EPS	O limite superior para o número permitido de Eventos por Segundo (EPS).
Código de idioma do banco de dados	Para instalações de diveross idiomas, use o campo **Código de idioma do banco de dados** para especificar o idioma a ser usado.
Conjunto de códigos do banco de dados	Para instalações de diveross idiomas, use o campo **Conjunto de códigos** para especificar o conjunto de caracteres a ser usado.
Usar Comunicação de Canal Nomeado	Conexões de canal nomeado para os bancos de dados MSDE requerem que o campo nome de usuário e senha use um nome de usuário e uma senha de autenticação do Windows em vez de um nome de usuário e senha do banco de dados. A configuração da fonte de log deve utilizar um canal nomeado padrão no banco de dados MSDE.
Usar NTLMv2	A caixa de seleção **Usar NTLMv2** não interrompe as comunicações das conexões MSDE que não requererem autenticação NTLMv2.

Opções de configuração do JDBC SiteProtector

É possível configurar as origens de log para usar o protocolo Java™ Database Connectivity (JDBC) SiteProtector para pesquisar remotamente por eventos no banco de dados IBM Proventia® Management SiteProtector®.

O protocolo JDBC - SiteProtector combina informações das tabelas SensorData1 e SensorDataAVP1 na criação da carga útil de fonte de log. As tabelas SensorData1 e SensorDataAVP1 estão no banco de dados IBM Proventia® Management SiteProtector®. O número máximo de linhas que o protocolo JDBC - SiteProtector consegue pesquisar em uma única consulta é 30.000.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo JDBC - SiteProtector:

Tabela 3. Parâmetros do protocolo JDBC - SiteProtector

Parâmetro	Descrição
Configuração do Protocolo	**JDBC - SiteProtector**
Tipo do Banco de Dados	Na lista, selecione **MSDE** como o tipo de banco de dados a ser utilizado para a origem de eventos.
Nome do Banco de Dados	Digite `RealSecureDB` como o nome do banco de dados ao qual o protocolo pode se conectar.
IP ou Nome do Host	O endereço IP ou o nome do host do servidor de banco de dados.
Porta	O número da porta que é utilizado pelo servidor de banco de dados. A porta de configuração do JDBC SiteProtector deve corresponder à porta do listener do banco de dados. O banco de dados deve ter conexões TCP de entrada ativadas. Se você definir uma **Instância de Banco de Dados** com o MSDE como o tipo de banco de dados, deve-se deixar o parâmetro **Porta** em branco em sua configuração de fonte de log.
Nome do Usuário	Se você desejar controlar o acesso a um banco de dados pelo protocolo JDBC, será possível criar um uso específico para seu sistema QRadar.
Domínio de Autenticação	Se selecionar MSDE e o banco de dados estiver configurado para Windows, é preciso definir um domínio do Windows. Se a rede não usar um domínio, deixe este campo em branco.
Instância de Banco de Dados	Se você selecionar o MSDE e houver diversas instâncias do servidor de SQL em um servidor, defina a instância a qual você deseja se conectar. Se uma porta não padrão for utilizada na configuração do seu banco de dados ou o acesso está bloqueado à porta 1434 para a resolução do banco de dados SQL, deve-se deixar o parâmetro **Instância do Banco de Dados** em branco na sua configuração.
Consulta Predefinida	A consulta predefinida do banco de dados para sua fonte de log. As consultas de banco de dados predefinidas estão disponíveis apenas para conexões com a fonte de log especial.
Nome da tabela	`SensorData1`
Nome da Visualização de AVP	`SensorDataAVP`
Nome da Visualização de Resposta	`SensorDataResponse`
Selecionar Lista	Digite `*` para incluir todos os campos na tabela ou visualização.
Comparar Campo	`SensorDataRowID`

Tabela 3. Parâmetros do protocolo JDBC - SiteProtector (continuação)

Parâmetro	Descrição
Usar Instruções Preparadas	Instruções preparadas permitem que a origem do protocolo JDBC configurem a instrução SQL e, em seguida, executem a instrução SQL várias vezes com parâmetros diferentes. Por motivos de segurança e desempenho, utilize as instruções preparadas. É possível desmarcar essa caixa de seleção para utilizar um método alternativo de consulta que não utiliza instruções pré-compiladas.
Incluir Eventos de Auditoria	Especifica para coletar eventos de auditoria do IBM SiteProtector®.
Data e Horário de Início	Opcional. Uma data e hora de início para quando o protocolo pode começar a pesquisar o banco de dados.
Intervalo de Pesquisa	A quantia de tempo entre as consultas para a tabela de eventos. É possível definir um intervalo de pesquisa maior ao anexar H para horas ou M para minutos ao valor numérico. Os valores numéricos sem uma pesquisa de designador H ou M em segundos.
Regulador de EPS	O número de Eventos por Segundo (EPS) que você não deseja que esse protocolo exceda.
Código de idioma do banco de dados	Para instalações de diveross idiomas, use o campo **Código de idioma do banco de dados** para especificar o idioma a ser usado.
Conjunto de códigos do banco de dados	Para instalações de diveross idiomas, use o campo **Conjunto de códigos** para especificar o conjunto de caracteres a ser usado.
Usar Comunicação de Canal Nomeado	Se você selecionar o MSDE como o tipo de banco de dados, marque essa caixa de seleção para utilizar um método alternativo para uma conexão de porta TCP/IP. Ao usar uma conexão de canal nomeado, o nome de usuário e a senha devem ser o nome de usuário e a senha de autenticação apropriados do Windows e não o nome de usuário e senha do banco de dados. A configuração da fonte de log deve utilizar o canal nomeado padrão.
Nome do Cluster do Banco de Dados	O nome do cluster para assegurar que as comunicações de canal nomeado funcionem corretamente.
Usar NTLMv2	Força as conexões MSDE a usarem o protocolo NTLMv2 com servidores SQL que requerem autenticação NTLMv2. A caixa de seleção **Usar NTLMv2** não interrompe as comunicações das conexões MSDE que não requererem autenticação NTLMv2.
Usar SSL	Ativa a criptografia SSL para o protocolo JDBC.
Idioma de Origem do Log	Selecione o idioma dos eventos que são gerados pela fonte de log. O idioma da fonte de log ajuda o sistema a analisar eventos a partir de dispositivos ou sistemas operacionais externos que possam criar eventos em diversos idiomas.

Opções de configuração de protocolo Sophos Enterprise Console JDBC

Para receber eventos dos Sophos Enterprise Consoles, configure uma fonte de log para utilizar o protocolo Sophos Enterprise Console JDBC.

O protocolo Sophos Enterprise Console JDBC combina as informações de carga útil a partir dos logs do controle de aplicativo, logs de controle de dispositivo, logs de controle de dados, logs de proteção contra violação e logs de firewall na tabela vEventsCommonData. Se o Sophos Enterprise Console não tiver o Sophos Reporting Interface, será possível utilizar o protocolo JDBC padrão para coletar eventos de antivírus.

A tabela a seguir descreve os parâmetros para o protocolo Sophos Enterprise Console JDBC:

Tabela 4. Parâmetros do protocolo Sophos Enterprise Console JDBC

Parâmetro	Descrição
Configuração do Protocolo	**Sophos Enterprise Console JDBC**
Tipo do Banco de Dados	**MSDE**
Nome do Banco de Dados	O nome do banco de dados deve corresponder ao nome do banco de dados que é especificado no campo **Identificador de Origem de Log**.
Porta	A porta padrão para o MSDE no Sophos Enterprise Console é 1168. A porta de configuração JDBC deve corresponder à porta do listener do banco de dados Sophos para se comunicar com QRadar. O banco de dados Sophos deve ter conexões TCP de entrada ativadas. Se uma **Instância de Banco de Dados** for usada com o tipo de banco de dados MSDE, deve-se deixar o parâmetro **Porta** em branco.
Domínio de Autenticação	Se a rede não usar um domínio, deixe este campo em branco.
Instância de Banco de Dados	A instância do banco de dados, se necessário. Os bancos de dados MSDE podem incluir diversas instâncias do servidor SQL em um servidor. Quando uma porta não padrão é utilizada para o banco de dados ou os administradores bloquearem o acesso à porta 1434 para a resolução do banco de dados SQL, o parâmetro **Instância do Banco de Dados** deverá estar em branco.
Nome da tabela	`vEventsCommonData`
Selecionar Lista	*
Comparar Campo	`InsertedAt`
Usar Instruções Preparadas	Instruções preparadas permitem que a origem do protocolo configure a instrução SQL e, em seguida, execute a instrução SQL várias vezes com parâmetros diferentes. Por motivos de segurança e desempenho, a maioria das configurações pode usar as instruções preparadas. Desmarque essa caixa de seleção para utilizar um método alternativo de consulta que não utilize instruções pré-compiladas.
Data e Horário de Início	Opcional. Uma data e hora de início para quando o protocolo pode começar a pesquisar o banco de dados. Se um horário de início não estiver definido, o protocolo tentará pesquisar eventos após a configuração de fonte de log ser salva e implementada.

Tabela 4. Parâmetros do protocolo Sophos Enterprise Console JDBC (continuação)

Parâmetro	Descrição
Intervalo de Pesquisa	O intervalo de pesquisa, que é a quantia de tempo entre as consultas para o banco de dados. É possível definir um intervalo de pesquisa maior ao anexar H para horas ou M para minutos ao valor numérico. O intervalo máximo de pesquisa é 1 semana em qualquer formato de horário. Os valores numéricos sem uma pesquisa de designador H ou M em segundos.
Regulador de EPS	O número de Eventos por Segundo (EPS) que você não deseja que esse protocolo exceda.
Usar Comunicação de Canal Nomeado	Se o MSDE estiver configurado como o tipo de banco de dados, os administradores poderão marcar essa caixa de seleção para utilizar um método alternativo para uma conexão de porta TCP/IP. As conexões de canal nomeadas para os bancos de dados MSDE requerem que o campo de nome de usuário e senha use um nome de usuário e uma senha de autenticação do Windows e não o nome de usuário e a senha do banco de dados. A configuração da fonte de log deve utilizar um canal nomeado padrão no banco de dados MSDE.
Nome do Cluster do Banco de Dados	Se você utilizar seu servidor SQL em um ambiente em cluster, defina o nome do cluster para assegurar que as comunicações de canal nomeado funcionem corretamente.
Usar NTLMv2	Força as conexões MSDE a usarem o protocolo NTLMv2 com servidores SQL que requerem autenticação NTLMv2. O valor padrão da caixa de seleção é selecionado. A caixa de seleção **Usar NTLMv2** não interrompe as comunicações das conexões MSDE que não requererem autenticação NTLMv2.

Opções de configuração de protocolo Juniper Networks NSM

Para receber os eventos de log do Juniper Networks NSM e do Juniper Networks Secure Service Gateway (SSG), configure uma fonte de log para usar protocolo Juniper Networks NSM.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo Juniper Networks Network and Security Manager:

Tabela 5. Parâmetros de protocolo Juniper Networks NSM

Parâmetro	Descrição
Tipo de origem de log	**Juniper Networks Network and Security Manager**
Configuração do Protocolo	**Juniper NSM**

Opções de configuração de protocolo OPSEC/LEA

Para receber eventos na porta 18484, configure uma fonte de log para utilizar o protocolo OPSEC/LEA é um protocolo.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo OPSEC/LEA:

Tabela 6. Parâmetros do protocolo OPSEC/LEA

Parâmetro	Descrição
Configuração do Protocolo	**OPSEC/LEA**
Porta do Servidor	Deve-se verificar se o QRadar pode se comunicar na porta 18184 utilizando o protocolo OPSEC/LEA.
Intervalo do Relatório de Estatísticas	O intervalo, em segundos, durante o qual o número de eventos do syslog é registrado no arquivo `qradar.log`.
Atributo SIC de Objeto de Aplicativo OPSEC (Nome do SIC)	O nome do Seguro de Comunicação Interna (SIC) é o nome distinto (DN) do aplicativo, por exemplo: `CN=LEA, o=fwconsole..7psasx`.
Atributo SIC da Origem de Log (Nome do SIC de Entidade)	O nome SIC do servidor, por exemplo: `cn=cp_mgmt,o=fwconsole.7 psasx`.
Aplicativo OPSEC	O nome do aplicativo que faz a solicitação de certificado.

Opções de configuração de protocolo SDEE

É possível configurar uma fonte de log para utilizar o protocolo Security Device Event Exchange (SDEE). O QRadar utiliza o protocolo para coletar eventos a partir de dispositivos que utilizam servidores SDEE.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo SDEE:

Tabela 7. Parâmetros do protocolo SDEE

Parâmetro	Descrição
Configuração do Protocolo	**SDEE**
URL	A URL HTTP ou HTTPS que são necessárias para acessar a fonte de log, por exemplo, https:// www.mysdeeserver.com/cgi-bin/sdee-server. Para SDEE/CIDEE (Cisco IDS v5.x e superior), a URL deve terminar com `/cgi-bin/sdee-server`. Para administradores com RDEP (Cisco IDS v4.x e superior), a URL deve terminar com `/cgi-bin/event-server`.
Forçar Assinatura	Quando a caixa de seleção for marcada, o protocolo força o servidor a eliminar o mínimo de conexões ativas e aceitar uma nova conexão de assinatura SDEE para a origem do log.
Espera Máxima para Bloqueio de Eventos	Quando uma solicitação de coleta é feita e nenhum evento novo estiver disponível, o protocolo permite um bloqueio de eventos. O bloqueio evita que outra solicitação de evento seja feita em um dispositivo remoto que não tinha nenhum novo evento. Esse tempo limite é destinado a conservar recursos do sistema.

Opções de configuração de protocolo SNMPv2

É possível configurar uma fonte de log para utilizar o protocolo SNMPv2 para receber eventos SNMPv2.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo SNMPv2:

Tabela 8. Parâmetros do protocolo SNMPv2

Parâmetro	Descrição
Configuração do Protocolo	**SNMPv3**
Comunidade	O nome da comunidade do SNMP que é necessária para acessar o sistema que contém eventos SNMP.
Incluir OIDs na Carga Útil do Evento	Especifica que a carga útil do evento SNMP seja construída utilizando os pares nome-valor em vez do formato de carga útil de eventos. Ao selecionar origens de log específicas na lista **Tipos de Origem de Log**, OIDs na carga útil do evento são requeridas para processamento de eventos SNMPv2 ou SNMPv3.

Opções de configuração de protocolo SNMPv3

É possível configurar uma fonte de log para utilizar o protocolo SNMPv3 para receber eventos do SNMPv3.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo do SNMPv3:

Tabela 9. Parâmetros do protocolo SNMPv3

Parâmetro	Descrição
Configuração do Protocolo	**SNMPv3**
Protocolo de Autenticação	Os algoritmos a serem utilizados para autenticar os traps SNMP:
Incluir OIDs na Carga Útil do Evento	Especifica que a carga útil do evento SNMP é construída utilizando os pares nome-valor em vez do formato de carga útil de eventos padrão. Ao selecionar origens de log específicas na lista **Tipos de Origem de Log**, OIDs na carga útil do evento são requeridas para processamento de eventos SNMPv2 ou SNMPv3.

Opções de configuração de protocolo Sourcefire Defense Center Estreamer

Para receber eventos a partir de um serviço Sourcefire Defense Center Estreamer (Event Streamer), configure uma fonte de log para utilizar o protocolo Sourcefire Defense Center Estreamer.

Os arquivos de eventos são transmitidos para o QRadar para serem processados após o Sourcefire Defense Center DSM ser configurado.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo Sourcefire Defense Center Estreamer:

Tabela 10. Parâmetros do protocolo Sourcefire Defense Center Estreamer

Parâmetro	Descrição
Configuração do Protocolo	**Sourcefire Defense Center Estreamer**
Porta do Servidor	A porta padrão que o QRadar utiliza para o Sourcefire Defense Center Estreamer é 8302.

Tabela 10. Parâmetros do protocolo Sourcefire Defense Center Estreamer (continuação)

Parâmetro	Descrição
Nome do Arquivo Keystore	O caminho do diretório e o nome do arquivo para a chave privada do keystore e para o certificado associado. Por padrão, o script de importação cria o arquivo keystore no seguinte diretório: `/opt/qradar/conf/estreamer.keystore`.
Nome do Arquivo de Armazenamento Confiável	O arquivo de armazenamento confiável contém os certificados que são confiáveis pelo cliente. Por padrão, o script de importação cria o arquivo de armazenamento confiável no seguinte diretório: `/opt/qradar/conf/estreamer.truststore`.
Solicitar dados extras	Selecione essa opção para solicitar dados extras do Sourcefire Defense Center Estreamer, por exemplo, dados extras incluem o endereço IP original de um evento.
Usar Solicitações estendidas	Selecione essa opção para usar um método alternativo para recuperar eventos de uma fonte eStreamer. Solicitações estendidas são suportadas no Sourcefire DefenseCenter Estreamer versão 5.0 ou mais recente.

Opções de configuração de protocolo de arquivo de log

Para receber eventos a partir de hosts remotos, configure uma fonte de log para usar o protocolo de arquivo de log.

O protocolo de arquivo de log é destinado a sistemas que gravam diariamente logs de eventos. Não é apropriado utilizar o protocolo de arquivo de log para dispositivos que anexam informações a seus arquivos de eventos.

Os arquivos de log são recuperados um de cada vez. O protocolo de arquivo de log pode gerenciar o texto simples, arquivos compactados ou archives. Os archives devem conter arquivos de texto simples que podem ser processados uma linha de cada vez. Quando o protocolo de arquivo de log faz download de um arquivo de evento, as informações que são recebidas no arquivo atualizam a guia **Atividade do Log**. Se mais informações forem gravadas no arquivo após o download ser concluído, as informações anexadas não são processadas.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo Arquivo de Log:

Tabela 11. Parâmetros de protocolo de arquivo de log

Parâmetro	Descrição
Configuração do Protocolo	**Arquivo de Log**
Porta Remota	Se o host remoto utilizar um número de porta não padrão, deve-se ajustar o valor da porta para recuperar eventos.
Arquivo-chave de SSH	O caminho para a chave SSH, se o sistema estiver configurado para utilizar a autenticação de chave. Quando um arquivo-chave SSH é utilizado, o campo **Senha Remota** será ignorado.

Tabela 11. Parâmetros de protocolo de arquivo de log (continuação)

Parâmetro	Descrição
Diretório Remoto	Por FTP, se os arquivos de log estão no usuário remoto do diretório inicial, você pode deixar o diretório remoto em branco. Um campo de diretório remoto em branco suporta sistemas em que uma mudança no comando de diretório ativo (CWD) é restrita.
Recursivo	Esta opção é ignorada para as transferências de arquivos SCP.
Padrão do Arquivo de FTP	A expressão regular (regex) necessária para identificar os arquivos para download a partir do host remoto.
Modo de Transferência por FTP	Para transferências ASCII no FTP, deve-se selecionar `NONE` no campo **Processador** e `LINEBYLINE` no campo **Gerador de Evento**.
Recorrência	O intervalo de tempo para determinar com que frequência o diretório remoto é varrido em busca de novos arquivos de log de evento. O intervalo de tempo pode incluir valores em horas (H), minutos (M) ou dias (D). Por exemplo, UMA recorrência de 2H varre o diretório remoto a cada 2 horas.
Executar no Salvamento	Inicia a importação do arquivo de log imediatamente após a configuração da fonte de log ser salva. Quando selecionada, esta caixa de opções limpa a lista de arquivos transferidos por download e processados anteriormente. Após a importação do primeiro arquivo, o protocolo de arquivo de log segue o horário de início e o planejamento de recorrência que é definido pelo administrador.
Regulador de EPS	O número de Eventos por Segundo (EPS) que o protocolo não pode exceder.
Alterar Diretório Local?	Altera o diretório local no **Coletor de Eventos de Destino** para armazenar os logs de eventos antes de serem processados.
Diretório Local	O diretório local no **Coletor de Eventos de Destino**. O diretório deverá existir antes de o protocolo de arquivo de log tentar recuperar eventos.
Codificação de Arquivo	A codificação de caracteres usada pelos eventos em seu arquivo de log.
Separador de Pasta	O caractere que é utilizado para separar as pastas para seu sistema operacional. A maioria das configurações pode utilizar o valor padrão no campo **Separador de pasta**. Este campo é destinado a sistemas operacionais que utilizam um caractere diferente para definir pastas separadas. Por exemplo, pontos que separam as pastas em sistemas mainframe.

Opções de configuração de protocolo Microsoft Security Event Log

É possível configurar uma fonte de log para usar o protocolo Microsoft Security Event Log. É possível usar a Instrumentação de Gerenciamento do Windows (WMI) da Microsoft para coletar logs de eventos customizados ou Logs de eventos do Windows sem agente.

A API WMI requer que as configurações de firewall aceitem comunicações externas recebidas na porta 135 e em quaisquer portas dinâmicas que forem necessárias para o DCOM. A lista a seguir descreve as limitações de fonte de log usadas no protocolo Microsoft Security Event Log:

- Os sistemas que excederem 50 eventos por segundo (eps) podem exceder os recursos deste protocolo. Utilize WinCollect para sistemas que excederem 50 eps.
- Uma instalação integrada do QRadar pode suportar até 250 origens de log com o protocolo Microsoft Security Event Log.
- Os Coletores de eventos dedicados podem suportar até 500 origens de log usando o protocolo Microsoft Security Event Log.

O protocolo Microsoft Security Event Log não é recomendável para servidores remotos acessados por meio de links de rede, por exemplo, os sistemas com altos tempos de atraso de roundtrip, como as redes lentas de longa distância ou via satélite. É possível confirmar atraso de roundtrip, examinando os pedidos e tempo de resposta que estiverem entre um ping do servidor. Os atrasos de rede que forem criados por conexões lentas diminuem o rendimento de EPS disponível para esses servidores remotos. Além disso, a coleção de eventos a partir de servidores ocupados ou controladores de domínio depende dos tempos de atraso de roundtrip baixos para acompanhar os eventos de entrada. Se não for possível diminuir o tempo de atraso de roundtrip da rede, o WinCollect poderá ser utilizado para processar eventos do Windows.

O Microsoft Security Event Log suporta as versões de software a seguir com a API de Instrumentação de Gerenciamento do Windows (WMI) da Microsoft:

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R3
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo Microsoft Security Event Log:

Tabela 12. Parâmetros do protocolo Microsoft Security Event Log

Parâmetro	Descrição
Configuração do Protocolo	**Windows Security Event Log**

Opções de configuração de protocolo Microsoft DHCP

Para receber eventos dos servidores Microsoft DHCP, configure uma fonte de log para usar o protocolo Microsoft DHCP.

Para ler os arquivos de log, os caminhos de pastas que contiverem um compartilhamento administrativo (C$), solicite privilégios NetBIOS no compartilhamento administrativo (C$). Os administradores locais ou de domínio possuem privilégios suficientes para acessar os arquivos de log em compartilhamentos administrativos.

Os campos para o protocolo Microsoft DHCP que suportam caminhos de arquivos permitem que os administradores definam uma letra da unidade com as

informações de caminho. Por exemplo, o campo pode conter o diretório `c$/LogFiles/` para um compartilhamento administrativo ou o diretório `LogFiles/` para um caminho de pasta de compartilhamento público, mas não pode conter o diretório `c:/LogFiles`.

Restrição: O protocolo de autenticação NTLMv2 da Microsoft não é suportado pelo protocolo Microsoft DHCP.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo Microsoft DHCP:

Tabela 13. Parâmetros do protocolo Microsoft DHCP

Parâmetro	Descrição
Configuração do Protocolo	**Microsoft DHCP**
Domínio	Opcional.
Caminho da Pasta	O caminho do diretório para os arquivos de log DHCP.
Padrão do Arquivo	A expressão regular (regex)que identifica os logs de eventos. Os arquivos de log devem conter uma abreviação de três caracteres para um dia da semana. Use um dos padrões de arquivo a seguir: • Padrão de arquivo IPv4: `DhcpSrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri| Sat)\.log`. • Padrão de arquivo IPv6: `DhcpV6SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) \.log`. • Padrão do arquivo IPv4 e IPv6 combinados: `Dhcp.*SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`.

Opções de configuração de protocolo Microsoft Exchange

Para receber eventos do SMTP, OWA e servidores do Microsoft Exchange 2007 e 2010, configure uma fonte de log para usar o protocolo Microsoft Windows Exchange para suportar.

Para ler os arquivos de log, os caminhos de pastas que contiverem um compartilhamento administrativo (C$), solicite privilégios NetBIOS no compartilhamento administrativo (C$). Os administradores locais ou de domínio possuem privilégios suficientes para acessar os arquivos de log em compartilhamentos administrativos.

Os campos para o protocolo Microsoft Exchange que suportam os caminhos de arquivo permitem que os administradores definam uma letra da unidade com as informações de caminho. Por exemplo, o campo pode conter o diretório `c$/LogFiles/` para um compartilhamento administrativo ou o diretório `LogFiles/` para um caminho de pasta de compartilhamento público, mas não pode conter o diretório `c:/LogFiles`.

Importante: O protocolo Microsoft Exchange não suporta o Microsoft Exchange 2003 nem o protocolo de autenticação NTLMv2 Session da Microsoft.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo Microsoft Exchange:

Tabela 14. Parâmetros do protocolo Microsoft Exchange

Parâmetro	Descrição
Configuração do Protocolo	**Microsoft Exchange**
Domínio	Opcional.
Caminho de Pasta do Log do SMTP	Quando o caminho da pasta for limpo, a coleta de eventos SMTP estará desativada.
Caminho de Pasta do Log do OWA	Quando o caminho da pasta for limpo, a coleta de eventos do OWA será desativada.
Caminho de Pasta do Log do MSGTRK	O rastreamento de mensagens está disponível nos servidores Microsoft Exchange 2007 ou 2010 designados à função de servidor de Hub Transport, Mailbox ou Edge Transport.
Padrão do Arquivo	A expressão regular (regex) que identifica os logs de eventos. O padrão é `.*\.(?:log|LOG)`.
Forçar Leitura de Arquivo	Se a caixa de seleção estiver desmarcada, o arquivo de log será lido apenas quando oQRadar detectar uma mudança no horário ou no tamanho do arquivo modificado.
Eventos Reguladores/ Segundo	O número máximo de eventos que o protocolo Exchange pode encaminhar por segundo.

Opções de configuração de protocolo Microsoft IIS

É possível configurar uma fonte de log para utilizar o protocolo Microsoft IIS. Este protocolo suporta um único ponto de coleta para arquivos de log no formato W3C que estão localizados em um servidor da web Microsoft IIS.

Para ler os arquivos de log, os caminhos de pastas que contiverem um compartilhamento administrativo (C$), solicite privilégios NetBIOS no compartilhamento administrativo (C$). Os administradores locais ou de domínio possuem privilégios suficientes para acessar os arquivos de log em compartilhamentos administrativos.

Os campos para o protocolo Microsoft IIS que suportam os caminhos de arquivo permitem que os administradores definam uma letra da unidade com as informações de caminho. Por exemplo, o campo pode conter o diretório `c$/LogFiles/` para um compartilhamento administrativo ou o diretório `LogFiles/` para um caminho de pasta de compartilhamento público, mas não pode conter o diretório `c:/LogFiles`.

Restrição: O protocolo de autenticação NTLMv2 da Microsoft não é suportado pelo protocolo Microsoft IIS.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo Microsoft IIS:

Tabela 15. Parâmetros do protocolo Microsoft IIS

Parâmetro	Descrição
Configuração do Protocolo	**Microsoft IIS**
Padrão do Arquivo	A expressão regular (regex) que identifica os logs de eventos.
Eventos Reguladores/ Segundo	O número máximo de eventos que o protocolo IIS pode encaminhar por segundo.

Opções de configuração de protocolo SMB Tail

É possível configurar uma fonte de log para utilizar o protocolo SMB Tail. Utilize esse protocolo para ver os eventos em um compartilhamento Samba remoto e receber eventos do compartilhamento Samba quando novas linhas forem incluídas no log de eventos.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo SMB Tail:

Tabela 16. Parâmetros do protocolo SMB Tail

Parâmetro	Descrição
Configuração do Protocolo	**SMB Tail**
Caminho de Pasta do Log	O caminho do diretório para acessar os arquivos de log. Por exemplo, os administradores podem utilizar o diretório `c$/LogFiles/` para um compartilhamento administrativo, ou o diretório `LogFiles/` para um caminho de pasta de compartilhamento público. No entanto, o diretório `c:/LogFiles` não é um caminho de pasta de log suportado. Se um caminho de pasta de log contiver um compartilhamento administrativo (C$), os usuários com acesso NetBIOS no compartilhamento administrativo (C$) terão os privilégios que são necessários para ler os arquivos de log. Privilégios de administrador de sistema local ou de domínio também são suficientes para acessar arquivos de log que estão em um compartilhamento administrativo.
Padrão do Arquivo	A expressão regular (regex) que identifica os logs de eventos.
Forçar Leitura de Arquivo	Se a caixa de seleção estiver desmarcada, o arquivo de log será lido apenas quando oQRadar detectar uma mudança no horário ou no tamanho do arquivo modificado.
Eventos Reguladores/ Segundo	O número máximo de eventos que o protocolo SMB Tail encaminha por segundo.

Opções de configuração de protocolo EMC VMware

Para receber dados do evento a partir do serviço da web de VMWare para ambientes virtuais, configure uma fonte de log para usar o protocolo EMC VMWare.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo EMC VMware:

Tabela 17. Parâmetros do protocolo EMC VMware

Parâmetro	Descrição
Configuração do Protocolo	**EMC VMware**
Identificador de Origem de Log	O valor desse parâmetro deve corresponder ao parâmetro **IP do VMware**.
IP do VMware	O endereço IP do servidor VMWare ESXi, por exemplo, `1.1.1.1`. O protocolo VMware anexa o endereço IP de seu servidor VMware ESXi com o HTTPS antes de o protocolo solicitar dados do evento.

Opções de configuração de protocolo Oracle Database Listener

Para coletar remotamente os arquivos de log que são gerados a partir de um servidor de banco de dados Oracle, configure uma fonte de log para utilizar a origem do protocolo Oracle Database Listener.

Antes de configurar o protocolo Oracle Database Listener para monitorar arquivos de log para processamento, você deverá obter o caminho do diretório para os arquivos de log do banco de dados Oracle.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo Oracle Database Listener:

Tabela 18. Parâmetros do protocolo Oracle Database Listener

Parâmetro	Descrição
Configuração do Protocolo	**Listener de Banco de Dados Oracle**
Padrão do Arquivo	A expressão regular (regex) que identifica os logs de eventos.

Opções de configuração de protocolo Cisco NSEL

Para monitorar fluxos de pacote NetFlow a partir de um Cisco Adaptive Security Appliance (ASA), configure a origem do protocolo Cisco Network Security Event Logging (NSEL).

Para integrar o Cisco NSEL com QRadar, deverá ser criada manualmente uma fonte de log para receber eventos NetFlow. O QRadar não descobre ou cria automaticamente origens de log para eventos syslog a partir do Cisco NSEL. Para obter mais informações, consulte o *Guia de Configuração do DSM*.

A tabela a seguir descreve os Parâmetros específicos de protocolo para o protocolo de Cisco NSEL:

Tabela 19. Parâmetros do protocolo Cisco NSEL

Parâmetro	Descrição
Configuração do Protocolo	**Cisco NSEL**
Identificador de Origem de Log	Se a rede contiver dispositivos conectados a um console de gerenciamento, será possível especificar o endereço IP do dispositivo individual que criou o evento. Um identificador exclusivo para cada um deles, como um endereço IP, evita que procuras de eventos identifiquem o console de gerenciamento como a origem de todos os eventos.
Porta do Coletor	O número da porta UDP que utiliza o Cisco ASA para encaminhar eventos de NSEL. O QRadar usa a porta 2055 para dados de fluxo no QRadar QFlow Collectors. Deve-se designar uma porta UDP diferente no Cisco Adaptive Security Appliance para NetFlow.

Opções de configuração de protocolo PCAP Syslog Combination

Para coletar eventos a partir de dispositivos Juniper Networks SRX Series que encaminham dados de captura de pacote (PCAP), configure uma fonte de log para usar o protocolo PCAP Syslog Combination.

Antes de configurar uma fonte de log que utiliza o protocolo PCAP Syslog Combination, determine a porta do PCAP de saída que é configurada no dispositivo Juniper Networks SRX. Os dados de PCAP não podem ser encaminhados para a porta 514.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo PCAP Syslog Combination:

Tabela 20. Parâmetros do protocolo PCAP Syslog Combination.

Parâmetro	Descrição
Configuração do Protocolo	**PCAP Syslog Combination**
Porta de PCAP Recebido	Se a porta do PCAP de saída for editada no dispositivo Juniper Networks SRX Series, deve-se editar a fonte de log para atualizar a entrada da Porta do PCAP. Depois de editar o campo **Porta PCAP de Entrada**, deve-se implementar as alterações.

Opções de configuração de protocolo redirecionado

Para receber eventos de outro Console em sua implementação, configure uma fonte de log para utilizar o Protocolo redirecionado.

O Protocolo redirecionado geralmente é utilizado para redirecionar eventos para outro Console QRadar. Por exemplo, Console A possui Console B configurado como um destino externo. Dados de origens de log automaticamente descobertos são encaminhados para o Console B. Criadas manualmente, as origens de log no Console A também devem ser incluídas como fonte de log para o Console B com o Protocolo redirecionado.

Opções de configuração de protocolo syslog TLS

Para receber eventos syslog criptografados de até 50 dispositivos de rede que suportam o encaminhamento de eventos de TLS Syslog, configure uma fonte de log para usar o protocolo TLS Syslog.

A fonte de log cria uma porta de atendimento para receber eventos de TLS Syslog e gera um arquivo de certificado para os dispositivos de rede. Até 50 dispositivos de rede podem encaminhar eventos à porta de atendimento criada para a fonte de log. Se desejar mais de 50 dispositivos de rede, crie portas de atendimento adicionais.

A tabela a seguir descreve os parâmetros específicos para o protocolo TLS Syslog:

Tabela 21. Parâmetros de protocolo syslog TLS

Parâmetro	Descrição
Configuração do Protocolo	**TLS Syslog**
Porta de Atendimento do TLS	A porta de atendimento TLS padrão é 6514.

Tabela 21. Parâmetros de protocolo syslog TLS (continuação)

Parâmetro	Descrição
Modo de autenticação	O modo pelo qual sua conexão TLS é autenticada. Se selecionar a opção **Autenticação de cliente e de TLS**, você deverá configurar os parâmetros de certificado.
Caminho do certificado de cliente	O caminho absoluto no disco para o certificado de cliente. O certificado deve estar armazenado no Console ou no Coletor de eventos da fonte de log.
Tipo de certificado	O tipo de certificado a ser utilizado na autenticação. Se selecionar a opção **Fornecer certificado**, é preciso configurar os caminhos de arquivo para o certificado do servidor e para a chave privada.
Caminho fornecido do certificado do servidor	O caminho absoluto para o certificado do servidor.
Caminho fornecido para a chave privada	O caminho absoluto para a chave privada. **Nota:** A chave privada correspondente deve ser uma chave PKCS8 codificada em DER. A configuração falha com qualquer outro formato de chave.

Casos de uso do TLS syslog

Os casos de uso a seguir representam configurações possíveis de serem criadas:

Autenticação de cliente
É possível fornecer um certificado de cliente que permita que o protocolo participe da autenticação de cliente. Caso selecione esta opção e forneça o certificado, as conexões recebidas são validadas com relação ao certificado de cliente.

Certificado do servidor fornecido pelo usuário
É possível configurar seu próprio certificado do servidor e a chave privada correspondente. O provedor de TLS Syslog configurado usa o certificado e a chave. Conexões recebidas são apresentadas com o certificado fornecido pelo usuário, em vez do certificado de TLS Syslog gerado automaticamente.

Autenticação padrão
Para usar o método de autenticação padrão, use os valores padrão para os parâmetros **Modo de autenticação** e **Tipo de certificado**. Após a fonte de log ser salva, um certificado `syslog-tls` será criado para o dispositivo de fonte de log. O certificado deve ser copiado para qualquer dispositivo em sua rede que encaminha dados syslog criptografados.

Opções de configuração de protocolo Juniper Security Binary Log Collector

É possível configurar uma fonte de log para utilizar o protocolo Security Binary Log Collector. Com este protocolo, os dispositivos Juniper podem enviar eventos de auditoria, sistema, firewall e sistema de prevenção de intrusão (IPS) em formato binário para o QRadar.

O formato de log binário a partir de dispositivos Juniper SRX ou J Series é fluído utilizando o protocolo UDP. Deve-se especificar uma porta exclusiva para eventos em formato binário de fluxo. A porta syslog padrão 514 não pode ser utilizada

para eventos no formato binário. A porta padrão que é designada para receber fluxo de eventos binários a partir de dispositivos Juniper é a porta 40798.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo Juniper Security Binary Log Collector:

Tabela 22. Parâmetros do protocolo Juniper Security Binary Log Collector

Parâmetro	Descrição
Configuração do Protocolo	**Security Binary Log Collector**
Local do Arquivo de Modelo XML	O caminho para o arquivo XML utilizado para decodificar o fluxo binário do seu dispositivo Juniper SRX ou Juniper J Series. Por padrão, o módulo de suporte de dispositivo (DSM) inclui um arquivo XML para decodificar o fluxo binário. O arquivo XML está no seguinte diretório: `/opt/qradar/conf/security_log.xml`.

Opções de configuração de protocolo syslog multilinhas UDP

Para criar um evento único syslog a partir de um evento multilinhas, configure uma fonte de log para utilizar o protocolo multilinhas UDP. O protocolo syslog multilinhas UDP utiliza uma expressão regular para identificar e remontar as mensagens do syslog multilinhas na carga útil do evento única.

O evento original deve conter um valor que repete uma expressão regular que pode identificar e remontar o evento multilinhas. Por exemplo, este evento contém um valor repetido:

```
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SEARCH RESULT tag=101
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH base="dc=iso-n,dc=com"
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH attr=gidNumber
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=1 SRCH base="dc=iso-n,dc=com"
```

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo syslog de multilinhas UDP:

Tabela 23. Parâmetros de protocolo syslog multilinhas UDP

Parâmetro	Descrição
Configuração do Protocolo	**UDP Multiline Syslog**
Padrão de ID de Mensagem	A expressão regular (regex) necessária para filtrar as mensagens de carga útil do evento. As mensagens de eventos multilinhas UDP devem conter um valor de identificação comum que seja repetido em cada linha da mensagem do evento.

Após a fonte de log ser salva, um certificado syslog-tls será criado para a fonte de log. O certificado deve ser copiado para qualquer dispositivo em sua rede que seja configurada para encaminhar syslog criptografado. Outros dispositivos de rede que possuem um arquivo de certificado syslog-tls e o número da porta de atendimento do TLS podem ser descobertos automaticamente como uma fonte de log syslog TLS.

Opções de configuração de protocolo syslog de multilinhas TCP

É possível configurar uma fonte de log que usa o protocolo syslog de multilinhas TCP. Para criar um evento único, este protocolo utiliza expressões regulares para identificar o padrão de início e de encerramento de eventos multilinhas.

O exemplo a seguir é um evento multilinhas:

```
06/13/2012 08:15:15 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5156
EventType=0
TaskCategory=Filtering Platform Connection
Keywords=Audit Success
Message=The Windows Filtering Platform permitted a connection.
Process ID: 4
Application Name: System
Direction: Inbound
Source Address: 1.1.1.1
Source Port: 80
Destination Address: 1.1.1.12
Destination Port:444
```

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo syslog de multilinhas TCP:

Tabela 24. Parâmetros do protocolo syslog multilinhas TCP

Parâmetro	Descrição
Configuração do Protocolo	**Syslog de Multilinhas TCP**
Porta de Atendimento	A porta de atendimento padrão é 12468.
Formatador de Eventos	Utilize a opção **Multilinhas do Windows** para eventos multilinhas que forem formatados especificamente para o Windows.
Padrão de Início do Evento	A expressão regular (regex) que é necessária para identificar o início de uma carga útil do evento multilinhas TCP. Os cabeçalhos syslog geralmente começam com uma data ou registro de data e hora. O protocolo pode criar um evento único que é baseado em apenas um padrão de início de evento, como um registro de data e hora. Quando apenas um padrão de início estiver disponível, o protocolo capturará todas as informações entre cada valor inicial para criar um evento válido.
Padrão de Término do Evento	A expressão regular (regex) que é necessária para identificar o último campo de uma carga útil do evento multilinhas TCP. Se o evento syslog terminar com o mesmo valor, será possível utilizar uma expressão regular para determinar o término de um evento. O protocolo pode capturar eventos que são baseados em apenas um padrão de término de evento. Quando somente um padrão de término estiver disponível, o protocolo capturará todas as informações entre o valor inicial e final para criar um evento válido.

Opções de configuração de protocolo VMware vCloud Director

Para coletar eventos a partir dos ambientes virtuais do VMware vCloud Director, é possível criar uma fonte de log que utiliza o protocolo do VMware vCloud Director.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo do VMware vCloud Director:

Tabela 25. Parâmetros do protocolo do VMware vCloud Director

Parâmetro	Descrição
Configuração do Protocolo	**VMware vCloud Director**
URL do vCloud	A URL que é configurada no dispositivo VMware vCloud para acessar a API REST. A URL deve corresponder ao endereço que é configurado como a URL de base da API REST pública VCD no vCloud Server, por exemplo, `https://1.1.1.1.`.
Nome do Usuário	O nome de usuário que é necessário para acessar remotamente o vCloud Server, por exemplo, `console/user@organization`. Para configurar uma conta somente leitura para uso com o protocolo vCloud Director, um usuário deve ter permissão Somente Acesso do Console.

As opções de configuração de protocolo IBM Tivoli Endpoint Manager SOAP

Para receber eventos formatados com Log Extended Event Format (LEEF) de dispositivos do IBM Tivoli Endpoint Manager, configure uma fonte de log que utiliza o protocolo IBM Tivoli Endpoint Manager SOAP.

Esse protocolo requer o IBM Tivoli Endpoint Manager nas versões V8.2.x ou posteriores e o aplicativo Web Reports for Tivoli Endpoint Manager.

O protocolo Tivoli Endpoint Manager SOAP recupera eventos em intervalos de 30 segundos sobre HTTP ou HTTPS. Conforme os eventos são recuperados, o IBM Tivoli Endpoint Manager DSM analisa e categoriza os eventos.

A tabela a seguir descreve os parâmetros específicos de protocolo para o protocolo IBM Tivoli Endpoint Manager SOAP:

Tabela 26. Parâmetros de protocolo do IBM Tivoli Endpoint Manager SOAP

Parâmetro	Descrição
Configuração do Protocolo	**IBM Tivoli Endpoint Manager SOAP**
Usar HTTPS	Se um certificado for necessário para se conectar com HTTPS, copie os certificados necessários para o seguinte diretório: `/opt/qradar/conf/trusted_certificates`. Certificados que possuem extensões dos arquivos a seguir: `.crt`, `.certou.der` são suportados. Copie os certificados no diretório de certificados confiáveis antes que a fonte de log seja salva e implementada.

Tabela 26. Parâmetros de protocolo do IBM Tivoli Endpoint Manager SOAP (continuação)

Parâmetro	Descrição
Porta SOAP	Por padrão, a porta 80 é o número de porta de comunicação com o IBM Tivoli Endpoint Manager. A maioria das configurações utiliza a porta 443 para comunicação HTTPS.

Visão geral do protocolo Syslog Redirect

O protocolo Syslog Redirect é usado como uma alternativa para o protocolo Syslog. Use esse protocolo quando desejar identificar com o QRadar o nome do dispositivo específico que enviou os eventos. O QRadar pode atender passivamente os eventos do Syslog na porta 517 do UDP.

A tabela a seguir descreve os parâmetros específicos do protocolo para o protocolo Syslog Redirect:

Tabela 27. Parâmetros do protocolo Syslog Redirect

Parâmetro	Descrição
Configuração do Protocolo	**Syslog Redirect**
Identificador de fonte de log RegEx	`devname=([\w-]+)`
Porta de Atendimento	`517`
Protocolo	**UDP**

Incluindo origens de log em massa

É possível incluir até 500 origens de logs do Microsoft Windows ou Universal DSM de uma vez. Ao incluir várias origens de log de uma vez, é incluída uma fonte de log em massa em QRadar. Origens de log em massa devem compartilhar uma configuração comum.

Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Origens de Log**.
3. Na lista **Ações em massa**, selecione **Inclusão em massa**.
4. Configure os parâmetros para a fonte de log em massa.
   - Upload de arquivo - Faça upload de um arquivo de texto que tenha um nome de host ou um IP por linha
   - Manual - Insira o nome do host ou o IP do host que deseja incluir
5. Clique em **Salvar**.
6. Clique em **Continuar** para incluir as origens de log.
7. Na guia **Administrador**, clique em **Implementar Mudanças**.

Incluindo uma ordem de análise de fonte de log

É possível designar uma ordem de prioridade para quando os eventos forem analisados pelo coletor de eventos de destino.

Sobre Esta Tarefa

É possível solicitar a importância das origens de log ao definir a ordem de análise para as origens de log que compartilham um endereço IP ou nome do host comum. Definir a ordem de análise para as origens de log assegura que determinadas origens de log sejam analisadas em uma ordem específica, independentemente das mudanças na configuração da fonte de log. A ordem da análise assegura que o desempenho do sistema não seja afetado pelas mudanças na configuração da fonte de log ao evitar análises desnecessárias. A ordem da análise assegura que as origens de eventos de baixo nível não sejam analisadas para eventos antes de fonte de log mais importantes.

Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Ordenação de Análise de Origem de Log**.
3. Selecione uma fonte de log.
4. Opcional: Na lista **Coletor de Eventos Selecionado**, selecione o Coletor de Eventos para definir a ordem de análise de fonte de log.
5. Opcional: Na lista **Host de Origem de Log**, selecione uma fonte de log.
6. Priorize a ordem de análise de fonte de log.
7. Clique em **Salvar**.

Capítulo 2. Extensões de origem de log

Um documento de extensão pode estender ou modificar a maneira como os elementos de uma determinada origem de log são analisados. É possível usar o documento de extensão para corrigir um problema de análise ou substituir a análise padrão de um evento a partir de um DSM existente.

Um documento de extensão também poderá fornecer suporte de evento quando um DSM não existir para analisar eventos de um dispositivo ou dispositivo de segurança em sua rede.

Um documento de extensão é um documento formatado de Linguagem de Marcação Extensível (XML) que pode ser criado ou editado usando qualquer editor comum de texto, código ou marcação. É possível criar vários documentos de extensão, mas uma origem de log pode ter apenas um aplicado a ela.

O formato XML requer que todos os padrões de expressão regular (regex) estejam contidos nas seções de dados de caractere (CDATA) para evitar que os caracteres especiais necessários para as expressões regulares interfiram no formato de marcação. Por exemplo, o código a seguir mostra o regex para localizar protocolos:

```
<pattern id="ProtocolPattern" case-insensitive="true" xmlns="">
<![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
```

`(TCP|UDP|ICMP|GRE)` é o padrão de expressão regular.

A configuração de extensão de origens de log consiste nas seções a seguir:

Padrão
Padrões de expressões regulares associados a um determinado nome de campo. Os padrões são referenciados várias vezes dentro do arquivo de extensão de origem de log.

Grupos de correspondência
Uma entidade dentro de um grupo de correspondência que é analisada, por exemplo, EventName, e é emparelhada com o padrão e o grupo apropriados para análise. Qualquer número de grupos de correspondência pode aparecer no documento de extensão.

Exemplos de extensões de origem de log no fórum do QRadar

É possível criar extensões de origem de log (LSX) para origens de log que não tenham um DSM suportado. Para ajudar a criar suas próprias extensões de origem de log (também conhecidas como extensões DSM), modifique extensões existentes que foram criadas.

É possível acessar exemplos de extensão de origem de log (https://www.ibm.com/developerworks/community/forums/html/topic?id=d15cac8d-b0fa-4461-bb1e-dc1b291de440&ps=25) no fórum de Discussion about DSM Extensions, Custom Properties and other REGEX related topics (https://www.ibm.com/developerworks/community/forums/html/forum?id=11111111-0000-0000-0000-000000003046&ps=25).

Os fóruns do IBM Security QRadar é um site de discussão on-line em que os usuários e especialistas no assunto colaboram e compartilham informações.

Conceitos relacionados:

"Criando um documento de extensões de origem de log" na página 36
Crie extensões de origem de log (LSX) para origens de log que não tenham um DSM suportado ou para reparar um evento que tenha informações ausentes ou incorretas, ou para analisar um evento quando o DSM associado falhar ao produzir um resultado.

Padrões nos documentos de extensão de origem de log

Em vez de associar uma expressão regular diretamente a um determinado nome de campo, padrões (`patterns`) são declarados separadamente no início do documento de extensão. Esses padrões de regex podem ser então referenciados várias vezes dentro do arquivo de extensão de origem de log.

Todos os caracteres entre a tag de início <pattern> e a tag de término </pattern> são considerados parte do padrão. Não use espaços extras ou retornos forçados dentro ou ao redor de seu padrão, ou a expressão <CDATA>. Caracteres ou espaços extras podem evitar que a extensão DSM corresponda ao padrão desejado.

Tabela 28. Descrição de parâmetros padrão

Padrão	Tipo	Descrição
`id` (Necessário)	Sequência	Uma sequência regular que é exclusiva dentro do documento de extensão.
`case-insensitive` (Opcional)	Booleano	Se true, as maiúsculas e minúsculas do caractere serão ignoradas. Por exemplo, `abc` é o mesmo que `ABC`. Se não especificado, esse parâmetro será padronizado como false.
`trim-whitespace` (Opcional)	Booleano	Se true, espaço em branco e retorno de linha serão ignorados. Se as seções CDATA forem divididas em linhas diferentes, os espaços extras e os retornos de linha não serão interpretados como parte do padrão. Se não especificado, esse parâmetro será padronizado como false.

Grupos de correspondência

Um *grupo de correspondência* (`match-group`) é um conjunto de padrões usados para analisar ou modificar um ou mais tipos de eventos.

Um *correspondente* é uma entidade dentro de um grupo de correspondência que é analisada, por exemplo, EventName, e é emparelhada com o padrão e o grupo apropriados para análise. Qualquer número de grupos de correspondência pode aparecer no documento de extensão.

Tabela 29. Descrição de parâmetros de grupos de correspondência

Parâmetro	Descrição
`order` (Necessário)	Um número inteiro maior que zero que define a ordem em que os grupos de correspondência são executados. Ele deve ser exclusivo dentro do documento de extensão.
`description` (Opcional)	Uma descrição para o grupo de correspondência, que pode ser qualquer sequência. Essas informações podem aparecer nos logs. Se não especificado, esse parâmetro será padronizado como empty.
`device-type-id-override` (Opcional)	Defina um ID de dispositivo diferente para substituir o QID. Permite que o grupo de correspondência específico procure no dispositivo especificado o tipo de evento. Deve ser um ID de tipo de origem de log válido, representado como um número inteiro. Uma lista de IDs de tipo de origem de log é apresentada na Tabela 36 na página 48. Se não especificado, esse parâmetro será padronizado com o tipo de origem de log da origem de log à qual a extensão está anexada.

Os grupos de correspondência podem ter estas entidades:

- "Correspondente (matcher)"
- "Modificador de único evento (`event-match-single`)" na página 32
- "Modificador de múltiplos eventos (`event-match-multiple`)" na página 32

Correspondente (matcher)

Uma entidade correspondente é um campo que é analisado, por exemplo, EventName, e é emparelhado com o padrão e o grupo apropriados para análise.

Os correspondentes possuem uma ordem associada. Se vários correspondentes forem especificados para o mesmo nome de campo, eles serão executados na ordem apresentada até que uma análise bem-sucedida seja localizada ou que ocorra uma falha.

Tabela 30. Descrição de parâmetros correspondentes

Parâmetro	Descrição
`field` (Necessário)	O campo ao qual você deseja que o padrão seja aplicado, por exemplo, EventName ou SourceIp. É possível usar qualquer um dos nomes de campo listados na tabela Lista de nomes de campo correspondentes válidos.

Tabela 30. Descrição de parâmetros correspondentes (continuação)

Parâmetro	Descrição
`pattern-id` (Necessário)	O padrão que você deseja usar quando o campo é analisado a partir da carga útil. Esse valor deve corresponder (incluindo maiúsculas e minúsculas) ao parâmetro ID do padrão definido anteriormente em um parâmetro ID do padrão (Tabela 28 na página 26).
`order` (Necessário)	A ordem que você deseja que esse padrão tente entre os correspondentes designados ao mesmo campo. Se dois correspondentes forem designados ao campo EventName, aquele com a menor ordem será tentado primeiro.
`capture-group` (Opcional)	Referenciado na expressão regular entre parêntese ( ). Essas capturas são indexadas a partir de um e processadas da esquerda para a direita no padrão. O campo `capture-group` deve ser um número inteiro positivo menor ou igual ao número de grupos de captura contidos no padrão. O valor padrão é zero, que é a correspondência inteira. Por exemplo, é possível definir um único padrão para um endereço IP e uma porta de origem, em que o correspondente SourceIp pode usar um grupo de captura 1, e o correspondente SourcePort pode usar um grupo de captura 2, mas somente um padrão precisa ser definido. Esse campo possui um propósito dual quando combinado com o parâmetro `enable-substitutions`. Para ver um exemplo, revise o exemplo de documento de extensão.

Tabela 30. Descrição de parâmetros correspondentes (continuação)

Parâmetro	Descrição

`enable-substitutions` (Opcional)	Booleano
	
	Quando configurado como `true`, um campo não pode ser adequadamente representado com uma captura de grupo linear. É possível combinar vários grupos com texto extra para formar um valor.
	
	Esse parâmetro muda o significado do parâmetro `capture-group`. O parâmetro `capture-group` cria o novo valor, e as substituições de grupo são especificadas usando `\x`, em que `x` é um número de grupo, de 1 a 9. É possível usar os grupos várias vezes, e qualquer texto de formato livre também pode ser inserido no valor. Por exemplo, para formar um valor fora do grupo 1, seguido de um sublinhado, seguido do grupo 2, de um @ e, em seguida, do grupo 1 novamente, a sintaxe apropriada de capture-group é mostrada no código a seguir:
	
	`capture-group="\1_\2@\1"`
	
	Em outro exemplo, um endereço MAC é separado por dois pontos (:), mas no QRadar, os endereços de MAC são geralmente separados por hífen. A sintaxe para analisar e capturar as partes individuais é mostrada no exemplo a seguir:
	
	`capture-group="\1:\2:\3:\4:\5:\6"`
	
	Se não houver nenhum grupo especificado no grupo de captura quando as substituições forem ativadas, ocorrerá uma substituição de texto direta.
	
	O padrão é false.

`ext-data` (Opcional)	Um parâmetro extra-data que define qualquer informação ou formatação de campo extra que um campo correspondente pode fornecer na extensão. O único campo que usa esse parâmetro é DeviceTime. Por exemplo, é possível que você tenha um dispositivo que envie eventos usando um único registro de data e hora, mas você deseja que o evento seja reformatado para um horário de dispositivo padrão. Use o parâmetro ext-data incluído com o campo DeviceTime para reformatar o registro de data e hora do evento. Para obter mais informações, consulte a Lista de nomes de campo correspondentes válidos.

A tabela a seguir lista os nomes de campo correspondentes válidos.

Tabela 31. Lista de nomes de campo correspondentes válidos

Nome do campo	Descrição
EventName (Necessário)	O nome do evento a ser recuperado do QID para identificar o evento. **Nota:** Esse parâmetro não aparece como um campo na guia **Atividade do log**.
EventCategory	Uma categoria de evento para qualquer evento com uma categoria não manipulada por uma entidade de única correspondência de evento ou uma entidade de múltipla correspondência de evento. Combinada com EventName, EventCategory é usada para procurar o evento no QID. Os campos usados para consultas QIDmap requerem que uma sinalização de substituição seja configurada quando os dispositivos já forem conhecidos do QRadar, por exemplo, `<event-match-single event-name= "Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity= "OverrideAndNeverSend" />` O `force-qidmap-lookup-on-fixup="true"` é a substituição da sinalização. **Nota:** Esse parâmetro não aparece como um campo na guia **Atividade do log**.
SourceIp	O endereço IP de origem da mensagem.
SourcePort	A porta de origem da mensagem.
SourceIpPreNAT	O endereço IP de origem da mensagem antes que a Conversão de Endereço de Rede (NAT) ocorra.
SourceIpPostNAT	O endereço IP de origem da mensagem depois que NAT ocorre.
SourceMAC	O endereço MAC de origem da mensagem.
SourcePortPreNAT	A porta de origem da mensagem antes que NAT ocorra.
SourcePortPostNAT	A porta de origem da mensagem depois que NAT ocorre.
DestinationIp	O endereço IP de destino da mensagem.
DestinationPort	A porta de destino da mensagem.
DestinationIpPreNAT	O endereço IP de destino da mensagem antes que NAT ocorra.
DestinationIpPostNAT	O endereço IP de destino da mensagem depois que NAT ocorre.
DestinationPortPreNAT	A porta de destino da mensagem antes que NAT ocorra.
DestinationPortPostNAT	A porta de destino da mensagem depois que NAT ocorre.

Tabela 31. Lista de nomes de campo correspondentes válidos (continuação)

Nome do campo	Descrição
DestinationMAC	O endereço MAC de destino da mensagem.
DeviceTime	O horário e o formato usados pelo dispositivo. Esse registro de data e hora representa o horário de envio do evento, de acordo com o dispositivo. Esse parâmetro não representa o horário de chegada do evento. O campo `DeviceTime` suporta a capacidade de usar um registro de data e hora customizado para o evento usando o atributo correspondente ext-data. A lista a seguir contém exemplos de formatos de registro de data e hora que podem ser usados no campo `DeviceTime`: • ext-data="dd/MMM/YYYY:hh:mm:ss" 11/Mar/2015:05:26:00 • ext-data="MMM dd YYYY / hh:mm:ss" Mar 11 2015 / 05:26:00 • ext-data="hh:mm:ss:dd/MMM/YYYY" 05:26:00:11/Mar/2015 Para obter mais informações sobre os possíveis valores para o formato do registro de data e hora, consulte a página da web Joda-Time (http://www.joda.org/joda-time/key_format.html). DeviceTime é o único campo de evento que usa o parâmetro opcional ext-data.
Protocolo	O protocolo que está associado ao evento, por exemplo, TCP, UDP ou ICMP.
UserName	O nome do usuário que está associado ao evento.
HostName	O nome do host que está associado ao evento. Geralmente, esse campo é associado a eventos de identidade.
GroupName	O nome do grupo que está associado ao evento. Geralmente, esse campo é associado a eventos de identidade.
NetBIOSName	O nome do NetBIOS que está associado ao evento. Geralmente, esse campo é associado a eventos de identidade.
ExtraIdentityData	Quaisquer dados específicos do usuário que estão associados ao evento. Geralmente, esse campo é associado a eventos de identidade.
SourceIpv6	O endereço IP de origem IPv6 da mensagem.
DestinationIpv6	O endereço IP de destino IPv6 da mensagem.

Modificador de múltiplos eventos (event-match-multiple)

O modificador de múltiplos eventos (event-match-multiple) corresponde a um intervalo de tipos de eventos e, em seguida, os modifica, conforme especificado pelo parâmetro pattern-id e o parâmetro capture-group-index.

Essa correspondência não é feita na carga útil, mas nos resultados do EventName correspondente analisado anteriormente fora da carga útil.

Essa entidade permite a mutação de eventos bem-sucedidos mudando a categoria de evento do dispositivo, a severidade ou o método usado pelo evento para enviar eventos de identidade. O capture-group-index deve ser um valor de número inteiro (substituições não são suportadas) e pattern-ID deve referenciar uma entidade de padrão existente. Todas as outras propriedades são idênticas a suas contrapartes no modificador de único evento.

Modificador de único evento (event-match-single)

O modificador de único evento (event-match-single) corresponde e, em seguida, modifica exatamente um tipo de evento, conforme especificado pelo parâmetro necessário EventName, que faz distinção entre maiúsculas e minúsculas.

Essa entidade permite a mutação de eventos bem-sucedidos mudando a categoria de evento do dispositivo, a severidade ou o método para enviar eventos de identidade.

Quando os eventos que correspondem a esse nome de evento são analisados, a categoria do dispositivo, a severidade e as propriedades de identidade são impostas sobre o evento resultante.

Deve-se configurar um atributo event-name e esse valor de atributo corresponde ao valor do campo **EventName**. Além disso, uma entidade event-match-single consiste nestas propriedades opcionais:

Tabela 32. Descrição de parâmetros de único evento

Parâmetro	Descrição
device-event-category	Uma nova categoria para procurar um QID para o evento. Esse é um parâmetro de otimização porque alguns dispositivos possuem a mesma categoria para todos os eventos.
severity	A severidade do evento. Esse parâmetro deve ser um valor de número inteiro entre 1 e 10. Se uma severidade menor que 1 ou maior que 10 for especificada, o sistema será padronizado com 5. Se não especificada, o padrão será o que for localizado no QID.

Tabela 32. Descrição de parâmetros de único evento (continuação)

Parâmetro	Descrição
`send-identity`	Especifica o envio de informações de mudança de identidade do evento. Escolha uma das opções a seguir: • `UseDSMResults` Se o DSM retornar um evento de identidade, o evento será transmitido. Se o DSM não retornar um evento de identidade, a extensão não criará ou modificará as informações de identificação. Essa opção será o valor padrão se nenhum valor for especificado. • `SendIfAbsent` Se o DSM criar informações de identificação, o evento de identidade será passado por meio de não afetado. Se nenhum evento de identidade for produzido pelo DSM, mas houver informações suficientes no evento para criar um evento de identidade, um evento será gerado com todos os campos relevantes configurados. • `OverrideAndAlwaysSend` Ignora o evento de identidade retornado pelo DSM e criará um novo evento de identidade, se houver informações suficientes. • `OverrideAndNeverSend` Suprime as informações de identificação retornadas pelo DSM. Opção sugerida, a menos que você esteja processando eventos que deseje que passem para atualizações de ativo.

Modelo de documento de extensão

O exemplo de um documento de extensão fornece informações sobre como analisar um determinado tipo de Cisco FWSM para que os eventos não sejam enviados com um nome de evento incorreto.

Por exemplo, para resolver a palavra `session`, que está integrada no meio do nome do evento:

```
Nov 17 09:28:26 129.15.126.6 %FWSM-session-0-302015:
Built UDP connection for faddr 38.116.157.195/80
gaddr 129.15.127.254/31696 laddr 10.194.2.196/2157
duration 0:00:00 bytes 57498 (TCP FINs)
```

Essa condição faz com que o DSM não reconheça nenhum evento e todos os eventos ficam sem análise e são associados ao criador de logs genérico.

Embora uma parte da sequência de texto (`302015`) seja usada para a procura QID, a sequência de texto inteira (`%FWSM-session-0-302015`) identifica o evento como vindo de um Cisco FWSM. Como a sequência de texto inteira não é válida, o DSM assume que o evento não é válido.

Exemplo de documento de extensão para analisar um tipo de evento

Um dispositivo FWSM possui vários tipos de eventos e vários com formatos exclusivos. O exemplo de documento de extensão a seguir indica como analisar um tipo de evento.

Nota: Os IDs padrão não precisam corresponder aos nomes de campos que estão analisando. Embora o exemplo a seguir duplique o padrão, o campo `SourceIp` e o campo `SourceIpPreNAT` podem usar o mesmo exato padrão nesse caso. Esta situação pode não ser verdadeira em todos os eventos FWSM.

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(tcp|udp|icmp|gre)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
      <matcher field="EventName" order="1" pattern-id="EventNameFWSM_Pattern" capture-group="1"/>
      <matcher field="SourceIp" order="1" pattern-id="SourceIp_Pattern" capture-group="1" />
      <matcher field="SourcePort" order="1" pattern-id="SourcePort_Pattern" capture-group="2"/>
      <matcher field="SourceIpPreNAT" order="1" pattern-id="SourceIpPreNAT_Pattern" capture-group="1" />
      <matcher field="SourceIpPostNAT" order="1" pattern-id="SourceIpPostNAT_Pattern" capture-group="1" />
      <matcher field="SourcePortPreNAT" order="1" pattern-id="SourcePortPreNAT_Pattern" capture-group="2" />
      <matcher field="SourcePortPostNAT" order="1" pattern-id="SourcePortPostNAT_Pattern" capture-group="2" />
      <matcher field="DestinationIp" order="1" pattern-id="DestinationIp_Pattern" capture-group="1" />
      <matcher field="DestinationPort" order="1" pattern-id="DestinationIp_Pattern" capture-group="2" />
      <matcher field="Protocol" order="1" pattern-id="Protocol_Pattern" capture-group="1" />
      <matcher field="Protocol" order="2" pattern-id="Protocol_6_Pattern" capture-group="TCP" enable-substitutions=true/>
      <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
   </match-group>
</device-extension>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<!-- Do not remove the "allEventNames" value -->
<pattern id="EventName-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceIp-Fakeware_Pattern" xmlns=""><![CDATA[]]</pattern>
<pattern id="SourcePort-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceMAC-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationIp-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationPort-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<pattern id="Protocol-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceIp" order="1" pattern-id="SourceIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="SourcePort" order="1" pattern-id="SourcePort-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceMAC" order="1" pattern-id="SourceMAC-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationIp" order="1" pattern-id="DestinationIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationPort" order="1" pattern-id="SDestinationPort-Fakeware_Pattern" capture-group="1" />
   <matcher field="Protocol" order="1" pattern-id="Protocol-Fakeware_Pattern" capture-group="1" />
   <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
</match-group>
</device-extension>
```

Conceitos básicos da análise

O exemplo de documento de extensão anterior demonstra alguns dos aspectos básicos de análise:

- Endereços IP
- Portas
- Protocolo
- Vários campos que usam o mesmo padrão com grupos diferentes

Esse exemplo analisa todos os eventos FWSM que seguem o padrão especificado. Os campos que forem analisados poderão não estar presentes nesses eventos quando os eventos incluírem conteúdo diferente.

As informações que eram necessárias para criar essa configuração que não estavam disponíveis no evento:

- O nome do evento é somente os 6 últimos dígitos (`302015`) da parte `%FWSM-session-0-302015` do evento.

- O FWSM possui uma categoria de evento de dispositivo codificado permanentemente de `Cisco Firewall`.
- O DSM do FWSM usa o Cisco Pix QIDmap e, portanto, inclui o parâmetro `device-type-id-override="6"` no grupo correspondente. O ID do tipo de origem de log do Pix firewall é 6. Para obter mais informações, consulte "IDs dos tipos de origem de log" na página 48).

Nota: Se as informações de QID não forem especificadas ou estiverem indisponíveis, é possível modificar o mapeamento de eventos. Para obter mais informações, consulte a seção Modificando o mapeamento de eventos no *IBM Security QRadar SIEM Users Guide*.

Nome do evento e categoria de evento do dispositivo

Um nome de evento e uma categoria de evento de dispositivo são necessários quando o QIDmap é procurado. Essa categoria de evento de dispositivo é um parâmetro de agrupamento no banco de dados que ajuda a definir eventos equivalentes em um dispositivo. O `event-match-multiple` no término do grupo correspondente inclui codificação permanente da categoria. O `event-match-multiple` usa o padrão EventNameId no nome de evento analisado para corresponder a até 6 dígitos. Esse padrão não é executado na carga útil completa, somente nessa parte analisada como o campo EventName.

O padrão EventName referencia a parte `%FWSM` dos eventos; todos os eventos Cisco FWSM contêm a parte `%FWSM`. O padrão no exemplo corresponde a `%FWSM` seguido de qualquer número (zero ou mais) de letras e traços. Essa correspondência de padrões resolve a palavra `session` que está integrada no meio do nome do evento que precisa ser removido. A severidade do evento (de acordo com Cisco) seguida de um traço e, em seguida, o nome verdadeiro do evento, conforme esperado pelo QRadar. A sequência `(\d{6})` é a única sequência no padrão EventNameFWSM que tem um grupo de captura.

Os endereços IP e as portas do evento seguem o mesmo padrão básico: um endereço IP seguido de dois pontos (:), seguido do número da porta. Esse padrão analisa duas partes de dados (o endereço IP e a porta) e especifica grupos de captura diferentes na seção correspondente.

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\] </pattern>
<pattern id="Username">(TLSv1)</pattern>
<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1"
       capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username" capture-group="1"/>
</match-group>
</device-extension>
```

Padrões de endereço IP e de porta

Os padrões de endereço IP e de porta são quatro conjuntos de um a três dígitos, separados por pontos, seguidos de dois pontos (:) e do número da porta. A seção de endereço IP está em um grupo, assim como o número da porta, mas os dois pontos (:), não. As seções correspondentes para esses campos referenciam o mesmo nome padrão, mas um grupo de captura diferente (o endereço IP é grupo 1 e a porta é grupo 2).

O protocolo é um padrão comum que procura a carga útil para a primeira instância de TCP, UDP, ICMP ou GRE. O padrão é marcado com o parâmetro sem distinção entre maiúsculas e minúsculas para que qualquer ocorrência corresponda.

Embora um segundo padrão de protocolo não ocorra no evento usado no exemplo, há um segundo padrão de protocolo definido com uma ordem de dois. Se o padrão de protocolo com a menor ordem não corresponder, o próximo será tentado, e assim por diante. O segundo padrão de protocolo também demonstra substituição direta; não há grupos de correspondência no padrão, mas com o parâmetro enable-substitutions ativado, o próximo TCP poderá ser usado no lugar de protocol=6.

Criando um documento de extensões de origem de log

Crie extensões de origem de log (LSX) para origens de log que não tenham um DSM suportado ou para reparar um evento que tenha informações ausentes ou incorretas, ou para analisar um evento quando o DSM associado falhar ao produzir um resultado.

Para origens de log que não tenham um DSM oficial, use um DSM Universal, ou UDSM, para integrar origens de log. Uma extensão de origem de log (também conhecida como uma extensão de dispositivo) é então aplicada ao UDSM para fornecer a lógica para análise dos logs. O LSX baseia-se em expressões regulares Java e pode ser usado em qualquer protocolo de log, como syslog, JDBC e LFPS. Valores podem ser extraídos dos logs e mapeados para todos os campos comuns no QRadar.

Ao usar extensões de origem de log para reparar conteúdo ausente ou incorreto, quaisquer novos eventos que forem produzidos pelas extensões de origem de log serão associados à origem de log que falhou ao analisar a carga útil original. A criação de uma extensão evita que eventos desconhecidos ou não categorizados sejam armazenados como desconhecidos no IBM Security QRadar.

Siga estas etapas para criar uma extensão de origem de log:

1. Assegure-se de que uma origem de log seja criada no QRadar.

   Use o DSM Universal como o tipo de origem de log para manipular itens que não estejam na lista. Também é possível criar manualmente uma origem de log para evitar que os logs sejam classificados automaticamente.
2. Para determinar os campos disponíveis, use a guia **Atividade do log** para exportar os logs para avaliação.
3. Use o modelo de exemplo de documento de extensão para determinar os campos que podem ser usados. (“Modelo de documento de extensão” na página 33).

   Não é necessário usar todos os campos no modelo. Determine os valores na origem de log que podem ser mapeados para os campos no modelo de documento de extensão. Para obter mais informações, consulte “Modelo de documento de extensão” na página 33.
4. Remova os campos não usados e seus IDs de padrão correspondentes do documento de extensão de origem de log.
5. Faça upload do documento de extensão e aplique a extensão à origem do log.
6. Mapeie os eventos para seus equivalentes no QIDmap.

   Esta ação manual na guia **Atividade do log** é usada para mapear eventos de origem de log desconhecidos para eventos conhecidos do QRadar para que possam ser categorizados e processados.

Conceitos relacionados:

"Exemplos de extensões de origem de log no fórum do QRadar" na página 25
É possível criar extensões de origem de log (LSX) para origens de log que não tenham um DSM suportado. Para ajudar a criar suas próprias extensões de origem de log (também conhecidas como extensões DSM), modifique extensões existentes que foram criadas.

Construindo um DSM Universal

A primeira etapa na construção de um DSM Universal é criar a origem de log no IBM Security QRadar. Quando você cria a origem de log, ela evita que os logs sejam classificados automaticamente e é possível exportar os logs para revisão.

Procedimento

1. Na guia **Administrador**, crie uma nova origem clicando no ícone **Origens de log**.
2. Clique em **Incluir**.
3. Especifique o nome no campo **Nome da origem de log**.
4. Na lista **Tipo de origem de log**, selecione **DSM Universal**.

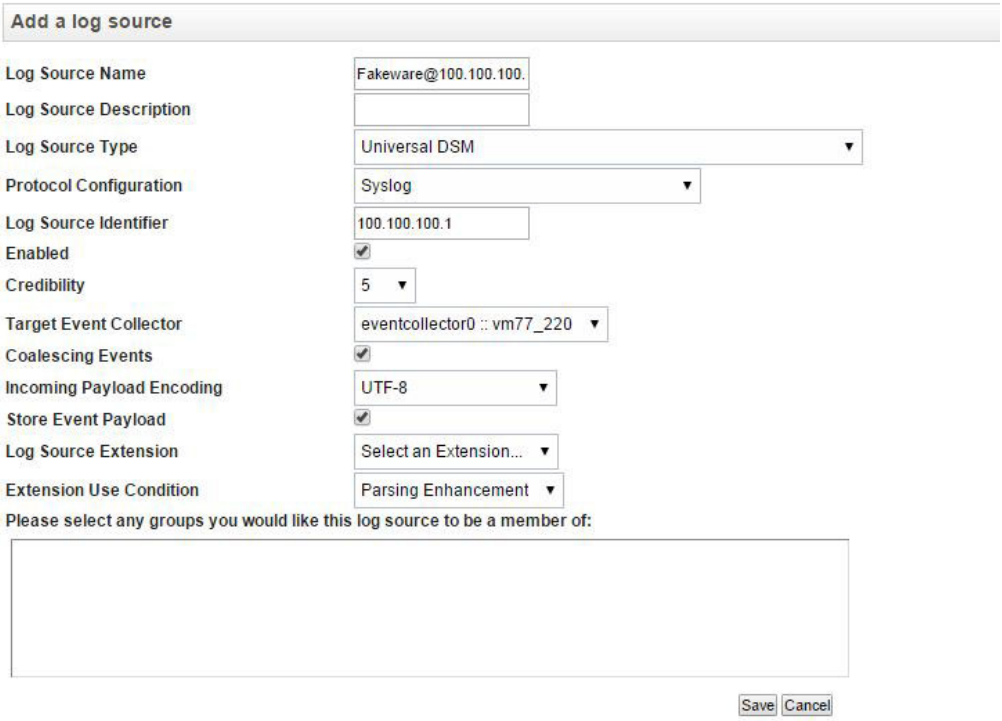

Figura 1. Incluir uma origem de log

É possível que você não veja a **Extensão de origem de log** ou a **Condição de uso da extensão**, a menos que já tenha aplicado uma extensão de origem de log ao QRadar Console

5. Na lista **Configuração do protocolo**, especifique o protocolo que deseja usar.

   Esse método é usado pelo QRadar para obter os logs da origem de log não suportada.
6. Para o **Identificador de origem de log**, insira o endereço IP ou o nome do host da origem de log não suportada.

7. Clique em **Salvar** para salvar a nova origem de log e fechar a janela.
8. Na **guia Administradores**, clique em **Implementar mudanças**.

O que Fazer Depois

"Exportando os logs"

Exportando os logs

Exporte os logs criados depois de construir um DSM Universal

Sobre Esta Tarefa

Geralmente, deseja-se um número significativo de logs para revisão. Dependendo da taxa de EPS da origem de log não suportada, pode demorar várias horas para obter uma amostra de log abrangente.

Quando o QRadar não pode detectar o tipo de origem de log, os eventos são coletados, mas não são analisados. É possível filtrar esses eventos não analisados e, em seguida, revisar a última notificação de sistema recebida. Depois de revisar a notificação do sistema, é possível criar uma procura que se baseie nesse prazo.

Procedimento

1. Para examinar apenas os eventos não analisados, filtre os logs.
   a. Clique na guia **Atividade do log**.
   b. Clique em **Incluir filtro**.
   c. Selecione **O evento não está analisado**.

      Dica: Digite dentro da caixa de texto **Parâmetro** para ver o item **O evento não está analisado**.
   d. Selecione um prazo.
   e. Se você vir eventos de **Informações** nas notificações do sistema, clique com o botão direito para filtrá-los.
   f. Revise a coluna **IP de origem** para determinar qual dispositivo está enviando os eventos.

      É possível visualizar as cargas úteis do evento bruto. Geralmente, os fabricantes colocam nomes de produtos identificáveis nos cabeçalhos, portanto, é possível configurar sua procura como **Exibir: Eventos brutos** para mostrar as cargas úteis sem ter que abrir cada evento manualmente. Classificar pela rede também pode ajudar a localizar um dispositivo específico do qual o evento se originou.
2. Crie uma procura para exportar os logs.
   a. Na guia **Atividade do log**, selecione **Procurar** > **Editar procura**.
   b. Para o **Intervalo de tempo**, especifique o tempo suficiente, por exemplo, 6 horas, de quando a origem de log foi criada.
   c. Em **Parâmetros de procura**, na lista **Parâmetro**, selecione **Origem de log (indexada)**, na lista **Operador**, selecione **Equivale a** e na lista **Grupo de origem de log**, selecione **Outro**, especifique a origem de log que foi criada quando o DSM Universal foi construído.

Nota: Dependendo de suas configurações, é possível ver **Origem de log** na lista **Parâmetro**, em vez de **Origem de log (indexada)**.

d. Clique em **Procurar** para visualizar os resultados.

3. Revise os resultados no console para verificar a carga útil.
4. Opcionalmente, é possível exportar os resultados clicando em **Ações** > **Exportar para XML** > **Exportação completa (todas as colunas)**.

   Não selecione **Exportar para CSV** porque a carga útil pode ser dividida entre várias colunas, ficando, assim, difícil de localizar a carga útil. XML é o formato preferencial para revisões de eventos.

   a. Você é solicitado a fazer download de um arquivo compactado. Abra o arquivo compactado e, em seguida, abra o arquivo resultante.
   b. Revise os logs.

      As cargas úteis do evento ficam entre as tags a seguir:

      ```
      <payloadAsUTF>
      ...
      </payloadAsUTF>
      ```

      O código a seguir mostra um exemplo de carga útil:

      ```
      <payloadAsUTF>ecs-ep (pid 4162 4163 4164) is running... </payloadAsUTF>
      ```

      Uma etapa crítica na criação de um DSM Universal é revisar os logs quanto à usabilidade. No mínimo, os logs devem ter um valor que possa ser mapeado para um nome de evento. O nome do evento deve ser um valor exclusivo que possa distinguir os vários tipos de log.

      O código a seguir mostra um exemplo de logs utilizáveis:

      ```
      May 20 17:16:14 dropbear[22331]: bad password attempt for 'root'
      from 192.168.50.80:3364
      May 20 17:16:26 dropbear[22331]: password auth succeeded for
      'root' from 192.168.50.80:3364
      May 20 16:42:19 kernel: DROP IN=vlan2 OUT=
      MAC=00:01:5c:31:39:c2:08:00 SRC=172.29.255.121
      DST=255.255.255.255 PROTO=UDP SPT=67 DPT=68
      ```

      Os códigos de exemplo a seguir mostram os logs um pouco menos utilizáveis:

      ```
      Oct 26 08:12:08 loopback 1256559128 autotrace[215824]: W: trace:
      no map for prod 49420003, idf 010029a2, lal 00af0008
      Oct 26 16:35:00 sxpgbd0081 last message repeated 7 times
      Nov 24 01:30:00 sxpgbd0081 /usr/local/monitor-rrd/sxpgbd0081/.rrd
      (rc=-1, opening '/usr/local/monitor-rrd/sxpgbd0081/.rrd':
      No such file or directory)
      ```

Expressões regulares comuns

Use expressões regulares para corresponder padrões de texto no arquivo de origem de log. É possível varrer mensagens em busca de padrões de letras, números ou uma combinação de ambos. Por exemplo, é possível criar expressões regulares que correspondam a endereços IP de origem e de destino, portas, endereços de MAC e muito mais.

Os códigos a seguir mostram várias expressões regulares comuns:

```
\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3} \d{1,5}
(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2} (TCP|UDP|ICMP|GRE)
\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
\s \t .*?
```

O caractere de escape, ou "\", é usado para denotar um caractere literal. Por exemplo, o caractere "." significa "qualquer caractere único" e corresponde a A, B, 1, X, etc. Para corresponder os caracteres ".", uma correspondência literal, deve-se usar "\."

Tabela 33. Expressões regex comuns

Tipo	Expressão
Tipo	\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
Endereço IP	\d{1,5}
Número da porta	(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}
Protocolo	(TCP|UDP|ICMP|GRE)
Horário do dispositivo	\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
Espaço em branco	\s
Tab	\t
Corresponder a qualquer coisa	.*?

Dica: Para assegurar-se de que não corresponda acidentalmente outros caracteres, escape qualquer caractere que não for dígito ou alfanumérico.

Construindo padrões de expressão regular

Para criar um DSM Universal, use expressões regulares (regex) para corresponder sequências de texto da origem de log não suportada.

Sobre Esta Tarefa

O exemplo a seguir mostra uma entrada de log referenciada nas etapas.

```
May 20 17:24:59 kernel: DROP MAC=5c:31:39:c2:08:00
SRC=172.29.255.121 DST=10.43.2.10 LEN=351 TOS=0x00 PREC=0x00 TTL=64 ID=9582
PROTO=UDP SPT=67 DPT=68 LEN=331
May 20 17:24:59 kernel: PASS MAC=5c:14:ab:c4:12:59
SRC=192.168.50.10 DST=192.168.10.25 LEN=351 TOS=0x00 PREC=0x00 TTL=64
ID=9583 PROTO=TCP SPT=1057 DPT=80 LEN=331
May 20 17:24:59 kernel: REJECT
MAC=5c:ad:3c:54:11:07 SRC=10.10.10.5 DST=192.168.100.25 LEN=351
TOS=0x00 PREC=0x00 TTL=64 ID=9584 PROTO=TCP SPT=25212 DPT=6881 LEN=331
```

Procedimento

1. Analise visualmente a origem de log não suportada para identificar padrões exclusivos.

   Esses padrões serão, mais tarde, convertidos em expressões regulares.
2. Localize as sequências de texto a serem correspondidas.

   Dica: Para fornecer verificação básica de erro, inclua caracteres antes e depois dos valores para evitar que valores semelhantes sejam correspondidos sem querer. Posteriormente, é possível isolar o valor real dos caracteres extras.
3. Desenvolva pseudocódigo para padrões de correspondência e inclua o caractere de espaço para denotar o início e o término de um padrão.

É possível ignorar as aspas. No exemplo de entrada de log, os nomes dos eventos são DROP, PASS e REJECT. A lista a seguir mostra os campos de evento utilizáveis.

- EventName: " kernel: VALUE "
- SourceMAC: " MAC=VALUE "
- SourceIp: " SRC=VALUE "
- DestinationIp: " DST=VALUE "
- Protocol: " PROTO=VALUE "
- SourcePort: " SPT=VALUE "
- DestinationPort: " DPT=VALUE "

4. Substitua um espaço pela expressão regular `\s`.

   Deve-se usar um caractere de escape para caracteres que não forem dígitos ou alfanuméricos. Por exemplo, = torna-se \= e : torna-se \:.

5. Converta o pseudocódigo em uma expressão regular.

Tabela 34. Convertendo pseudocódigo em expressões regulares

Campo	Pseudocódigo	Expressão regular
EventName	" kernel: VALUE "	\skernel\:\s.*?\s
SourceMAC	" MAC=VALUE "	\sMAC\=(?:[0-9a-fA-F]{2}\ :){5}[0-9a-fA-F]{2}\s
SourceIP	" SRC=VALUE "	\sSRC\=\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3}\s
DestinationIp	" DST=VALUE "	\sDST\=\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3}\s
Protocolo	" PROTO=VALUE "	\sPROTO\ =(TCP|UDP|ICMP|GRE)\s
SourcePort	" SPT=VALUE "	\sSPT\=\d{1,5}\s
DestinationPort	" DPT=VALUE "	\sDPT\=\d{1,5}\s

6. Especifique grupos de captura.

   Um grupo de captura isola um determinado valor na expressão regular.

   Por exemplo, no padrão SourcePort no exemplo anterior, não é possível passar o valor inteiro, uma vez que ele inclui espaços e `SRC=<code>`. Em vez disso, especifique somente o número da porta usando um grupo de captura. O valor no grupo de captura é o que é passado para o campo relevante no IBM Security QRadar.

   Insira parêntese ao redor dos valores que deseja capturar:

Tabela 35. Mapeando expressões regulares para capturar grupos para campos de evento

Campo	Expressão regular	Grupo de captura
EventName	\skernel\:\s.*?\s	\skernel\:\s(.*?)\s
SourceMAC	\sMAC\=(?:[0-9a-fA- F]{2}\:){5}[0-9a-fA-F]{2}\s	\sMAC\=((?:[0-9a-fA- F]{2}\:){5}[0-9a-fA-F]{2})\s
SourceIP	\sSRC\=\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3}\s	\sSRC\=(\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3})\s
Destination IP	\sDST\=\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3}\s	\sDST\=(\d{1,3}\.\d{1,3}\.\ d{1,3}\.\d{1,3})\s
Protocolo	\sPROTO\ =(TCP|UDP|ICMP|GRE)\s	\sPROTO\ =((TCP|UDP|ICMP|GRE))\s
SourcePort	\sSPT\=\d{1,5}\s	\sSPT\=(\d{1,5})\s

Tabela 35. Mapeando expressões regulares para capturar grupos para campos de evento (continuação)

Campo	Expressão regular	Grupo de captura
DestinationPort	\sDPT\=\d{1,5}\s	\sDPT\=(\d{1,5})\s

7. Migre os padrões e os grupos de captura para o documento de extensões de origem de log.

   O fragmento de código a seguir mostra parte do documento usado.

```
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
```

Fazendo upload de documentos de extensão para o QRadar

É possível criar vários documentos de extensão e, em seguida, fazer upload deles e associá-los a vários tipos de origem de log. A lógica da extensão de origem de log (LSX) é então usada para analisar os logs da origem de log não suportada.

Os documentos de extensão podem ser armazenados em qualquer lugar antes de serem transferidos por upload para o IBM Security QRadar.

Procedimento

1. Na guia **Administrador**, clique em **Origens de dados** > **Extensões de origem de log**.
2. Na janela Incluir extensões de origem de log, clique em **Incluir**.
3. Designe um nome.
4. Clique em **Condição de uso como substituição de análise**.
5. Se você estiver usando o DSM Universal, não selecione o documento de extensão como o padrão para um **Tipo de origem de log**.

   Ao selecionar o DSM Universal como o padrão, ele afeta todas as origens de log associadas. Um DSM Universal pode ser usado para definir a lógica de análise de várias origens de eventos customizadas e não suportadas.
6. Opcional: Para aplicar essa extensão de origem de log a mais de uma instância de um tipo de origem de log, selecione o tipo de origem de log na lista **Tipo de origem de log** disponível e clique na seta de inclusão para configurá-lo como o padrão.

   Configurar o tipo de origem de log padrão aplica a extensão de origem de log a todos os eventos de um tipo de origem de log, incluindo as origens de log que são descobertas automaticamente.

   Assegure-se de testar a extensão para o tipo de origem de log primeiro para assegurar que os eventos sejam analisados corretamente.
7. Clique em **Procurar** para localizar o LSX que foi salvo e, em seguida, clique em **Fazer upload**.

   O QRadar valida o documento no XSD interno e verifica sua validade antes de o documento de extensão ser transferido por upload para o sistema.
8. Clique em **Salvar** e feche a janela.
9. Associe a extensão de origem de log a uma origem de log.
   a. Na guia **Administrador**, clique em **Origens de dados** > **Origens de log**.
   b. Clique duas vezes no tipo de origem de log para o qual criou o documento de extensão.

c. Na lista **Extensão de origem de log**, selecione o documento criado.
d. Na lista **Condição de uso da extensão**, selecione **Substituição de análise**.
e. Clique em **Salvar** e feche a janela.

Mapeando eventos desconhecidos

Inicialmente, todos os eventos do DSM Universal aparecem como desconhecidos na guia **Atividade do log** no QRadar. Deve-se mapear manualmente todos os eventos desconhecidos para seus equivalentes no mapa de QID.

Embora os nomes de eventos, como DROP, DENY e ACCEPT possam ser valores entendidos ao serem vistos nos arquivos de log, o QRadar não entende o que eles representam. Para o QRadar, esses valores são sequências de texto não mapeadas para nenhum valor conhecido. Os valores aparecem conforme o esperado e são tratados como eventos normalizados até que sejam manualmente mapeados

Em algumas instâncias, como um sistema de detecção de intrusão (IDS) ou um sistema de detecção e prevenção de intrusão (IDP), milhares de eventos existem e requerem mapeamento. Nessas situações, é possível mapear uma categoria como o nome do evento, em vez dele mesmo. Por exemplo, no exemplo a seguir, para reduzir o número de mapeamentos, em vez de usar o campo de nome para o Nome de evento, use o campo de categoria. É possível usar uma propriedade customizada para exibir o nome do evento (Code Red v412):

```
date: "Feb 25 2010 00:43:26"; name: "SQL Slammer v312"; category: "Worm
Activity"; source ip: "100.100.200.200";⌂date:
"Feb 25 2015 00:43:26"; name: "Code Red v412"; category: "Worm Activity";
source ip: "100.100.200.200"; date: "Feb 25 2015 00:43:26"; name:
"Annoying Toolbar"; category: "Malware"; source ip: "100.100.200.200";
```

Em vez de usar o campo de nome para o Nome de evento, use o campo de categoria. O nome do evento real, por exemplo, Code Red v412 pode ser exibido usando uma propriedade customizada.

Antes de Iniciar

Assegure-se de que tenha transferido por upload o documento de extensão de origem de log e que o tenha aplicado ao DSM Universal. Para obter mais informações, consulte “Fazendo upload de documentos de extensão para o QRadar” na página 42.

Procedimento

1. Na guia **Atividade do log**, clique em **Procurar** > **Editar procura**
2. Nas opções de **Intervalo de tempo**, escolha tempo suficiente, como 15 minutos, a partir de quando a extensão de origem de log foi aplicada ao DSM Universal.
3. Em **Parâmetros de procura**, selecione **Origem de log [indexada]** na lista **Parâmetro**, **Equivale a** na lista **Operador** e, em seguida, selecione a origem de log que foi criada no **Grupo de origem de log** e nas **listas de Origem de log**.
4. Clique em **Procurar** para visualizar os resultados.

   Todos os eventos aparecem como desconhecidos.
5. Clique duas vezes em uma entrada desconhecida para visualizar os detalhes do evento.
6. Clique em **Mapear evento** na barra de ferramentas.

   O valor **ID do evento de origem de log** exibe um **valor EventName**, por exemplo, DROP, DENY ou ACCEPT, na extensão de origem de log. O valor não

pode ficar em branco. Um valor em branco indica que há um erro no documento de extensão de origem de log.

7. Mapeie o valor exibido como o **ID do evento de origem de log** para o QID apropriado.

   Use **Procurar por categoria** ou **Procura de QID**, ou ambos, para localizar um valor que melhor corresponda ao valor **ID do evento de origem de log**. Por exemplo, o valor DROP pode ser mapeado para **Negação de firewall do QID - CRE do evento**.

   Use o QID com o CRE do evento no nome. A maioria dos eventos é específica de um determinado tipo de origem de log. Por exemplo, ao mapear para um firewall aleatório, **Negar QID** é semelhante ao mapeamento do DSM Universal para eventos de outro tipo de origem de log. As entradas de QID que contêm o nome CRE do evento são genéricas e não são ligadas a um determinado tipo de origem de log.

8. Repita essas etapas até que todos os eventos desconhecidos sejam mapeados com êxito.

   Desse ponto, quaisquer outros eventos do DSM Universal que contiverem esse ID do evento de origem de log específico aparecerão como o QID especificado. Eventos que tenham chegado antes do mapeamento de QID permanecem desconhecidos. Não há método suportado para mapeamento de eventos anteriores para um QID atual. Esse processo deve ser repetido até que todos os tipos de evento desconhecidos sejam mapeados com êxito para um QID.

Problemas e exemplos de análise

Ao criar uma extensão de origem de log, é possível encontrar alguns problemas de análise. Use estes exemplos de XML para resolver problemas de análise específicos.

Convertendo um protocolo

O exemplo a seguir mostra uma conversão típica de protocolo que procura TCP, UDP, ICMP ou GRE em qualquer lugar na carga útil. O padrão de procura é circundado por qualquer limite de palavra, por exemplo, tabulação, espaço, término de linha. Além disso, as maiúsculas e minúsculas do caractere são ignoradas:

```
<pattern id="Protocol" case-insensitive="true" xmlns="">
<![CDATA[\b(TCP|UDP|ICMP|GRE)\b]]>
</pattern>
<matcher field="Protocol" order="1" pattern-id="Protocol" capture-group="1" />
```

Fazendo uma única substituição

O exemplo a seguir mostra uma substituição que analisa o endereço IP de origem e, em seguida, substitui o resultado e configura o endereço IP como 100.100.100.100, ignorando o endereço IP na carga útil.

Este exemplo supõe que o endereço IP de origem corresponde a algo semelhante a `SrcAddress=10.3.111.33`, seguido de vírgula:

```
<pattern id="SourceIp_AuthenOK" xmlns="">
<![CDATA[SrcAddress=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}),]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIp_AuthenOK"
capture-group="100.100.100.100" enable-substitutions="true"/>
```

Gerando um endereço MAC separado por dois pontos (:)

O QRadar detecta endereços de MAC em um formato separado por dois pontos (:). Como todos os dispositivos podem não usar esse formato, o exemplo a seguir mostra como corrigir essa situação:

```
<pattern id="SourceMACWithDashes" xmlns="">
    <![CDATA[SourceMAC=([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-
    ([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})]]>
</pattern>
 <matcher field="SourceMAC" order="1" pattern-id="
    SourceMACWithDashes" capture-group="\1:\2:\3:\4:\5:\6" />
```

No exemplo antecedente, `SourceMAC=12-34-56-78-90-AB` é convertido em um endereço MAC `12:34:56:78:90:AB`.

Se os traços forem removidos do padrão, o padrão converterá um endereço MAC e não terá separadores. Se espaços forem inseridos, o padrão converterá um endereço MAC separado por espaço.

Combinando endereço IP e porta

Geralmente, um endereço IP e uma porta são combinados em um campo, que é separado por dois pontos (:).

O exemplo a seguir usa vários grupos de captura com um padrão:

```
pattern id="SourceIPColonPort" xmlns="">
<! [CDATA[Source=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([\d]{1,5})]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIPColonPort" capture-group="1" />
<matcher field="SourcePort" order="1" pattern-id="SourceIPColonPort" capture-group="2" />
```

Modificando uma Categoria de evento

Uma categoria de evento de dispositivo pode ser codificada permanentemente, ou a severidade pode ser ajustada.

O exemplo a seguir ajusta a severidade para um único tipo de evento:

```
<event-match-single event-name="TheEvent" device-event-category="Actual
Category" severity="6" send-identity="UseDSMResults" />
```

Suprimindo eventos de mudança de identidade

Um DSM pode enviar, desnecessariamente, eventos de mudança de identidade.

Os exemplos a seguir mostram como suprimir eventos de mudança de identidade de serem enviados de um único tipo de evento e de um grupo de eventos.

```
// Never send identity for the event with an EventName of Authen OK
<event-match-single event-name="Authen OK" device-event-category="ACS"
severity="6" send-identity="OverrideAndNeverSend" />

// Never send any identity for an event with an event name starting with 7,
followed by one to five other digits:
<pattern id="EventNameId" xmlns=""><![CDATA[(7\d{1,5})]]>
</pattern>

<event-match-multiple pattern-id="EventNameId" capture-group-index="1"
device-event-category="Cisco Firewall" severity="7"
send-identity="OverrideAndNeverSend"/>
```

Codificando logs

Os formatos de codificação a seguir são suportados:

- US-ASCII
- UTF-8

É possível encaminhar logs para o sistema em uma codificação que não corresponda a formatos US-ASCII ou UTF-8. É possível configurar uma sinalização avançada para assegurar que a entrada possa ser novamente codificada para UTF-8 para propósitos de análise e armazenamento.

Por exemplo, para assegurar que os logs de origem cheguem na codificação SHIFT-JIS (ANSI/OEM japonês), digite o código a seguir:

```
<device-extension source-encoding=SHIFT-JIS xmlns=event_parsing/device_extension>
```

Os logs são colocados no formato UTF-8.

Formatando registros de data e hora dos eventos

Uma extensão de origem de log pode detectar vários formatos de registro de data e hora diferentes nos eventos.

Como os fabricantes de dispositivo não se adequam a um formato de registro de data e hora padrão, o parâmetro opcional ext-data é incluído na extensão de origem de log para permitir que DeviceTime seja reformatado. O exemplo a seguir mostra como um evento pode ser reformatado para corrigir a formatação do registro de data e hora:

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\]</pattern>
<pattern id="Username">(TLSv1)</pattern>

<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1_Pattern" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1_Pattern"
   capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username_Pattern" capture-group="1"/>
</match-group>
</device-extension>
```

Vários formatos de log em uma única origem de log

Ocasionalmente, vários formatos de log são incluídos em uma única origem de log.

```
May 20 17:15:50 kernel: DROP IN=vlan2 OUT= MAC= SRC=67.149.62.133
DST=239.255.255.250 PROTO=UDP SPT=1900 DPT=1900
May 20 17:16:26 dropbear[22331]: password auth succeeded for 'root' from 192.168.50.80:3364
May 20 17:16:28 dropbear[22331]: exit after auth (root): Exited normally </br>
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root' from 192.168.50.80:3364
```

Por exemplo, há 2 formatos de log: um para eventos de firewall e outro para eventos de autenticação. Deve-se gravar vários padrões para analisar os eventos. É possível especificar a ordem a ser analisada. Geralmente, os eventos mais frequentes são analisados primeiro, seguidos dos eventos menos frequentes. É possível ter tantos padrões quantos necessários para analisar todos os eventos. A variável order determina a ordem em que os padrões são correspondidos.

O exemplo a seguir mostra vários formatos para os campos EventName e UserName a seguir

Padrões separados são gravados para analisar cada tipo de log exclusivo. Ambos os padrões são referenciados ao designar o valor aos campos normalizados.

```
<pattern id="EventName-DDWRT-FW_Pattern" xmlns=""><![CDATA[kernel\:\s(.*?)\s]]></pattern>
<pattern id="EventName-DDWRT-Auth_Pattern" xmlns=""><![CDATA[sdrophear\[\d{1,5}\]|:\s(.*?\s.*?)\s]]>
</pattern>

<pattern id="UserName_DDWRT-Auth1__Pattern" xmlns=""><![CDATA[\sfor\s\'(.*?)\'s]]></pattern>
<pattern id="UserName_DDWRT-Auth2__Pattern" xmlns=""><![CDATA[\safter\sauth\s\((.*?)\)\:]]></pattern>

<match-group order="1" description="DD-WRT Device Extensions xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-DDWRT-FW_Pattern" capture-group="1"/>
   <matcher field="EventName" order="2" pattern-id="EventName-DDWRT-Auth_Pattern" capture-group="1"/>

   <matcher field="UserName" order="1" pattern-id="UserName-DDWRT-Auth1_Pattern" capture-group="1"/>
   <matcher field="UserName" order="2" pattern-id="UserName-DDWRT-Auth2_Pattern" capture-group="1"/>
```

Analisando um formato de log CSV

Um arquivo de log formatado por CSV pode usar um único analisador que tenha vários grupos de captura. Nem sempre é necessário criar vários IDs de padrão ao analisar esse tipo de log.

Sobre Esta Tarefa

A amostra de log a seguir é usada:

```
Event,User,Source IP,Source Port,Destination IP,Destination Port
Failed Login,bjones,192.168.50.100,1024,10.100.24.25,22
Successful Login,nlabadie,192.168.64.76,1743,10.100.24.25,110
Privilege Escalation,bjones,192.168.50.100,1028,10.100.1.100,23
```

Procedimento

1. Crie um analisador que corresponda a todos os valores relevantes usando os padrões anteriores.

   ```
   .*?\,.*?\,\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
   \,\d{1,5}\,\d{1,3}\.\d{1,3} \.\d{1,3}\.\d{1,3}\,\d{1,5}
   ```

2. Coloque os grupos de captura ao redor de cada valor:

   ```
   (.*?)\,(.*?)\,(\d{1,3}\.\d{1,3}\.\d{1,3}\.
   \d{1,3})\,(\d{1,5})\,(\d{1,3} \.\d{1,3}\.\d{1,3}\.\d{1,3})\,(\d{1,5})
   ```

3. Mapeie o campo para o qual cada grupo de captura está mapeado, incrementando o valor enquanto se move.

   ```
   1 = Event, 2 = User, 3 = Source IP,
   4 = Source Port, 5 = Destination IP, 6 = Destination Port
   ```

4. Inclua os valores na extensão de origem de log mapeando o grupo de captura para o evento relevante.

   O código a seguir mostra um exemplo parcial de mapeamento do grupo de captura para o evento relevante.

   ```
   <pattern id="CSV-Parser_Pattern" xmlns=""><![CDATA 9.*?)\,(.*?)\,(\d{1,3}\.\{1,3}\.{1,3}]]></pattern>
   <match-group order="1" description="Log Source Extension xmlns="">
      <matcher field="EventName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="1"/>
      <matcher field="SourceIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="3"/>
      <matcher field="SourcePort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="4"/>
      <matcher field="DestinationIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="5"/>
      <matcher field="DestinationPort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="6"/>
      <matcher field="UserName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="2"/>
   ```

5. Faça upload da extensão de origem de log.
6. Mapeie os eventos.

Tarefas relacionadas:

"Mapeando eventos desconhecidos" na página 43
Inicialmente, todos os eventos do DSM Universal aparecem como desconhecidos na guia **Atividade do log** no QRadar. Deve-se mapear manualmente todos os eventos desconhecidos para seus equivalentes no mapa de QID.

IDs dos tipos de origem de log

O IBM Security QRadar suporta várias origens de log e cada uma possui um identificador. Use os IDs dos tipos de origem de log em uma instrução `match-group`:

A tabela a seguir lista o tipo de origem de log suportado e seus IDs.

Tabela 36. ID do tipo de origem de log

ID	Tipo de origem de log
2	Snort Open Source IDS
3	Check Point Firewall-1
4	Filtro de firewall configurável
5	Firewall e VPN da Juniper Networks
6	Cisco PIX Firewall
7	Filtro de mensagem de autenticação configurável
9	Enterasys Dragon Network IPS
10	Servidor HTTP Apache
11	S.O. Linux
12	Log de eventos de segurança do Microsoft Windows
13	Windows IIS
14	Linux iptables Firewall
15	IBM Proventia Network Intrusion Prevention System (IPS)
17	Juniper Networks Intrusion Detection and Prevention (IDP)
19	TippingPoint Intrusion Prevention System (IPS)
20	Cisco IOS
21	Comutador VPN Contivity da Nortel
22	Roteador Multiprotocolo Nortel
23	Cisco VPN 3000 Series Cntrator
24	Mensagens de autenticação do Sistema operacional Solaris
25	Dispositivo IPS McAfee IntruShield Network
26	Cisco CSA
28	Comutador E1 Matrix da Enterasys
29	Logs Sendmail do Sistema operacional Solaris
30	Cisco Intrusion Prevention System (IDS)
31	Cisco Firewall Services Module (FWSM)
33	IBM Proventia Management SiteProtector
35	Família Cyberguard FW/VPN KS
36	VPN SSL da Juniper Networks Secure Access (SA)

Tabela 36. ID do tipo de origem de log (continuação)

ID	Tipo de origem de log
37	Comutador VPN Contivity da Nortel
38	Top Layer Intrusion Prevention System (IPS)
39	Universal DSM
40	Tripwire Enterprise
41	Cisco Adaptive Security Appliance (ASA)
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager (NSM)
46	Squid Web Proxy
47	Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)
48	Registros de auditoria do RDBMS da Oracle
49	F5 Networks BIG-IP LTM
50	Logs DHCP do sistema operacional Solaris
55	Gateway de acesso SSL VPN da Array Networks
56	Cisco CatOS para Comutadores Catalyst
57	ProFTPD Server
58	Linux DHCP Server
59	Controlador Infranet da Juniper Networks
64	Plataforma Juniper JunOS
68	Comutador Matrix da Enterasys, série K/N/S
70	Sistema operacional (SO) ExtremeWare da Extreme Networks
71	Dispositivo de segurança Sidewinder G2
73	Gateway de segurança Fortinet FortiGate
78	Dispositivo SonicWall UTM/Firewall/VPN
79	Vericept Content 360
82	Dispositivo Symantec Gateway Security (SGS)
83	Juniper Steel Belted Radius
85	IBM AIX Server
86	Metainfo MetaIP
87	SymantecSystemCenter
90	Cisco ACS
92	Forescout CounterACT
93	McAfee ePolicy Orchestrator
95	Dispositivo CiscoNAC
96	Dispositivos TippingPoint X Series
97	Microsoft DHCP Server
98	Microsoft IAS Server

Tabela 36. ID do tipo de origem de log (continuação)

ID	Tipo de origem de log
99	Servidor Exchange da Microsoft
100	Trend Interscan VirusWall
101	Microsoft SQL Server
102	MAC OS X
103	Dispositivo Bluecoat SG
104	Firewall 6000 com comutador da Nortel
106	Comutador 3Com 8800 Series
107	Gateway VPN da Nortel
108	Nortel Threat Protection System (TPS) Intrusion Sensor
110	Comutador de aplicativos da Nortel
111	Plataforma de aceleração de aplicativos Juniper DX
112	SNARE Reflector Server
113	Roteadores Cisco, série 12000
114	Comutadores Cisco, série 6500
115	Roteadores Cisco, série 7600
116	Sistema de roteamento Cisco Carrier
117	Roteador de serviços integrados Cisco
118	Roteamento de borda de multisserviço Juniper M-Series
120	Firewall 5100 com comutador da Nortel
122	Roteador de serviços Ethernet Juniper MX-Series
123	Plataforma núcleo Juniper T-Series
134	Comutador de roteamento Ethernet 8300/8600 da Nortel
135	Comutador de roteamento Ethernet 2500/4500/5500 da Nortel
136	Roteador seguro da Nortel
138	S.O. OpenBSD
139	Comutador de Ethernet Juniper Ex-Series
140	Sysmark Power Broker
141	Listener do banco de dados Oracle
142	Samhain HIDS
143	Controlador de serviço AAA da Bridgewater Systems
144	Par Nome-valor
145	Secure Network Access Switch (SNAS) da Nortel
146	Starent Networks Home Agent (HA)
148	IBM AS/400 iSeries

Tabela 36. ID do tipo de origem de log (continuação)

ID	Tipo de origem de log
149	Foundry Fastiron
150	Gateway de serviços da Juniper, série SRX
153	CRYPTOCard CRYPTOShield
154	Imperva Securesphere
155	Controlador de mobilidade Aruba
156	Enterasys NetsightASM
157	Enterasys HiGuard
158	Motorola SymbolAP
159	Enterasys HiPath
160	Symantec Endpoint Protection
161	IBM RACF
163	RSA Authentication Manager
164	Redback ASE
165	Trend Micro Office Scan
166	Roteadores de segurança Enterasys XSR
167	Comutadores empilháveis e independentes Enterasys
168	Juniper Networks AVT
169	OS Services Qidmap
170	Enterasys, série A
171	Enterasys, série B2
172	Enterasys, série B3
173	Enterasys, série C2
174	Enterasys, série C3
175	Enterasys, série D
176	Enterasys, série G
177	Enterasys, série I
178	Trend Micro Control Manager
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module (WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	Tandem HP
188	Sentrigo Hedgehog
189	Sybase ASE
191	Microsoft ISA
192	Juniper SRC
193	Radware DefensePro

Tabela 36. ID do tipo de origem de log (continuação)

ID	Tipo de origem de log
194	Cisco ACE Firewall
195	IBM DB2
196	Oracle Audit Vault
197	Sourcefire Defense Center
198	Websense V Series
199	Registro de auditoria do SO RDBMS da Oracle
206	Palo Alto PA Series
208	HP ProCurve
209	Microsoft Operations Manager
210	EMC VMWare
211	IBM WebSphere Application Server
213	F5 Networks BIG-IP ASM
214	FireEye
215	Fair Warning
216	IBM Informix
217	CA Top Secret
218	Enterasys NAC
219	System Center Operations Manager
220	McAfee Web Gateway
221	CA Access Control Facility (ACF2)
222	McAfee Application / Change Control
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Área segura Cyber-Ark
228	Itron Smart Meter
230	Bit9 Parity
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper Networks vGW
239	Oracle BEA WebLogic
240	Dispositivo de segurança da web Sophos
241	Gateway de segurança Sophos Astaro
243	Infoblox NIOS
244	Tropos Control
245	Novell eDirectory

Tabela 36. ID do tipo de origem de log (continuação)

ID	Tipo de origem de log
249	IBM Guardium
251	Centro de gerenciamento Stonesoft
252	SolarWinds Orion
254	Great Bay Beacon
255	Damballa Failsafe
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI
263	Comutador digital China Networks, série DCS e DCRS
264	Coletor de log binário de segurança Juniper
265	Trend Micro Deep Discovery
266	Tivoli Access Manager for e-business
268	Verdasys Digital Guardian
269	Comutador Hauwei S Series
271	HBGary Active Defense
272	APC UPS
272	Controlador Cisco LAN wireless
276	IBM Customer Information Control System (CICS)
278	Barracuda Spam e Virus Firewall
279	Open LDAP
280	DbProtect do Application Security
281	Barracuda Web Application Firewall
283	Huawei AR Series Router
286	IBM AIX Audit
289	IBM Tivoli Endpoint Manager
290	Juniper Junos WebApp Secure
291	Nominum Vantio
292	Comutador Enterasys, série 800
293	IBM zSecure Alert
294	IBM Security Network Protection (XGS)
295	IBM Security Identity Manager
296	F5 Networks BIG-IP AFM
297	IBM Security Network IPS (GX)
298	Fidelis XPS
299	Arpeggio SIFT-IT
300	Barracuda Web Filter
302	Brocade FabricOS

Tabela 36. ID do tipo de origem de log (continuação)

ID	Tipo de origem de log
303	ThreatGRID Malware Threat Intelligence Platform
304	IBM Security Access Manager for Enterprise Single Sign-On
306	Venustech Venusense Unified Threat Management
307	Venustech Venusense Firewall
308	Venustech Venusense Network Intrusion Prevention System
309	ObserveIT
311	Pirean Access: One
312	Venustech Venusense Security Platform
313	PostFix MailTransferAgent
314	Oracle Fine Grained Auditing
315	VMware vCenter
316	Cisco Identity Services Engine
318	Honeycomb Lexicon File Integrity Monitor
319	Oracle Acme Packet SBC
320	Juniper WirelessLAN
330	Arbor Networks Peakflow SP
331	Zscaler Nss
332	Proofpoint Enterprise Protection/Enterprise Privacy
338	Microsoft Hyper-V
339	Cilasoft QJRN/400
340	Segurança de dados Vormetric
341	SafeNet DataSecure/KeySecure
343	STEALTHbits StealthINTERCEPT
344	Juniper DDoS Secure
345	Arbor Networks Pravail
346	Trusteer Apex
348	IBM Security Directory Server
349	Enterasys A4-Series
350	Enterasys B5-Series
351	Enterasys C5-Series
354	Gateway VPN Avaya
356	DG Technology MEAS
358	CloudPassage Halo
359	CorreLog Agent for IBM zOS
360	WatchGuard Fireware OS
361	IBM Fiberlink MaaS360

Tabela 36. ID do tipo de origem de log (continuação)

ID	Tipo de origem de log
362	Trend Micro Deep Discovery Analyzer
363	AccessData InSight
364	BM Privileged Session Recorder
367	Universal CEF
369	FreeRADIUS
370	Riverbed SteelCentral NetProfiler
372	SSH CryptoAuditor
373	IBM WebSphere DataPower
374	Symantec Critical System Protection
375	Kisco Information Systems SafeNet/i
376	IBM Federated Directory Server
378	Lastline Enterprise
379	genua genugate
383	Oracle Enterprise Manager

Capítulo 3. Gerenciamento de extensão de fonte de log

É possível criar extensões de fonte de log para estender ou modificar as rotinas de análise de dispositivos específicos.

Uma *extensão de fonte de log* é um arquivo XML que inclui todos os padrões de expressão regular que são necessários para identificar e categorizar eventos a partir da carga útil do evento. Arquivos de extensão podem ser utilizados para analisar eventos quando se deve corrigir um problema de análise ou substituir a análise padrão para um evento de um DSM. Quando um DSM não existir para analisar eventos de um dispositivo ou dispositivo de segurança em sua rede, uma extensão pode fornecer suporte de eventos. A guia **Atividade do Log** identifica os eventos da origem do log nesses tipos básicos:

- Origens de log que analisam corretamente o evento. Eventos analisados corretamente são designados ao tipo e categoria de fonte de log corretos. Neste caso, nenhuma intervenção ou extensão é necessária.
- Origens de log que analisam eventos, mas possuem um valor **Desconhecido** no parâmetro **Origem de Log**. Eventos desconhecidos são eventos de fonte de log em que o tipo de fonte de log é identificado, mas as informações de carga útil não podem ser entendidas pelo DSM. O sistema não pode determinar um identificador de eventos a partir das informações disponíveis para categorizar corretamente o evento. Nesse caso, o evento pode ser mapeado para uma categoria ou uma extensão de fonte de log que pode ser gravada para reparar a análise de evento para eventos desconhecidos.
- As origens de log que não podem identificar o tipo de fonte de log e que possuem um valor de evento **Armazenado** no parâmetro **Origem de Log**. Eventos armazenados requerem a atualização de seus arquivos DSM ou a gravação de uma extensão de fonte de log para analisar corretamente o evento. Após o evento ser analisado, será possível, em seguida, mapear os eventos.

Antes de poder incluir uma extensão de fonte de log, deve-se criar o documento de extensão. O documento de extensão é um documento XML o qual é possível criar com qualquer aplicativo de processamento comum ou palavra de edição de texto. Diversos documentos de extensão podem ser criados, transferidos por upload e associados a diversos tipos de fonte de log. O formato do documento de extensão deve estar de acordo com um documento de esquema XML (XSD) padrão. Para desenvolver um documento de extensão, será necessário ter conhecimento e experiência com a codificação XML.

Incluindo uma extensão de fonte de log

É possível incluir uma extensão de fonte de log para estender ou modificar as rotinas de análise de dispositivos específicos.

Procedimento

1. Clique na guia **Administrador**.
2. Clique no ícone **Extensões de Origem de Log**.
3. Clique em **Incluir**.
4. Na lista **Condição de uso**, selecione uma das opções a seguir:

Opção	Descrição
Aprimoramento de Análise	Selecione esta opção quando o módulo de suporte de dispositivo (DSM) analisar corretamente a maioria dos campos para a fonte de log. Os valores de campo analisados incorretamente são aprimorados com os novos valores XML.
Substituição de Análise	Selecione esta opção quando o módulo de suporte de dispositivo (DSM) for incapaz de analisar corretamente. A extensão de fonte de log substitui completamente a análise com falha pelo DSM e substitui a análise pelos novos valores XML.

5. Na lista **Tipos de Origem de Log**, selecione uma das seguintes opções:

Opção	Descrição
Disponível	Selecione esta opção quando o módulo de suporte de dispositivo (DSM) analisar corretamente a maioria dos campos para a fonte de log. Os valores de campo analisados incorretamente são aprimorados com os novos valores XML.
Configurar para padrão de	Selecione as origens de log para incluir ou remover da análise da extensão. É possível incluir ou remover extensões a partir de uma fonte de log. Quando uma extensão de fonte de log for **Configurar para o padrão de** uma fonte de log, novas origens de log do mesmo **Tipo de Origem de Log** utilizarão a extensão de fonte de log designada.

6. Clique em **Procurar** para localizar o documento XML de extensão de fonte de log.
7. Clique em **Upload**. O conteúdo da extensão de fonte de log é exibido para assegurar que o arquivo de extensão apropriado seja transferido por upload. O arquivo de extensão é avaliado com relação ao XSD para erros quando o arquivo é transferido por upload.
8. Clique em **Salvar**.

Resultados

Se o arquivo de extensão não contiver nenhum erro, a nova extensão de fonte de log será criada e ativada. É possível fazer upload de uma extensão de fonte de log sem aplicar a extensão a uma fonte de log. Qualquer mudança no status de uma extensão será aplicada imediatamente e os hosts ou Consoles gerenciados aplicam os novos parâmetros de análise de evento na extensão de fonte de log.

O que Fazer Depois

Na guia **Atividade do Log**, verifique se os padrões de análise de eventos são aplicados corretamente. Se a fonte de log categorizar eventos como **Armazenados**, o padrão de análise na extensão de fonte de log requer ajuste. É possível revisar o arquivo de extensão com relação aos eventos de fonte de log para localizar

qualquer questão de análise sintática do evento.

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 mudanças 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).

Os termos a seguir são marcas comerciais ou marcas registradas de outras empresas:

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

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

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

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

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

Considerações de política de privacidade

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

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

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

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a política de privacidade da IBM em http://www.ibm.com/privacy, a Declaração de privacidade on-line 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

Impresso no Brasil