IBM Security QRadar
Version 7.1.x and 7.2.x

Log Sources User Guide

IBM

Contents

About this guide

Log sources are third-party devices that send events to IBM® Security QRadar® for collection, storage, parsing, and processing.

Intended audience

Administrators must have QRadar access and knowledge of the corporate network and networking technologies.

Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Introduction to log source management

You can configure IBM Security QRadar to accept event logs from log sources that are on your network. A *log source* is a data source that creates an event log.

For example, a firewall or intrusion protection system (IPS) logs security-based events, and switches or routers logs network-based events.

To receive raw events from log sources, QRadar supports many protocols. *Passive protocols* listen for events on specific ports. *Active protocols* use APIs or other communication methods to connect to external systems that poll and retrieve events.

Depending on your license limits, QRadar can read and interpret events from more than 300 log sources.

To configure a log source for QRadar, you must do the following tasks:

1. Download and install a device support module (DSM) that supports the log source. A *DSM* is software application that contains the event patterns that are required to identify and parse events from the original format of the event log to the format that QRadar can use. For more information about DSMs and the supported log sources, see the *DSM Configuration Guide.*

2. If automatic discovery is supported for the DSM, wait for QRadar to automatically add the log source to your list of configured log sources.

3. If automatic discover is not supported for the DSM, manually create the log source configuration.

Adding a log source

If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

About this task

The following table describes the common log source parameters for all log source types:

Table 1. Log source parameters

Parameter	Description
Log Source Identifier	The IPv4 address or host name that identifies the log source. If your network contains multiple devices that are attached to a single management console, specify the IP address of the individual device that created the event. A unique identifier for each, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.

Table 1. Log source parameters (continued)

Parameter	Description
Enabled	When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
Credibility	Credibility is a representation of the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events or adjusted as a response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	Specifies the QRadar Event Collector that polls the remote log source.

Use this parameter in a distributed deployment to improve Console system performance by moving the polling task to an Event Collector. |
| Coalescing Events | Increases the event count when the same event occurs multiple times within a short time interval. Coalesced events provide a way to view and determine the frequency with which a single event type occurs on the **Log Activity** tab.

When this check box is clear, events are viewed individually and events are not bundled.

New and automatically discovered log sources inherit the value of this check box from the **System Settings** configuration on the **Admin** tab. You can use this check box to override the default behavior of the system settings for an individual log source. |

Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Click **Add**.
4. Configure the common parameters for your log source.
5. Configure the protocol-specific parameters for your log source.
6. Click **Save**.
7. On the **Admin** tab, click **Deploy Changes**.

JDBC protocol configuration options

QRadar uses the JDBC protocol to collect information from tables or views that contain event data from several database types.

The following table describes the protocol-specific parameters for the JDBC protocol:

Table 2. JDBC protocol parameters

Parameter	Description
Database Type	From the list box, select the type of database that contains the events.
Database Name	The database name must match the database name that is specified in the **Log Source Identifier** field.
Port	The JDBC port must match the listen port that is configured on the remote database. The database must permit incoming TCP connections. If a **Database Instance** is used with the MSDE database type, administrators must leave the **Port** parameter blank in the log source configuration.
Username	A user account for QRadar in the database.
Authentication Domain	A domain must be configured for MSDE databases that are within a Windows domain. If your network does not use a domain, leave this field blank.
Database Instance	The database instance, if required. MSDE databases can include multiple SQL server instances on one server.

When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the **Database Instance** parameter must be blank in the log source configuration. |
Predefined Query	Optional.
Table Name	The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).
Select List	The list of fields to include when the table is polled for events. You can use a comma-separated list or type * to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the **Compare Field**.
Compare Field	A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. Enables the protocol to identify events that were previously polled by the protocol to ensure that duplicate events are not created.
Use Prepared Statements	Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.
Start Date and Time	If a start time is not defined, the protocol attempts to poll for events after the log source configuration is saved and deployed.
Polling Interval	The default polling interval is 10 seconds.
EPS Throttle	The upper limit for the permitted number of Events Per Second (EPS).

Table 2. JDBC protocol parameters (continued)

Parameter	Description
Use Named Pipe Communication	Named pipe connections for MSDE databases require that the user name and password field use a Windows authentication user name and password instead of the database user name and password. The log source configuration must use the default named pipe on the MSDE database.
Use NTLMv2	The **Use NTLMv2** check box does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.

JDBC SiteProtector configuration options

You can configure log sources to use the Java™ Database Connectivity (JDBC) SiteProtector™ protocol to remotely poll IBM Proventia® Management SiteProtector® databases for events.

The JDBC - SiteProtector protocol combines information from the SensorData1 and SensorDataAVP1 tables in the creation of the log source payload. The SensorData1 and SensorDataAVP1 tables are in the IBM Proventia® Management SiteProtector® database. The maximum number of rows that the JDBC - SiteProtector protocol can poll in a single query is 30,000 rows.

The following table describes the protocol-specific parameters for the JDBC - SiteProtector protocol:

Table 3. JDBC - SiteProtector protocol parameters

Parameter	Description
Protocol Configuration	**JDBC - SiteProtector**
Database Type	From the list, select **MSDE** as the type of database to use for the event source.
Database Name	Type RealSecureDB the name of the database to which the protocol can connect.
IP or Hostname	The IP address or host name of the database server.
Port	The port number that is used by the database server. The JDBC SiteProtector configuration port must match the listener port of the database. The database must have incoming TCP connections enabled. If you define a **Database Instance** when with MSDE as the database type, you must leave the **Port** parameter blank in your log source configuration.
Username	If you want to track access to a database by the JDBC protocol, you can create a specific use for your QRadar system.
Authentication Domain	If you select MSDE and the database is configured for Windows, you must define a Windows domain. If your network does not use a domain, leave this field blank.

Table 3. JDBC - SiteProtector protocol parameters (continued)

Parameter	Description
Database Instance	If you select MSDE and you have multiple SQL server instances on one server, define the instance to which you want to connect. If you use a non-standard port in your database configuration, or access is blocked to port 1434 for SQL database resolution, you must leave the **Database Instance** parameter blank in your configuration.
Predefined Query	The predefined database query for your log source. Predefined database queries are only available for special log source connections.
Table Name	`SensorData1`
AVP View Name	`SensorDataAVP`
Response View Name	`SensorDataResponse`
Select List	Type * to include all fields from the table or view.
Compare Field	`SensorDataRowID`
Use Prepared Statements	Prepared statements allow the JDBC protocol source to set up the SQL statement, and then execute the SQL statement numerous times with different parameters. For security and performance reasons, use prepared statements. You can clear this check box to use an alternative method of querying that does not use pre-compiled statements.
Include Audit Events	Specifies to collect audit events from IBM SiteProtector®.
Start Date and Time	Optional. A start date and time for when the protocol can start to poll the database.
Polling Interval	The amount of time between queries to the event table. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. Numeric values without an H or M designator poll in seconds.
EPS Throttle	The number of Events Per Second (EPS) that you do not want this protocol to exceed.
Use Named Pipe Communication	If you select MSDE as the database type, select the check box to use an alternative method to a TCP/IP port connection. When you use a Named Pipe connection, the user name and password must be the appropriate Windows authentication username and password and not the database user name and password. The log source configuration must use the default named pipe.
Database Cluster Name	The cluster name to ensure that named pipe communications function properly.
Use NTLMv2	Forces MSDE connections to use the NTLMv2 protocol with SQL servers that require NTLMv2 authentication. The **Use NTLMv2** check box does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
Use SSL	Enables SSL encryption for the JDBC protocol.
Log Source Language	Select the language of the events that are generated by the log source. The log source language helps the system parse events from external appliances or operating systems that can create events in multiple languages.

Sophos Enterprise Console JDBC protocol configuration options

To receive events from Sophos Enterprise Consoles, configure a log source to use the Sophos Enterprise Console JDBC protocol.

The Sophos Enterprise Console JDBC protocol combines payload information from application control logs, device control logs, data control logs, tamper protection logs, and firewall logs in the vEventsCommonData table. If the Sophos Enterprise Console does not have the Sophos Reporting Interface, you can use the standard JDBC protocol to collect antivirus events.

The following table describes the parameters for the Sophos Enterprise Console JDBC protocol:

Table 4. Sophos Enterprise Console JDBC protocol parameters

Parameter	Description
Protocol Configuration	**Sophos Enterprise Console JDBC**
Database Type	**MSDE**
Database Name	The database name must match the database name that is specified in the **Log Source Identifier** field.
Port	The default port for MSDE in Sophos Enterprise Console is 1168. The JDBC configuration port must match the listener port of the Sophos database to communicate with QRadar. The Sophos database must have incoming TCP connections enabled. If a **Database Instance** is used with the MSDE database type, you must leave the **Port** parameter blank.
Authentication Domain	If your network does not use a domain, leave this field blank.
Database Instance	The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or administrators block access to port 1434 for SQL database resolution, the **Database Instance** parameter must be blank.
Table Name	vEventsCommonData
Select List	*
Compare Field	InsertedAt
Use Prepared Statements	Prepared statements enable the protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most configurations can use prepared statements. Clear this check box to use an alternative method of querying that do not use pre-compiled statements.
Start Date and Time	Optional. A start date and time for when the protocol can start to poll the database. If a start time is not defined, the protocol attempts to poll for events after the log source configuration is saved and deployed.

Table 4. Sophos Enterprise Console JDBC protocol parameters (continued)

Parameter	Description
Polling Interval	The polling interval, which is the amount of time between queries to the database. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.
EPS Throttle	The number of Events Per Second (EPS) that you do not want this protocol to exceed.
Use Named Pipe Communication	If MSDE is configured as the database type, administrators can select this check box to use an alternative method to a TCP/IP port connection. Named pipe connections for MSDE databases require the user name and password field to use a Windows authentication username and password and not the database user name and password. The log source configuration must use the default named pipe on the MSDE database.
Database Cluster Name	If you use your SQL server in a cluster environment, define the cluster name to ensure that named pipe communications function properly.
Use NTLMv2	Forces MSDE connections to use the NTLMv2 protocol with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. The **Use NTLMv2** check box does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.

Juniper Networks NSM protocol configuration options

To receive Juniper Networks NSM and Juniper Networks Secure Service Gateway (SSG) logs events, configure a log source to use the Juniper Networks NSM protocol.

The following table describes the protocol-specific parameters for the Juniper Networks Network and Security Manager protocol:

Table 5. Juniper Networks NSM protocol parameters

Parameter	Description
Log Source Type	**Juniper Networks Network and Security Manager**
Protocol Configuration	**Juniper NSM**

OPSEC/LEA protocol configuration options

To receive events on port 18484, configure a log source to use the OPSEC/LEA protocol is a protocol.

The following table describes the protocol-specific parameters for the OPSEC/LEA protocol:

Table 6. OPSEC/LEA protocol parameters

Parameter	Description
Protocol Configuration	**OPSEC/LEA**
Server Port	You must verify that QRadar can communicate on port 18184 by using the OPSEC/LEA protocol.
Statistics Report Interval	The interval, in seconds, during which the number of syslog events are recorded in the `qradar.log` file.
OPSEC Application Object SIC Attribute (SIC Name)	The Secure Internal Communications (SIC) name is the distinguished name (DN) of the application, for example: `CN=LEA, o=fwconsole..7psasx`.
Log Source SIC Attribute (Entity SIC Name)	The SIC name of the server, for example: `cn=cp_mgmt,o=fwconsole..7psasx`.
OPSEC Application	The name of the application that makes the certificate request.

SDEE protocol configuration options

You can configure a log source to use the Security Device Event Exchange (SDEE) protocol. QRadar uses the protocol to collect events from appliances that use SDEE servers.

The following table describes the protocol-specific parameters for the SDEE protocol:

Table 7. SDEE protocol parameters

Parameter	Description
Protocol Configuration	**SDEE**
URL	The HTTP or HTTPS URL that is required to access the log source, for example, https://www.mysdeeserver.com/cgi-bin/sdee-server.
	For SDEE/CIDEE (Cisco IDS v5.x and later), the URL must end with `/cgi-bin/sdee-server`. Administrators with RDEP (Cisco IDS v4.x), the URL must end with `/cgi-bin/event-server`.
Force Subscription	When the check box is selected, the protocol forces the server to drop the least active connection and accept a new SDEE subscription connection for the log source.
Maximum Wait To Block For Events	When a collection request is made and no new events are available, the protocol enables an event block. The block prevents another event request from being made to a remote device that did not have any new events. This timeout is intended to conserve system resources.

SNMPv2 protocol configuration options

You can configure a log source to use the SNMPv2 protocol to receive SNMPv2 events.

The following table describes the protocol-specific parameters for the SNMPv2 protocol:

Table 8. SNMPv2 protocol parameters

Parameter	Description
Protocol Configuration	**SNMPv3**
Community	The SNMP community name that is required to access the system that contains SNMP events.
Include OIDs in Event Payload	Specifies that the SNMP event payload is constructed by using name-value pairs instead of the event payload format. When you select specific log sources from the **Log Source Types** list, OIDs in the event payload are required for processing SNMPv2 or SNMPv3 events.

SNMPv3 protocol configuration options

You can configure a log source to use the SNMPv3 protocol to receive SNMPv3 events.

The following table describes the protocol-specific parameters for the SNMPv3 protocol:

Table 9. SNMPv3 protocol parameters

Parameter	Description
Protocol Configuration	**SNMPv3**
Authentication Protocol	The algorithms to use to authenticate SNMP traps:
Include OIDs in Event Payload	Specifies that the SNMP event payload is constructed by using name-value pairs instead of the standard event payload format. When you select specific log sources from the **Log Source Types** list, OIDs in the event payload are required for processing SNMPv2 or SNMPv3 events.

Sourcefire Defense Center Estreamer protocol configuration options

To receive events from a Sourcefire Defense Center Estreamer (Event Streamer) service, configure a log source to use the Sourcefire Defense Center Estreamer protocol.

Event files are streamed to QRadar to be processed after the Sourcefire Defense Center DSM is configured.

The following table describes the protocol-specific parameters for the Sourcefire Defense Center Estreamer protocol:

Table 10. Sourcefire Defense Center Estreamer protocol parameters

Parameter	Description
Protocol Configuration	**Sourcefire Defense Center Estreamer**
Server Port	The default port that QRadar uses for Sourcefire Defense Center Estreamer is 8302.
Keystore Filename	The directory path and file name for the keystore private key and associated certificate. By default, the import script creates the keystore file in the following directory: /opt/qradar/conf/estreamer.keystore.

Table 10. Sourcefire Defense Center Estreamer protocol parameters (continued)

Parameter	Description
Truststore Filename	The truststore file contains the certificates that are trusted by the client. By default, the import script creates the truststore file in the following directory: /opt/qradar/conf/estreamer.truststore.

Log file protocol configuration options

To receive events from remote hosts, configure a log source to use the log file protocol.

The log file protocol is intended for systems that write daily event logs. It is not appropriate to use the log file protocol for devices that append information to their event files.

Log files are retrieved one at a time. The log file protocol can manage plain text, compressed files, or file archives. Archives must contain plain-text files that can be processed one line at a time. When the log file protocol downloads an event file, the information that is received in the file updates the **Log Activity** tab. If more information is written to the file after the download is complete, the appended information is not processed.

The following table describes the protocol-specific parameters for the Log File protocol:

Table 11. Log file protocol parameters

Parameter	Description
Protocol Configuration	**Log File**
Remote Port	If the remote host uses a non-standard port number, you must adjust the port value to retrieve events.
SSH Key File	The path to the SSH key, if the system is configured to use key authentication. When an SSH key file is used, the **Remote Password** field is ignored.
Remote Directory	For FTP, if the log files are in the remote user's home directory, you can leave the remote directory blank. A blank remote directory field supports systems where a change in the working directory (CWD) command is restricted.
Recursive	This option is ignored for SCP file transfers.
FTP File Pattern	The regular expression (regex) required to identify the files to download from the remote host.
FTP Transfer Mode	For ASCII transfers over FTP, you must select NONE in the **Processor** field and LINEBYLINE in the **Event Generator** field.
Recurrence	The time interval to determine how frequently the remote directory is scanned for new event log files. The time interval can include values in hours (H), minutes (M), or days (D). For example, a recurrence of 2H scans the remote directory every 2 hours.

Table 11. Log file protocol parameters (continued)

Parameter	Description
Run On Save	Starts the log file import immediately after you save the log source configuration. When selected, this check box clears the list of previously downloaded and processed files. After the first file import, the log file protocol follows the start time and recurrence schedule that is defined by the administrator.
EPS Throttle	The number of Events Per Second (EPS) that the protocol cannot exceed.
Change Local Directory?	Changes the local directory on the **Target Event Collector** to store event logs before they are processed.
Local Directory	The local directory on the **Target Event Collector**. The directory must exist before the log file protocol attempts to retrieve events.
File Encoding	The character encoding that is used by the events in your log file.
Folder Separator	The character that is used to separate folders for your operating system. Most configurations can use the default value in **Folder Separator** field. This field is intended for operating systems that use a different character to define separate folders. For example, periods that separate folders on mainframe systems.

Microsoft Security Event Log protocol configuration options

You can configure a log source to use the Microsoft Security Event Log protocol. You can use Microsoft Windows Management Instrumentation (WMI) to collect customized event logs or agent less Windows Event Logs.

The WMI API requires that firewall configurations accept incoming external communications on port 135 and on any dynamic ports that are required for DCOM. The following list describes the log source limitations that you use the Microsoft Security Event Log Protocol:

- Systems that exceed 50 events per second (eps) might exceed the capabilities of this protocol. Use WinCollect for systems that exceed 50 eps.
- A QRadar all-in-one installation can support up to 250 log sources with the Microsoft Security Event Log protocol.
- Dedicated Event Collectors can support up to 500 log sources by using the Microsoft Security Event Log protocol.

The Microsoft Security Event Log protocol is not suggested for remote servers that are accessed over network links, for example, systems that have high round-trip delay times, such as satellite or slow WAN networks. You can confirm round-trip delays by examining requests and response time that is between a server ping. Network delays that are created by slow connections decrease the EPS throughput available to those remote servers. Also, event collection from busy servers or domain controllers rely on low round-trip delay times to keep up with incoming events. If you cannot decrease your network round-trip delay time, you can use WinCollect to process Windows events.

The Microsoft Security Event Log supports the following software versions with the Microsoft Windows Management Instrumentation (WMI) API:

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

The following table describes the protocol-specific parameters for the Microsoft Security Event Log protocol:

Table 12. Microsoft Security Event Log protocol parameters

Parameter	Description
Protocol Configuration	**Windows Security Event Log**

Microsoft DHCP protocol configuration options

To receive events from Microsoft DHCP servers, configure a log source to use the Microsoft DHCP protocol.

To read the log files, folder paths that contain an administrative share (C$), require NetBIOS privileges on the administrative share (C$). Local or domain administrators have sufficient privileges to access log files on administrative shares.

Fields for the Microsoft DHCP protocol that support file paths allow administrators to define a drive letter with the path information. For example, the field can contain the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/`directory for a public share folder path, but cannot contain the `c:/LogFiles` directory.

Restriction: The Microsoft authentication protocol NTLMv2 is not supported by the Microsoft DHCP protocol.

The following table describes the protocol-specific parameters for the Microsoft DHCP protocol:

Table 13. Microsoft DHCP protocol parameters

Parameter	Description
Protocol Configuration	**Microsoft DHCP**
Domain	Optional.
Folder Path	The directory path to the DHCP log files.
File Pattern	The regular expression (regex) that identifies event logs. The log files must contain a three-character abbreviation for a day of the week. Use one of the following file patterns: • IPv4 file pattern: `DhcpSrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri| Sat)\.log`. • IPv6 file pattern: `DhcpV6SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) \.log`. • Mixed IPv4 and IPv6 file pattern: `Dhcp.*SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) \.log`.

Microsoft Exchange protocol configuration options

To receive events from SMTP, OWA, and Microsoft Exchange 2007 and 2010 servers, configure a log source to use the Microsoft Windows Exchange protocol to support.

To read the log files, folder paths that contain an administrative share (C$), require NetBIOS privileges on the administrative share (C$). Local or domain administrators have sufficient privileges to access log files on administrative shares.

Fields for the Microsoft Exchange protocol that support file paths allow administrators to define a drive letter with the path information. For example, the field can contain the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/`directory for a public share folder path, but cannot contain the `c:/LogFiles` directory.

Important: The Microsoft Exchange protocol does not support Microsoft Exchange 2003 or Microsoft authentication protocol NTLMv2 Session.

The following table describes the protocol-specific parameters for the Microsoft Exchange protocol:

Table 14. Microsoft Exchange protocol parameters

Parameter	Description
Protocol Configuration	**Microsoft Exchange**
Domain	Optional.
SMTP Log Folder Path	When the folder path is clear, SMTP event collection is disabled.
OWA Log Folder Path	When the folder path is clear, OWA event collection is disabled.
MSGTRK Log Folder Path	Message tracking is available on Microsoft Exchange 2007 or 2010 servers assigned the Hub Transport, Mailbox, or Edge Transport server role.
File Pattern	The regular expression (regex) that identifies the event logs. The default is `.*\.(?:log|LOG)`.
Force File Read	If the check box is cleared, the log file is read only when QRadar detects a change in the modified time or file size.
Throttle Events/Second	The maximum number of events the Exchange protocol can forward per second.

Microsoft IIS protocol configuration options

You can configure a log source to use the Microsoft IIS protocol. This protocol supports a single point of collection for W3C format log files that are located on a Microsoft IIS web server.

To read the log files, folder paths that contain an administrative share (C$), require NetBIOS privileges on the administrative share (C$). Local or domain administrators have sufficient privileges to access log files on administrative shares.

Fields for the Microsoft IIS protocol that support file paths allow administrators to define a drive letter with the path information. For example, the field can contain

the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/`directory for a public share folder path, but cannot contain the `c:/LogFiles` directory.

Restriction: The Microsoft authentication protocol NTLMv2 is not supported by the Microsoft IIS protocol.

The following table describes the protocol-specific parameters for the Microsoft IIS protocol:

Table 15. Microsoft IIS protocol parameters

Parameter	Description
Protocol Configuration	**Microsoft IIS**
File Pattern	The regular expression (regex) that identifies the event logs.
Throttle Events/Second	The maximum number of events the IIS protocol can forward per second.

SMB Tail protocol configuration options

You can configure a log source to use the SMB Tail protocol. Use this protocol to watch events on a remote Samba share and receive events from the Samba share when new lines are added to the event log.

The following table describes the protocol-specific parameters for the SMB Tail protocol:

Table 16. SMB Tail protocol parameters

Parameter	Description
Protocol Configuration	**SMB Tail**
Log Folder Path	The directory path to access the log files. For example, administrators can use the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/` directory for a public share folder path. However, the `c:/LogFiles` directory is not a supported log folder path.
	If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the privileges that are required to read the log files.
	Local system or domain administrator privileges are also sufficient to access a log files that are on an administrative share.
File Pattern	The regular expression (regex) that identifies the event logs.
Force File Read	If the check box is cleared, the log file is read only when QRadar detects a change in the modified time or file size.
Throttle Events/Second	The maximum number of events the SMB Tail protocol forwards per second.

EMC VMware protocol configuration options

To receive event data from the VMWare web service for virtual environments, configure a log source to use the EMC VMWare protocol.

The following table describes the protocol-specific parameters for the EMC VMware protocol:

Table 17. EMC VMware protocol parameters

Parameter	Description
Protocol Configuration	**EMC VMware**
Log Source Identifier	The value for this parameter must match the **VMware IP** parameter.
VMware IP	The IP address of the VMWare ESXi server, for example, 1.1.1.1. The VMware protocol appends the IP address of your VMware ESXi server with HTTPS before the protocol requests event data.

Oracle Database Listener protocol configuration options

To remotely collect log files that are generated from an Oracle database server, configure a log source to use the Oracle Database Listener protocol source.

Before you configure the Oracle Database Listener protocol to monitor log files for processing, you must obtain the directory path to the Oracle database log files.

The following table describes the protocol-specific parameters for the Oracle Database Listener protocol:

Table 18. Oracle Database Listener protocol parameters

Parameter	Description
Protocol Configuration	**Oracle Database Listener**
File Pattern	The regular expression (regex) that identifies the event logs.

Cisco NSEL protocol configuration options

To monitor NetFlow packet flows from a Cisco Adaptive Security Appliance (ASA), configure the Cisco Network Security Event Logging (NSEL) protocol source.

To integrate Cisco NSEL with QRadar, you must manually create a log source to receive NetFlow events. QRadar does not automatically discover or create log sources for syslog events from Cisco NSEL. For more information, see the *DSM Configuration Guide*.

The following table describes the protocol-specific parameters for the Cisco NSEL protocol:

Table 19. Cisco NSEL protocol parameters

Parameter	Description
Protocol Configuration	**Cisco NSEL**
Log Source Identifier	If the network contains devices that are attached to a management console, you can specify the IP address of the individual device that created the event. A unique identifier for each, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.
Collector Port	The UDP port number that Cisco ASA uses to forward NSEL events. QRadar uses port 2055 for flow data on QRadar QFlow Collectors. You must assign a different UDP port on the Cisco Adaptive Security Appliance for NetFlow.

PCAP Syslog Combination protocol configuration options

To collect events from Juniper Networks SRX Series appliances that forward packet capture (PCAP) data, configure a log source to use the PCAP Syslog Combination protocol .

Before you configure a log source that uses the PCAP Syslog Combination protocol, determine the outgoing PCAP port that is configured on the Juniper Networks SRX appliance. PCAP data cannot be forwarded to port 514.

The following table describes the protocol-specific parameters for the PCAP Syslog Combination protocol:

Table 20. PCAP Syslog Combination protocol parameters

Parameter	Description
Protocol Configuration	**PCAP Syslog Combination**
Incoming PCAP Port	If the outgoing PCAP port is edited on the Juniper Networks SRX Series appliance, you must edit the log source to update the incoming PCAP Port. After you edit the **Incoming PCAP Port** field, you must deploy your changes.

Forwarded protocol configuration options

To receive events from another Console in your deployment, configure a log source to use the Forwarded protocol.

The Forwarded protocol is typically used to forward events to another QRadar Console. For example, Console A has Console B configured as an off-site target. Data from automatically discovered log sources is forwarded to Console B. Manually created log sources on Console A must also be added as a log source to Console B with the forwarded protocol.

TLS syslog protocol configuration options

To receive encrypted syslog events from up to 50 network devices that support TLS Syslog event forwarding, configure a log source to use the TLS Syslog protocol.

The log source creates a listen port for incoming TLS Syslog events and generates a certificate file for the network devices. Up to 50 network appliances can forward events to the listen port that is created for the log source. If you require more than 50 network appliances, create additional listen ports.

The following table describes the protocol-specific parameters for the TLS Syslog protocol:

Table 21. TLS syslog protocol parameters

Parameter	Description
Protocol Configuration	**TLS Syslog**
TLS Listen Port	The default TLS listen port is 6514.

Table 21. TLS syslog protocol parameters (continued)

Parameter	Description
Authentication Mode	The mode by which your TLS connection is authenticated. If you select the **TLS and Client Authentication** option, you must configure the certificate parameters.
Client Certificate Path	The absolute path to the client-certificate on disk. The certificate must be stored on the Console or Event Collector for this log source.
Certificate Type	The type of certificate to use for authentication. If you select the **Provide Certificate** option, you must configure the file paths for the server certificate and the private key.
Provided Server Certificate Path	The absolute path to the server certificate.
Provided Private Key Path	The absolute path to the private key. **Note:** The corresponding private key must be a DER-encoded PKCS8 key. The configuration fails with any other key format.

TLS syslog use cases

The following use cases represent possible configurations that you can create:

Client Authentication
> You can supply a client-certificate that enables the protocol to engage in client-authentication. If you select this option and provide the certificate, incoming connections are validated against the client-certificate.

User-provided Server Certificates
> You can configure your own server certificate and corresponding private key. The configured TLS Syslog provider uses the certificate and key. Incoming connections are presented with the user-supplied certificate, rather than the automatically generated TLS Syslog certificate.

Default authentication
> To use the default authentication method, use the default values for the **Authentication Mode** and **Certificate Type** parameters. After the log source is saved, a `syslog-tls` certificate is created for log source device. The certificate must be copied to any device on your network that forwards encrypted syslog data.

Juniper Security Binary Log Collector protocol configuration options

You can configure a log source to use the Security Binary Log Collector protocol. With this protocol, Juniper appliances can send audit, system, firewall, and intrusion prevention system (IPS) events in binary format to QRadar.

The binary log format from Juniper SRX or J Series appliances are streamed by using the UDP protocol. You must specify a unique port for streaming binary formatted events. The standard syslog port 514 cannot be used for binary formatted events. The default port that is assigned to receive streaming binary events from Juniper appliances is port 40798.

The following table describes the protocol-specific parameters for the Juniper Security Binary Log Collector protocol:

Table 22. Juniper Security Binary Log Collector protocol parameters

Parameter	Description
Protocol Configuration	**Security Binary Log Collector**
XML Template File Location	The path to the XML file used to decode the binary stream from your Juniper SRX or Juniper J Series appliance. By default, the device support module (DSM) includes an XML file for decoding the binary stream. The XML file is in the following directory: `/opt/qradar/conf/security_log.xml`.

UDP multiline syslog protocol configuration options

To create a single-line syslog event from a multiline event, configure a log source to use the UDP multiline protocol. The UDP multiline syslog protocol uses a regular expression to identify and reassemble the multiline syslog messages into single event payload.

The original event must contain a value that repeats a regular expression that can identify and reassemble the multiline event. For example, this event contains a repeated value:

```
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"
```

The following table describes the protocol-specific parameters for the UDP multiline syslog protocol:

Table 23. UDP multiline syslog protocol parameters

Parameter	Description
Protocol Configuration	**UDP Multiline Syslog**
Message ID Pattern	The regular expression (regex) required to filter the event payload messages. The UDP multiline event messages must contain a common identifying value that repeats on each line of the event message.

After the log source is saved, a syslog-tls certificate is created for the log source. The certificate must be copied to any device on your network that is configured to forward encrypted syslog. Other network devices that have a syslog-tls certificate file and the TLS listen port number can be automatically discovered as a TLS syslog log source.

TCP multiline syslog protocol configuration options

You can configure a log source that uses the TCP multiline syslog protocol. To create a single-line event, this protocol uses regular expressions to identify the start and end pattern of multiline events.

The following example is a multiline event:

```
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
```

The following table describes the protocol-specific parameters for the TCP multiline syslog protocol:

Table 24. TCP multiline syslog protocol parameters

Parameter	Description
Protocol Configuration	**TCP Multiline Syslog**
Listen Port	The default listen port is 12468.
Event Formatter	Use the **Windows Multiline** option for multiline events that are formatted specifically for Windows.
Event Start Pattern	The regular expression (regex) that is required to identify the start of a TCP multiline event payload. Syslog headers typically begin with a date or time stamp. The protocol can create a single-line event that is based on solely an event start pattern, such as a time stamp. When only a start pattern is available, the protocol captures all the information between each start value to create a valid event.
Event End Pattern	The regular expression (regex) that is required to identify the last field of a TCP multiline event payload. If the syslog event ends with the same value, you can use a regular expression to determine the end of an event. The protocol can capture events that are based on solely on an event end pattern. When only an end pattern is available, the protocol captures all the information between end start value to create a valid event.

VMware vCloud Director protocol configuration options

To collect events from the VMware vCloud Director virtual environments, you can create a log source that uses the VMware vCloud Director protocol.

The following table describes the protocol-specific parameters for the VMware vCloud Director protocol:

Table 25. VMware vCloud Director protocol parameters

Parameter	Description
Protocol Configuration	**VMware vCloud Director**
vCloud URL	The URL that is configured on the VMware vCloud appliance to access the REST API. The URL must match the address that is configured as the VCD public REST API base URL on the vCloud Server, for example, `https://1.1.1.1.`.

Table 25. VMware vCloud Director protocol parameters (continued)

Parameter	Description
User Name	The user name that is required to remotely access the vCloud Server, for example, `console/user@organization`. To configure a read-only account to use with the vCloud Director protocol, a user must have Console Access Only permission.

IBM Tivoli Endpoint Manager SOAP protocol configuration options

To receive Log Extended Event Format (LEEF) formatted events from IBM Tivoli® Endpoint Manager appliances, configure a log source that uses the IBM Tivoli Endpoint Manager SOAP protocol.

This protocol requires IBM Tivoli Endpoint Manager versions V8.2.x or later and the Web Reports application for Tivoli Endpoint Manager.

The Tivoli Endpoint Manager SOAP protocol retrieves events in 30-second intervals over HTTP or HTTPS. As events are retrieved, the IBM Tivoli Endpoint Manager DSM parses and categorizes the events.

The following table describes the protocol-specific parameters for the IBM Tivoli Endpoint Manager SOAP protocol:

Table 26. IBM Tivoli Endpoint Manager SOAP protocol parameters

Parameter	Description
Protocol Configuration	**IBM Tivoli Endpoint Manager SOAP**
Use HTTPS	If a certificate is required to connect with HTTPS, copy the required certificates to the following directory: `/opt/qradar/conf/trusted_certificates`. Certificates that have following file extensions: `.crt`, `.cert`, or `.der` are supported. Copy the certificates to the trusted certificates directory before the log source is saved and deployed.
SOAP Port	By default, port 80 is the port number for communicating with IBM Tivoli Endpoint Manager. Most configurations use port 443 for HTTPS communications.

Syslog Redirect protocol overview

The Syslog Redirect protocol is used as an alternative to the Syslog protocol. Use this protocol when you want to QRadar identify the specific device name that sent the events. QRadar can passively listen for Syslog events on UDP port 517.

The following table describes the protocol-specific parameters for the Syslog Redirect protocol:

Table 27. Syslog Redirect protocol parameters

Parameter	Description
Protocol Configuration	**Syslog Redirect**
Log Source Identifier RegEx	`devname=([\w-]+)`
Listen Port	517

Table 27. Syslog Redirect protocol parameters (continued)

Parameter	Description
Protocol	**UDP**

Adding bulk log sources

You can add up to 500 Microsoft Windows or Universal DSM log sources at one time. When you add multiple log sources at one time, you add a bulk log source in QRadar. Bulk log sources must share a common configuration.

Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. From the **Actions** list, select **Bulk Add**.
4. Configure the parameters for the bulk log source.
5. Click **Save**.
6. Click **Continue** to add the log sources.
7. On the **Admin** tab, click **Deploy Changes**.

Adding a log source parsing order

You can assign a priority order for when the events are parsed by the target event collector.

About this task

You can order the importance of the log sources by defining the parsing order for log sources that share a common IP address or host name. Defining the parsing order for log sources ensures that certain log sources are parsed in a specific order, regardless of changes to the log source configuration. The parsing order ensures that system performance is not affected by changes to log source configuration by preventing unnecessary parsing. The parsing order ensures that low-level event sources are not parsed for events before more important log source.

Procedure

1. Click the **Admin** tab.
2. Click the **Log Source Parsing Ordering** icon.
3. Select a log source.
4. Optional: From the **Selected Event Collector** list, select the Event Collector to define the log source parsing order.
5. Optional: From the **Log Source Host** list, select a log source.
6. Prioritize the log source parsing order.
7. Click **Save**.

Chapter 2. Log source extension management

You can create log source extensions to extend or modify the parsing routines of specific devices.

A *log source extension* is an XML file that includes all of the regular expression patterns that are required to identify and categorize events from the event payload. Extension files can be used to parse events when you must correct a parsing issue or you must override the default parsing for an event from a DSM. When a DSM does not exist to parse events for an appliance or security device in your network, an extension can provide event support. The **Log Activity** tab identifies log source events in these basic types:

- Log sources that properly parse the event. Properly parsed events are assigned to the correct log source type and category. In this case, no intervention or extension is required.

- Log sources that parse events, but have a value **Unknown** in the **Log Source** parameter. Unknown events are log source events where the log source type is identified, but the payload information cannot be understood by the DSM. The system cannot determine an event identifier from the available information to properly categorize the event. In this case, the event can be mapped to a category or a log source extension can be written to repair the event parsing for unknown events.

- Log sources that cannot identify the log source type and have a value of **Stored** event in the **Log Source** parameter. Stored events require you to update your DSM files or write a log source extension to properly parse the event. After the event parses, you can then map the events.

Before you can add a log source extension, you must create the extension document. The extension document is an XML document that you can create with any common word processing or text editing application. Multiple extension documents can be created, uploaded, and associated with various log source types. The format of the extension document must conform to a standard XML schema document (XSD). To develop an extension document, knowledge of and experience with XML coding is required.

Adding a log source extension

You can add a log source extension to extend or modify the parsing routines of specific devices.

Procedure
1. Click the **Admin** tab.
2. Click the **Log Source Extensions** icon.
3. Click **Add**.
4. From the **Use Condition** list, select one of the following options:

Option	Description
Parsing Enhancement	Select this option when the device support module (DSM) correctly parses most fields for the log source. The incorrectly parsed field values are enhanced with the new XML values.
Parsing Override	Select this option when the device support module (DSM) is unable to parse correctly. The log source extension completely overrides the failed parsing by the DSM and substitutes the parsing with the new XML values.

5. From the **Log Source Types** list, select one of the following options:

Option	Description
Available	Select this option when the device support module (DSM) correctly parses most fields for the log source. The incorrectly parsed field values are enhanced with the new XML values.
Set to default for	Select log sources to add or remove from the extension parsing. You can add or remove extensions from a log source.
	When a log source extension is **Set to default for** a log source, new log sources of the same **Log Source Type** use the assigned log source extension.

6. Click **Browse** to locate your log source extension XML document.
7. Click **Upload**. The contents of the log source extension is displayed to ensure that the proper extension file is uploaded. The extension file is evaluated against the XSD for errors when the file is uploaded.
8. Click **Save**.

Results

If the extension file does not contain any errors, the new log source extension is created and enabled. It is possible to upload a log source extension without applying the extension to a log source. Any change to the status of an extension is applied immediately and managed hosts or Consoles enforce the new event parsing parameters in the log source extension.

What to do next

On the **Log Activity** tab, verify that the parsing patterns for events is applied correctly. If the log source categorizes events as **Stored**, the parsing pattern in the log source extension requires adjustment. You can review the extension file against log source events to locate any event parsing issues.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols

indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the

section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Index

B
bulk add   21

C
Cisco NSEL   15

E
EMC VMware protocol   14

F
forwarded protocol   16

I
IBM Proventia® Management
   SiteProtector®   4
IBM Tivoli Endpoint Manager
   protocol   20
introduction   v

J
JDBC protocol   3
JDBC SiteProtector protocol   4
Juniper Networks NSM protocol   7
Juniper Security Binary Log Collector
   protocol   17

L
log file protocol   10
log source
      status   1
log source extension
      disable extension   23
      enable extension   23
log source extensions   23
log sources   1

M
manage   23
Microsoft DHCP protocol   12
Microsoft Exchange protocol   13
Microsoft IIS protocol   13
Microsoft Security Event Log
   protocol   11

N
network administrator   v

O
OPSEC/LEA protocol   7
Oracle Database Listener protocol   15

overview   1

P
parsing order   21
PCAP Syslog Combination protocol   16

S
SDEE protocol   8
SMB Tail protocol   14
SNMPv2 protocol   8, 9
Sophos Enterprise Console JDBC
   protocol   6
Syslog Redirect protocol   20

T
TCP multiline syslog protocol   18
TLS syslog protocol   16

U
UDP multiline syslog protocol   18

V
vCloud Director protocol   19