IBM Security QRadar
Versão 7.2.2

Guia do Usuário do Log Sources

S517-1603-00

Nota

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 27.

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 por meio da prevenção, detecção e resposta ao acesso incorreto dentro e fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mau uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança individual pode ser completamente eficaz na prevenção do acesso ou uso impróprio. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que, necessariamente, envolverá procedimentos operacionais adicionais e poderá precisar de outros sistemas, produtos ou serviços para se tornar mais efetiva. A IBM NÃO GARANTE QUE QUAISQUER SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU QUE DEIXARÃO SUA EMPRESA ESTEJA IMUNE DE CONDUTAS MALICIOSAS OU ILEGAIS DE TERCEIROS.

Capítulo 1. Gerenciamento de fontes 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 *origem 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 proteção contra 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 origem 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 origem 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 origem 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 origem de log.

Incluindo uma origem de log

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

Sobre Esta Tarefa

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

Tabela 1. Parâmetros de origem de log

Parâmetro	Descrição
Identificador de Origem de Log	O endereço IPv4 ou o nome do host que identificam a origem 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 origem 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 origem de log. O valor da credibilidade que é designado a uma origem 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. Utilize este parâmetro em uma implementação distribuída para melhorar o desempenho do sistema do QRadar Console movendo 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 origem de log.
5. Configure os parâmetros específicos de protocolo para sua origem 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 origem 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 bancos de dados do MSDE que estiverem dentro de 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 origem 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 origem 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).
Usar Comunicação de Canal Nomeado	Conexões de canal nomeado para os bancos de dados do MSDE requerem que o campo nome de usuário e senha utilizem o nome de usuário e senha de autenticação do Windows em vez do nome e senha do usuário do banco de dados. A configuração da origem 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 utilizar o protocolo Java Database Connectivity (JDBC) SiteProtector para pesquisar remotamente os bancos de dados do IBM Proventia® Management SiteProtector® para eventos.

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

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

Tabela 3. JDBC - Parâmetros do protocolo SiteProtector

Parâmetro	Descrição
Configuração do Protocolo	**JDBC - SiteProtector**

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

Parâmetro	Descrição
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 JDBC SiteProtector deve corresponder à porta 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 origem 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 você selecionar MSDE e o banco de dados estiver configurado para Windows, deve-se 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 origem de log. As consultas de banco de dados predefinidas estão disponíveis apenas para conexões com a origem 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`
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 a partir do IBM SiteProtector®.

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

Parâmetro	Descrição
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.
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 utilizar uma conexão de Canal Nomeado, o nome de usuário e a senha devem ser o nome de usuário e a senha da autenticação do Windows apropriados, e não o nome de usuário e senha do banco de dados. A configuração da origem 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 origem de log. O idioma da origem 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 origem 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**

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

Parâmetro	Descrição
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 origem de log ser salva e implementada.
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.

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

Parâmetro	Descrição
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 nomeado para os bancos de dados do MSDE requerem que o campo de nome de usuário e senha utilizem um nome de usuário e senha de autenticação do Windows e não a senha e o nome de usuário do banco de dados. A configuração da origem 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 origem de log para utilizar o 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 origem 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`.

Tabela 6. Parâmetros do protocolo OPSEC/LEA (continuação)

Parâmetro	Descrição
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 origem 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 origem 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 origem 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**

Tabela 8. Parâmetros do protocolo SNMPv2 (continuação)

Parâmetro	Descrição
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 origem 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 origem 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`.

Opções de configuração de protocolo de arquivo de log

Para receber eventos a partir de hosts remotos, configure uma origem 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.
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**.

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

Parâmetro	Descrição
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 origem 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 origem de log para utilizar o protocolo Microsoft Security Event Log. É possível utilizar o Microsoft Windows Management Instrumentation (WMI) 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 origem de log utilizadas para o 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 utilizando o protocolo do Microsoft Security Event Log.

O protocolo Microsoft Security Event Log não é recomendado para servidores remotos que forem acessados por links de rede, por exemplo, sistemas que possuem tempos altos de atraso de roundtrip, como satélite ou redes WAN lentas. 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 do Windows Management Instrumentation (WMI):

- 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 de servidores Microsoft DHCP, configure uma origem de log para utilizar 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.

Campos para o protocolo Microsoft DHCP que os caminhos de arquivo de suportam 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 da Microsoft NTLMv2 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 IPv4: `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 origem de log para utilizar 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.

Campos para o protocolo Microsoft Exchange que os caminhos de arquivo de suportam 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 ou o protocolo de autenticação Microsoft NTLMv2 Session.

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.

Tabela 14. Parâmetros do protocolo Microsoft Exchange (continuação)

Parâmetro	Descrição
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 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 o QRadar 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 origem de log para utilizar o protocolo Microsoft IIS. Esse 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.

Campos para o protocolo Microsoft IIS que os caminhos de arquivo de suportam 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 da Microsoft NTLMv2 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 origem 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 origem 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 origem 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 origem 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 utiliza 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 origem de log para usar o protocolo PCAP Syslog Combination.

Antes de configurar uma origem 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 origem 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 origem 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 origem 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 origem de log para usar o protocolo TLS Syslog.

A origem 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 para a porta que é criada para a origem de log.

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

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.

Após a origem de log ser salva, um certificado `syslog-tls` será criado para o dispositivo de origem 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 origem 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 origem 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 origem de log ser salva, um certificado syslog-tls será criado para a origem 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 origem de log syslog TLS.

Opções de configuração de protocolo syslog de multilinhas TCP

É possível configurar uma origem 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 origem 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) a partir de dispositivos do IBM Tivoli Endpoint Manager, configure uma origem de log que utiliza o protocolo IBM Tivoli Endpoint Manager SOAP.

Esse protocolo requer o IBM Tivoli Endpoint Manager versões V8.2.x ou posterior 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 do protocolo 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 origem de log seja salva e implementada.

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

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

Incluindo origens de log em massa

É possível incluir até 500 origens de log do Microsoft Windows ou Universal DSM de uma vez. Ao incluir várias origens de log de uma vez, é incluída uma origem 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**, selecione **Inclusão em Massa**.
4. Configure os parâmetros para a origem de log em massa.
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 origem 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 origem de log. A ordem da análise assegura que o desempenho do sistema não seja afetado pelas mudanças na configuração da origem 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 origem de log mais importantes.

Procedimento

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

Capítulo 2. Gerenciamento de extensão de origem de log

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

Uma *extensão de origem 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 origem 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 origem de log em que o tipo de origem 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 origem 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 origem 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 origem 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 origem 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 origem 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 origem de log

É possível incluir uma extensão de origem 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 **Usar Condição**, selecione uma das seguintes opções:

Opção	Descrição
Aprimoramento de Análise	Selecione esta opção quando o módulo de suporte de dispositivo (DSM) analisar corretamente a maioria dos campos para a origem 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 origem de log substitui completamente a análise com falha pelo DSM e substitui a análise com os 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 origem 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 origem de log. Quando uma extensão de origem de log for **Configurar para o padrão de** uma origem de log, novas origens de log do mesmo **Tipo de Origem de Log** utilizarão a extensão de origem de log designada.

6. Clique em **Procurar** para localizar o documento XML de extensão de origem de log.
7. Clique em **Upload**. O conteúdo da extensão de origem 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 origem de log será criada e ativada. É possível fazer upload de uma extensão de origem de log sem aplicar a extensão a uma origem 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 origem de log.

O que Fazer Depois

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

para localizar quaisquer eventos de análise de problemas.

Avisos

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

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

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

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

Para consultas sobre licenças a respeito de informações do conjunto de caracteres de byte duplo (DBCS), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie consultas, por escrito, para:

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

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

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

Estas informações podem incluir imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

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

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

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

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-14
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

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

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

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

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

Todas as instruções relativas às direções ou intenções futuras da IBM estão sujeitas a mudanças ou retirada sem aviso prévio, e apenas representam metas e objetivos.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso. Os preços dos revendedores podem variar.

Essas informações contêm exemplos de dados e relatórios usados em operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

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

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se 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 registradas dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações forem publicadas. Estas marcas registradas também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atual de marcas registradas IBM está disponível na Web em Informações de copyright e de marca registrada (www.ibm.com/legal/copytrade.shtml).

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

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

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

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

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

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

Considerações de política de privacidade

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

Dependendo das configurações implementadas, essa Oferta de Software poderá usar cookies de sessão que coletam o ID da sessão de cada usuário para fins de

gerenciamento de sessões e autenticação. Estes cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

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

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de Privacidade da IBM em http://www.ibm.com/privacy, a seção intitulada “Cookies, Web Beacons e Outras Tecnologias”, na Declaração de Privacidade Online da IBM em http://www.ibm.com/privacy/details/br/pt/ e “IBM Software Products and Software-as-a-Service Privacy Statement” em http://www.ibm.com/software/info/product-privacy.

Índice Remissivo