IBM Security QRadar

DSM Configuration Guide Addendum

7.1.x and 7.2.x

IBM Security QRadar

DSM Configuration Guide Addendum

7.1.x and 7.2.x

Note

Before using this information and the product that it supports, read the information in "Notices" on page 215.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.4 and subsequent releases unless superseded by an updated version of this document.

Contents

About this DSM Configuration Guide Addendum

The *DSM Configuration Guide Addendum* provides instructions about how to collect data from your third-party devices, also known as *log sources*. The addendum includes information only for Device Support Module (DSM) integrations that were introduced or upgraded after IBM® Security QRadar® V7.2.2 was released and are supported by QRadar 7.1 and later. For information about previous DSMs, see the *DSM Configuration Guide*.

Intended audience

System administrators who are responsible for installing DSMs must be familiar with network security concepts and device configurations.

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. Event collection from third-party devices

To configure event collection from third-party devices, you need to complete configuration tasks on the third-party device, and your QRadar Console, Event Collector, or Event Processor. The key components that work together to collect events from third-party devices are log sources, DSMs, and automatic updates.

Log sources

A *log source* is any external device, system, or cloud service that is configured to either send events to your IBM Security QRadar system or be collected by your QRadar system. QRadar shows events from log sources in the **Log Activity** tab.

To receive raw events from log sources, QRadar supports several protocols, including syslog from OS, applications, firewalls, IPS/IDS, SNMP, SOAP, JDBC for data from database tables and views. QRadar also supports proprietary vendor-specific protocols such as OPSEC/LEA from Checkpoint.

For more information about supported protocols, see the *Log Sources User Guide*.

DSMs

A *Device Support Module (DSM)* is a configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output. Each type of log source has a corresponding DSM. For example, the IBM Fiberlink MaaS360 DSM parses and normalizes events from an IBM Fiberlink MaaS360 log source.

Automatic Updates

QRadar provides daily and weekly automatic updates on a recurring schedule. The weekly automatic update includes new DSM releases, corrections to parsing issues, and protocol updates. For more information about managing automatic updates, see the *IBM Security QRadar SIEM Administration Guide*.

Third-party device installation process

To collect events from third-party device, you must complete installation and configuration steps on both the log source device and your QRadar system. For some third-party devices, extra configuration steps are needed, such as configuring a certificate to enable communication between that device and QRadar.

The following steps represent a typical installation process:

1. Read the specific instructions for how to integrate your third-party device.
2. Download and install the RPM for your third-party device. RPMs are available for download from the IBM support website (http://www.ibm.com/support).

   Tip: If your QRadar system is configured to accept automatic updates, this step might not be required.
3. Configure the third-party device to send events to QRadar.

After some events are received, QRadar automatically detects some third-party devices and creates a log source configuration. The log source is listed on the Log Sources list and contains default information. You can customize the information.

4. If QRadar does not automatically detect the log source, manually add a log source. The list of supported DSMs and the device-specific topics indicate which third-party devices are not automatically detected.
5. Deploy the configuration changes and restart your web services.

Universal DSMs for unsupported third-party log sources

After the events are collected and before the correlation can begin, individual events from your devices must be properly normalized. *Normalization* means to map information to common field names, such as event name, IP addresses, protocol, and ports. If an enterprise network has one or more network or security devices that QRadar does not provide a corresponding DSM, you can use the Universal DSM. QRadar can integrate with most devices and any common protocol sources by using the *Universal DSM*.

To configure the Universal DSM, you must use device extensions to associate a Universal DSM to devices. Before you define device extension information in the Log Sources window in the **Admin** tab, you must create an extensions document for the log source. For more information, see the *Log Sources User Guide*.

For more information about Universal DSMs, see the IBM support website (http://www.ibm.com/support).

Adding a single DSM

If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

Restriction: Uninstalling a Device Support Module (DSM) is not supported in QRadar.

Procedure

1. Download the DSM RPM file from the IBM support website (http://www.ibm.com/support).
2. Copy the RPM file to your QRadar Console.
3. Using SSH, log in to the QRadar host as the root user.
4. Navigate to the directory that includes the downloaded file.
5. Type the following command:
   ```
   rpm -Uvh <rpm_filename>
   ```
6. Log in to the QRadar user interface.
7. On the **Admin** tab, click **Deploy Changes**.
8. On the **Admin** tab, selected **Advanced > Restart Web Services**.

Related concepts:

Chapter 2, “3Com Switch 8800,” on page 7
The IBM Security QRadar DSM for 3Com Switch 8800 receives events by using syslog.

Installing a DSM bundle

You can download and install a DSM bundle that is updated daily to include the most recent DSM releases and updates.

Procedure

1. Download the DSM bundle from the IBM support website (http://www.ibm.com/support).
2. Copy the bundle to your QRadar Console.
3. Using SSH, log in to the QRadar host as the root user.
4. Navigate to the directory that includes the downloaded file.
5. Type the following command to extract the contents of the bundle:

   ```
   tar -zxvf QRadar_bundled-DSM-your_qradar_version.tar.gz
   ```
6. Type the following command:

   ```
   for FILE in *Common*.rpm DSM-*.rpm; do rpm -Uvh "$FILE"; done
   ```
7. Log in to the QRadar user interface.
8. On the **Admin** tab, click **Deploy Changes**.
9. On the **Admin** tab, selected **Advanced > Restart Web Services**.

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.
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.

Table 1. Log source parameters (continued)

Parameter	Description
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**.

Related concepts:

Chapter 2, “3Com Switch 8800,” on page 7
The IBM Security QRadar DSM for 3Com Switch 8800 receives events by using syslog.

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 **Bulk Actions** list, select **Bulk Add**.
4. Configure the parameters for the bulk log source.
   - File Upload - Upload a text file that has one host name or IP per line
   - Manual - Enter the host name or IP of the host that you wish to add
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. 3Com Switch 8800

The IBM Security QRadar DSM for 3Com Switch 8800 receives events by using syslog.

The following table identifies the specifications for the 3Com Switch 8800 DSM:

Specification	Value
Manufacturer	3Com
DSM name	Switch 8800 Series
RPM file name	`DSM-3ComSwitch_`*`qradar-version_build-number`*`.noarch.rpm`
Supported versions	v3.01.30
Protocol	Syslog
QRadar recorded events	Status and network condition events
Automatically discovered?	Yes
Includes identity?	No
Includes custom event properties?	No
More information	3Com website (http://www.3com.com)

To send 3COM Switch 8800 events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent 3COM Switch 8800 RPM on your QRadar Console.
2. Configure each 3COM Switch 8800 instance to communicate with QRadar.
3. If QRadar does not automatically discover the DSM, create a log source on the QRadar Console for each 3COM Switch 8800 instance. Configure all the required parameters, and use the following table for specific values:

Parameter	Description
Log Source Type	3COM Switch 8800
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring your 3COM Switch 8800"
Configure your 3COM Switch 8800 to forward syslog events to IBM Security QRadar.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your 3COM Switch 8800

Configure your 3COM Switch 8800 to forward syslog events to IBM Security QRadar.

Procedure

1. Log in to 3COM Switch 8800.
2. To enable the information center, type the following command:

   ```
   info-center enable
   ```
3. To configure the log host, type the following command:

   ```
   info-center loghost QRadar_ip_address facility informational language english
   ```
4. To configure the ARP and IP information modules, type the following commands.

   ```
   info-center source arp channel loghost log level informational
   info-center source ip channel loghost log level informational
   ```

Chapter 3. AccessData InSight

The AccessData InSight DSM for IBM Security QRadar collects event logs from your AccessData InSight device.

The following table identifies the specifications for the AccessData InSight DSM:

Table 2. AccessData InSight DSM specifications

Specification	Value
Manufacturer	AccessData
DSM name	AccessData InSight
RPM file name	`DSM-AccessDataInSight-`*`build_number`*`.noarch.rpm`
Supported versions	V2
Event format	Log file
QRadar recorded event types	Volatile Data Memory Analysis Data Memory Acquisition Data Collection Data Software Inventory Process Dump Data Threat Scan Data Agent Remediation Data
Automatically discovered?	No
Included identity?	No
More information	AccessData website (http://www.accessdata.com/)

To send events from AccessData InSight to QRadar, use the following steps:

1. If automatic updates are not enabled, download the most recent versions of the following RPMs.
   - LogFileProtocol
   - DSMCommon
   - AccessData InSight DSM
2. Configure your AccessData InSight device to communicate with QRadar.
3. Create an AccessData InSight log source on the QRadar Console.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring your AccessData InSight device to communicate with QRadar"
To collect AccessData InSight events, you must configure your third-party device to generate event logs in LEEF format. You must also create an FTP site for AccessData InSight to transfer the LEEF files. QRadar can then pull the logs from the FTP server.

"Adding an AccessData InSight log source on your QRadar Console"
QRadar does not automatically discover the AccessData InSight log source. You must manually add the log source.

Configuring your AccessData InSight device to communicate with QRadar

To collect AccessData InSight events, you must configure your third-party device to generate event logs in LEEF format. You must also create an FTP site for AccessData InSight to transfer the LEEF files. QRadar can then pull the logs from the FTP server.

Procedure

1. Log in to your AccessData InSight device.
2. Open the `ADGIntegrationServiceHost.exe.config` file, which is in the `C:\Program Files\AccessData\eDiscovery\Integration Services` directory.
3. Change the text in the file to match the following lines:

   ```
   <Option Name="Version" Value="2.0" />
   <Option Name="Version" Value="2.0" />
   <Option Name="OutputFormat" Value="LEEF" />
   <Option Name="LogOnly" Value="1" />
   <Option Name="OutputPath" Value="C:\CIRT\logs" />
   ```
4. Restart the AccessData Third-Party Integration service.
5. Create an FTP site for the `C:\CIRT\logs` output folder:
   a. Open Internet Information Services Manager (IIS).
   b. Right-click the **Sites** tab and click **Add FTP Site**.
   c. Name the FTP site, and enter `C:\CIRT\logs` as the location for the generated LEEF files.
   d. Restart the web service.

Adding an AccessData InSight log source on your QRadar Console

QRadar does not automatically discover the AccessData InSight log source. You must manually add the log source.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. In the **Log Source Identifier** field, type the IP address or host name of the AccessData InSight device.
7. From the **Log Source Type** list, select **AccessData InSight**.
8. From the **Protocol Configuration** list, select **Log File**.

9. Configure the remaining parameters.
10. Click **Save**.

Chapter 4. AhnLab Policy Center

The IBM Security QRadar DSM for AhnLab Policy Center retrieves events from the DB2 database that AhnLab Policy Center uses to store their log.

The following table identifies the specifications for the AhnLab Policy Center DSM:

Table 3. AhnLab Policy Center DSM specifications

Specification	Value
Manufacturer	AhnLab
DSM	AhnLab Policy Center
RPM file names	`DSM-AhnLabPolicyCenter-`*`QRadar-Release_Build-Number`*`.noarch.rpm`
Supported versions	4.0
Protocol	AhnLabPolicyCenterJdbc
QRadar recorded events	Spyware detection, Virus detection, Audit
Automatically discovered?	No
Includes identity	Yes
More information	Ahnlab website (https://global.ahnlab.com/)

To integrate AhnLab Policy Center DSM with QRadar, complete the following steps:

1. Download and install the most recent versions of the following RPMs on your QRadar Console:
   - JDBC protocol RPM
   - AhnLabPolicyCenterJdbc protocol RPM
   - AhnLab Policy Center RPM

   Tip: For more information, see your DB2 documentation.
2. Ensure that your AhnLab Policy Center system meets the following criteria:
   - The DB2 Database allows connections from QRadar.
   - The port for AhnLabPolicyCenterJdbc Protocol matches the listener port of the DB2 Database.
   - Incoming TCP connections on the DB2 Database are enabled to communicate with QRadar.
3. For each AhnLab Policy Center server you want to integrate, create a log source on the QRadar Console. The following table identifies Ahnlab-specific protocol values:

Parameter	Value
Log Source Type	AhnLab Policy Center APC
Protocol Configuration	AhnLabPolicyCenterJdbc
Access credentials	Use the access credentials of the DB2 server.

Parameter	Value
Log Source Language	If you use QRadar v7.2 or later, you must select a log source language.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Chapter 5. Amazon AWS CloudTrail

The IBM Security QRadar DSM for Amazon AWS CloudTrail collects audit events from your Amazon AWS CloudTrail S3 bucket.

The following table lists the specifications for the Amazon AWS CloudTrail DSM:

Table 4. Amazon AWS CloudTrail DSM specifications

Specification	Value
Manufacturer	Amazon
DSM	Amazon AWS CloudTrail
RPM name	`DSM-AmazonAWSCloudTrail-`*`QRadar_version-Build_number`*`.noarch.rpm`
Supported versions	1.0
Protocol	Amazon AWS S3
QRadar recorded events	All events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Amazon Cloud Trail documentation (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/whatisawscloudtrail.html)

To integrate Amazon AWS CloudTrail with QRadar, complete the following steps:

1. Obtain and install a certificate to enable QRadar to communicate with the Amazon AWS CloudTrail S3 bucket.
2. Install the most recent version of the following RPMs on your QRadar Console or Event Collector.
   - Amazon REST API Protocol RPM
   - Amazon AWS CloudTrail DSM RPM
3. Configure the Amazon AWS CloudTrail log source in QRadar. Configure all required parameters and use the following table to help you determine values for Amazon AWS CloudTrail parameters:

Table 5. Amazon AWS CloudTrail log source parameters

Parameter	Description
Log Source Type	**Amazon AWS CloudTrail**
Protocol Configuration	**Amazon AWS S3**
Bucket Name	The name of the AWS CloudTrail S3 bucket where the log files are stored.
Public Key	The public access key that is required to access the AWS CloudTrail S3 bucket.
Access Key	The private access key that is required to access the AWS CloudTrail S3 bucket.

Table 5. Amazon AWS CloudTrail log source parameters (continued)

Parameter	Description
Use Proxy	When a proxy is configured, all traffic for the log source travels through the proxy for QRadar to access the Amazon AWS S3 buckets. Configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Directory Prefix	The root directory location on the AWS CloudTrail S3 bucket from which the files are retrieved, for example, `\user_account_name`
Recurrence	How often the Log File Protocol connects to the Amazon cloud API, checks for new files, and retrieves them if they exist. Every access to an AWS S3 bucket incurs a cost to the account that owns the bucket. Therefore, a smaller recurrence value increases the cost.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Chapter 6. Ambiron TrustWave ipAngel

The IBM Security QRadar DSM for Ambiron TrustWave ipAngel receives Snort-based events from the ipAngel console.

The following table identifies the specifications for the Ambiron TrustWave ipAngel DSM:

Table 6. Ambiron TrustWave ipAngel DSM specifications

Specification	Value
Manufacturer	Ambiron
DSM name	Ambiron TrustWave ipAngel

RPM file name	`DSM-AmbironTrustwaveIpAngel-`
	`Qradar_version-build_number``.noarch.rpm`

Supported versions	V4.0
Protocol	Syslog
Recorded event types	Snort-based events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Ambiron website (http://www.apache.org)

To send Ambiron TrustWave ipAngel events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Ambiron TrustWave ipAngel DSM RPM on your QRadar Console.
2. Configure your Ambiron TrustWave ipAngel device to forward your cache and access logs to QRadar. For information on forwarding device logs to QRadar, see your vendor documentation.
3. Add an Ambiron TrustWave ipAngel log source on the QRadar Console. The following table describes the parameters that require specific values that are required for Ambiron TrustWave ipAngel event collection:

Table 7. Ambiron TrustWave ipAngel log source parameters

Parameter	Value
Log Source type	Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Chapter 7. Arbor Networks Pravail

The IBM Security QRadar DSM for Arbor Networks Pravail receives event logs from your Arbor Networks Pravail servers.

The following table identifies the specifications for the Arbor Networks Pravail DSM:

Table 8. Arbor Networks Pravail DSM specifications

Specification	**Value**
Manufacturer	Arbor Networks
DSM	Arbor Networks Pravail
RPM file name	`DSM-ArborNetworksPravail-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	v3.1 and later
Protocol	Syslog
Recorded events	All relevant events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Arbor Networks website (www.arbornetworks.com)

To send Arbor Networks Pravail DSM events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent Arbor Networks Pravail DSM RPM on your QRadar Console.
2. Configure each Arbor Networks Pravail system to send events to QRadar.
3. If QRadar does not automatically discover the Arbor Networks Pravail system, create a log source on the QRadar Console. Configure the required parameters, and use the following table for the Arbor Networks Pravail specific parameters:

Parameter	**Value**
Log Source Type	Arbor Networks Pravail
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring your Arbor Networks Pravail system to send events to QRadar" on page 20
To collect all audit logs and system events from Arbor Networks Pravail, you must add a destination that specifies IBM Security QRadar as the syslog server.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your Arbor Networks Pravail system to send events to QRadar

To collect all audit logs and system events from Arbor Networks Pravail, you must add a destination that specifies IBM Security QRadar as the syslog server.

Procedure

1. Log in to your Arbor Networks Pravail server.
2. Click **Settings & Reports**.
3. Click **Administration > Notifications**.
4. On the Configure Notifications page, click **Add Destinations.**
5. Select **Syslog**.
6. Configure the following parameters:

Parameter	Description
Host	The IP address of the QRadar Console.
Port	**514**
Severity	**Info**
Alert Types	The alert types that you want to send to the QRadar Console.

7. Click **Save**.

Chapter 8. APC UPS

The IBM Security QRadar DSM for APC UPS accepts syslog events from the APC Smart-Uninterruptible Power Supply (UPS) family of products.

Restriction: Events from RC-Series Smart-UPS are not supported.

The following table identifies the specifications for the APC UPS DSM:

Table 9. APC UPS DSM specifications

Specification	Value
Manufacturer	APC
DSM name	APC UPS
RPM file name	`DSM-APCUPS-`*`Qradar_version-build_number`*`.noarch.rpm`
Protocol	Syslog
Recorded event types	UPS events Battery events Bypass events Communication events Input power events Low battery condition events SmartBoost events SmartTrim events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	APC website (http://www.apc.com)

To send APC UPS events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the APC UPS DSM RPM on your QRadar Console.
2. Create an APC UPS log source on the QRadar Console. Configure all the required parameters, and use the following table to configure the specific values that are requiredto collect APC UPS events:

Table 10. APC UPS log source parameters

Parameter	Value
Log Source type	APC UPS
Protocol Configuration	Syslog

3. Configure your APC UPS device to forward syslog events to QRadar.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

"Configuring your APC UPS to forward syslog events"
To collect events from your APC UPS, you must configure the device to forward syslog events to IBM Security QRadar.

Configuring your APC UPS to forward syslog events

To collect events from your APC UPS, you must configure the device to forward syslog events to IBM Security QRadar.

Procedure

1. Log in to the APC Smart-UPS web interface.
2. In the navigation menu, click **Network > Syslog**.
3. From the **Syslog** list, select **Enable**.
4. From the **Facility** list, select a facility level for your syslog messages.
5. In the **Syslog Server** field, type the IP address of your QRadar Console or Event Collector.
6. From the **Severity** list, select **Informational**.
7. Click **Apply**.

Chapter 9. Barracuda Web Application Firewall

The IBM Security QRadar DSM for Barracuda Web Application Firewall collects syslog LEEF and custom events from Barracuda Web Application Firewall devices.

The following table identifies the specifications for the Barracuda Web Application Firewall DSM:

Table 11. Barracuda Web Application Firewall DSM specifications

Specification	**Value**
Manufacturer	Barracuda
DSM name	Web Application Firewall
RPM file name	DSM-BarracudaWebApplicationFirewall-*QRadar_version-build_number*.noarch.rpm
Supported versions	V7.0.x and later
Protocol type	Syslog
QRadar recorded event types	System Web Access Audit
Automatically discovered?	If LEEF-formatted payloads, the log source is automatically discovered. If custom-formatted payloads, the log source is not automatically discovered.
Included identity?	Yes
More information	Barracuda Networks website (https://www.barracudanetworks.com)

To collect syslog events from Barracuda Web Application Firewall, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs on your QRadar Console:
   - Barracuda Web Application Firewall DSM RPM
   - DSMCommon RPM
2. Configure your Barracuda Web Application Firewall device to send syslog events to QRadar.
3. Add a Barracuda Web Application Firewall log source on the QRadar Console. The following table describes the parameters that require specific values that are required for Barracuda Web Application Firewall event collection:

Table 12. Barracuda Web Application Firewall log source parameters

Parameter	**Value**
Log Source type	Barracuda Web Application Firewall

Table 12. Barracuda Web Application Firewall log source parameters (continued)

Parameter	Value
Protocol Configuration	Syslog

Configuring Barracuda Web Application Firewall to send syslog events to QRadar

Configure your Barracuda Web Application Firewall appliance to send syslog events to IBM Security QRadar.

Before you begin

Verify that firewalls between the Barracuda appliance and QRadar allow UDP traffic on port 514.

Procedure

1. Log in to the Barracuda Web Application Firewall web interface.
2. Click the **Advanced** tab.
3. From the **Advanced** menu, select **Export Logs**.
4. Click **Add Syslog Server**.
5. Configure the parameters:

Option	Description
Name	The name of the QRadar Console or Event Collector
Syslog Server	The IP address of your QRadar Console or Event Collector.
Port	The port that is associated with the IP address of your QRadar Console or Event Collector. If syslog messages are sent by UDP, use the default port, 514.
Connection Type	The connection type that transmits the logs from the Barracuda Web Application Firewall to the QRadar Console or Event Collector. UDP is the default protocol for syslog communication.
Validate Server Certificate	**No**

6. In the **Log Formats** pane, select a format from the list box for each log type.
   - If you are using newer versions of Barracuda Web Application Firewall, select **LEEF 1.0 (QRadar)**.
   - If you are using older versions of Barracuda Web Application Firewall, select **Custom Format**.
7. Click **Save Changes**.

Chapter 10. Bit9 Security Platform

Use the IBM Security QRadar SIEM DSM for Bit9 Security Platform to collect events from Bit9 Parity devices.

The following table identifies the specifications for the Bit9 Security Platform DSM:

Table 13. DSM specifications for Bit9 Security Platform

Specification	**Value**
Manufacturer	Bit9
DSM name	Bit9 Security Platform
RPM file name	`DSM-Bit9Parity-`*`build_number`*`.noarch.rpm`
Supported versions	V6.0.2 and up
Event format	Syslog
Supported event types	All events
Automatically discovered?	Yes
Included identity?	Yes
More information	Bit9 website (http://www.bit9.com)

To integrate Bit9 Security Platform with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the Bit9 Security Platform DSM RPM.
2. Configure your Bit9 Security Platform device to enable communication with QRadar. You must create a syslog destination and forwarding policy on the Bit9 Security Platform device.
3. If QRadar does not automatically detect Bit9 Security Platform as a log source, create a Bit9 Security Platform log source on the QRadar Console. Use the following Bit9 Security Platform values to configure the log source parameters:

Log Source Identifier	The IP address or host name of the Bit9 Security Platform device
Log Source Type	Bit9 Security Platform
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring Bit9 Security Platform to communicate with QRadar

Configure your Bit9 Security Platform device to forward events to IBM Security QRadar in LEEF format.

Procedure

1. Log in to the Bit9 Security Platform console with Administrator or PowerUser privileges.
2. From the navigation menu, select **Administration** > **System Configuration**.
3. Click **Server Status** and click **Edit**.
4. In the **Syslog address** field, type the IP address of your QRadar Console or Event Collector.
5. From the **Syslog format** list, select **LEEF (Q1Labs)**.
6. Select the **Syslog enabled** check box and click **Update**.

Chapter 11. Blue Coat SG

The IBM Security QRadar DSM for Blue Coat SG collects events from Blue Coat SG appliances.

The following table lists the specifications for the Blue Coat SG DSM:

Table 14. Blue Coat SG DSM specifications

Specification	Value
Manufacturer	Blue Coat
DSM name	Blue Coat SG
RPM file name	`DSM-BlueCoatProxySG-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	SG v4.x and later
Protocol	Syslog Log File Protocol
Recorded event types	All events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	Yes
More information	Blue Coat website (http://www.bluecoat.com)

To send events from Blue Coat SG to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Blue Coat SG DSM RPM on your QRadar Console.
2. Configure your Blue Coat SG device to communicate with QRadar. Complete the following steps:
   - Create a custom event format.
   - Create a log facility.
   - Enable access logging.
   - Configure Blue Coat SG for Log File protocol or syslog uploads.
3. Add an Blue Coat SG log source on the QRadar Console. Configure all the required parameters, but use the following table to configure the parameters that are required to collect Blue Coat SG events:

Table 15. Blue Coat SG log source parameters

Parameter	Value
Log Source type	Bluecoat SG Appliance
Protocol Configuration	Log File Syslog

The instructions provided describe how to configure Blue Coat SG using a custom name-value pair format, however, QRadar also supports the following formats:

- Custom Format
- SQUID
- NCSA
- main
- IM
- Streaming
- smartreporter
- bcereportermain_v1
- bcreporterssl_v1
- p2p
- SSL
- bcreportercifs_v1
- CIFS
- MAPI

Related concepts:

"Creating extra custom format key-value pairs" on page 31

Related tasks:

"Creating a custom event format"
To collect events from Blue Coat SG, create a custom event format.

"Creating a log facility" on page 29
To use the custom log format that you created for IBM Security QRadar, you must associate the custom log format to a facility.

"Enabling access logging" on page 29
You must enable access logging on your Blue Coat SG device.

"Configuring Blue Coat SG for log file protocol uploads" on page 30
To collect the log file protocol events, configure the Blue Coat SG upload client to use the FTP client.

"Configuring Blue Coat SG for syslog uploads" on page 30
To allow syslog event collection, you must configure your Blue Coat SG appliance to forward syslog events to IBM Security QRadar.

Creating a custom event format

To collect events from Blue Coat SG, create a custom event format.

Procedure

1. Log in to the Blue Coat Management Console.
2. Select **Configuration > Access Logging > Formats**.
3. Select **New**.
4. Type a format name for the custom format.
5. Select **Custom format string**.
6. Type the following custom format:

   Attention: The line breaks that in these examples will cause this configuration to fail. Copy the code blocks into a text editor, remove the line breaks, and paste as a single line in the **Custom Format** column.

   ```
   Bluecoat|src=$(c-ip)|srcport=$(c-port)|dst=$(cs-uri-address)
   |dstport=$(cs-uri-port)|username=$(cs-username)|devicetime=$(gmttime)
   |s-action=$(s-action)|sc-status=$(sc-status)|cs-method=$(cs-method)
   |time-taken=$(time-taken)|sc-bytes=$(sc-bytes)|cs-bytes=$(cs-bytes)
   ```

```
|cs-uri-scheme=$(cs-uri-scheme)|cs-host=$(cs-host)|cs-uri-path=$(cs-uri-path)
|cs-uri-query=$(cs-uri-query)|cs-uri-extension=$(cs-uri-extension)
|cs-auth-group=$(cs-auth-group)|rs(Content-Type)=$(rs(Content-Type))
|cs(User-Agent)=$(cs(User-Agent))|cs(Referer)=$(cs(Referer))
|sc-filter-result=$(sc-filter-result)|filter-category=$(sc-filter-category)
|cs-uri=$(cs-uri)
```

7. Select **Log Last Header** from the list.
8. Click **OK**.
9. Click **Apply**.

   Note: The custom format for QRadar supports more key-value pairs by using the Blue Coat ELFF format. For more information, see "Creating extra custom format key-value pairs" on page 31.

What to do next

You are ready to create a log facility on your Blue Coat device.

Related tasks:

"Creating a log facility"
To use the custom log format that you created for IBM Security QRadar, you must associate the custom log format to a facility.

Creating a log facility

To use the custom log format that you created for IBM Security QRadar, you must associate the custom log format to a facility.

Procedure

1. Select **Configuration > Access Logging > Logs**.
2. Click **New**.
3. Configure the following parameters:

Parameter	Description
Log Name	A name for the log facility.
Log Format	The custom format you that created.
Description	A description for the log facility.

4. Click **OK**.
5. Click **Apply**.

Related tasks:

"Enabling access logging"
You must enable access logging on your Blue Coat SG device.

Enabling access logging

You must enable access logging on your Blue Coat SG device.

Procedure

1. Select **Configuration > Access Logging > General**.
2. Select the **Enable Access Logging** check box.
3. Optional: If you use Blue Coat SGOS 6.2.11.2 Proxy Edition, complete the following steps:

a. Select **Config > Policy > VisualPolicy Manager**.
b. In the Policy section, add **Web Access Layer for Logging**.
c. Select **Action > Edit** and enable logging to the log facility.

4. Click **Apply**.

Related concepts:

"Creating extra custom format key-value pairs" on page 31

Configuring Blue Coat SG for log file protocol uploads

To collect the log file protocol events, configure the Blue Coat SG upload client to use the FTP client.

Procedure

1. Select **Configuration > Access Logging > Logs > Upload Client**.
2. From the **Log** list, select the log that contains your custom format.
3. From the **Client type** list, select **FTP Client**.
4. Select the **text file** option.
5. Click **Settings**.
6. From the **Settings For** list, select **Primary FTP Server**.
7. Configure the following values:

Parameter	Description
Host	The IP address of the FTP server that you want to forward the Blue Coat events.
Port	The FTP port number.
Path	The directory path for the log files.
Username	The user name to access the FTP server.

8. Click **OK**.
9. Select the **Upload Schedule** tab.
10. From the **Upload the access log** option, select **Periodically**.
11. Configure the **Wait time between connect attempts** option.
12. Select to upload the log file to the FTP daily or on an interval.
13. Click **Apply**.

Configuring Blue Coat SG for syslog uploads

To allow syslog event collection, you must configure your Blue Coat SG appliance to forward syslog events to IBM Security QRadar.

About this task

When you send syslog events to multiple syslog destinations, a disruption in availability in one syslog destination might interrupt the stream of events to other syslog destinations from your Blue Coat SG appliance.

Procedure

1. Select **Configuration > Access Logging > Logs > Upload Client**.
2. From the **Log** list, select the log that contains your custom format.
3. From the **Client type** list, select **Custom Client**.

4. Click **Settings**.
5. From the **Settings For** list, select **Primary Custom Server**.
6. In the **Host** field, type the IP address for your QRadar system.
7. In the **Port** field, type 514.
8. Click **OK**.
9. Select the **Upload Schedule** tab.
10. From the **Upload the access log** list, select **Continuously**.
11. Click **Apply**.

Creating extra custom format key-value pairs

Use the Extended Log File Format (ELFF) custom format to forward specific Blue Coat data or events to IBM Security QRadar.

The custom format is a series of pipe-delimited fields that start with the `Bluecoat|` field and contains the `$(Blue Coat ELFF)` parameter.

For example:

```
Bluecoat|src=$(c-ip)|srcport=$(c-port)|dst=$(cs-uri-address)|dstport=$(cs-
uri-port)|username=$(cs-username)|devicetime=$(gmttime)|s-action=$(s-
action)|sc-status=$(sc-status)|cs-method=$(cs-method)
```

Table 16. Custom Format examples

Blue Coat ELFF Parameter	QRadar Custom Format Example
sc-bytes	$(sc-bytes)
rs(Content-type)	$(rs(Content-Type))

For more information about available Blue Coat ELFF parameters, see your Blue Coat appliance documentation.

Chapter 12. Cisco IronPort

The IBM Security QRadar DSM for Cisco IronPort provides event information for email spam, web content filtering, and corporate email policy enforcement.

The following table identifies the specifications for the Cisco IronPort DSM:

Table 17. Cisco IronPort DSM specifications

Specification	**Value**
Manufacturer	Cisco
DSM name	Cisco IronPort
RPM file name	`DSM-CiscoIronport-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V5.5 V6.5 V7.1 V7.5 (adds support for access logs)
Protocol	Syslog Log File Protocol
Recorded event types	Mail (syslog) System (syslog) Access (syslog) Web content filtering (Log File)
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Cisco website (http://www.cisco.com)

To collect events from Cisco IronPort, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Cisco IronPort DSM RPM on your QRadar Console.
2. Configure Cisco IronPort to communicate with QRadar. Select one of the following options:

   Mail, system, and access event logs

   Use the syslog protocol to send mail, system, and access events to QRadar. See "Configuring the Cisco IronPort to send syslog events" on page 34.

   Web content filtering logs

   Use the Log File Protocol to retrieve web content filtering events in W3C format from a remote source. Ensure that your QRadar system is running the most recent version of log file protocol. To configure your Cisco IronPort device to send web content filter events, you must configure a log subscription for the web content filter.

Monitoring a directory that has a large volume of files might lead to a delay in processing individual files. To improve monitoring performance, keep the remote directory clean and reduce the number of files in it.

For more information about configuring a log subscription, see your Cisco IronPort documentation.

3. Add a Cisco IronPort log source on the QRadar Console. Configure all required parameters and use the following table to determine specific values for Cisco IronPort event collection:

Table 18. Cisco IronPort log source parameters

Parameter	Value
Log Source type	Cisco IronPort
Protocol Configuration	Syslog (for mail, system, and access event logs Log File (Web content filtering logs)
Event Generator	W3C Configure this parameter if you select **Log File** in the **Protocol Configuration** list.
FTP File Pattern	Must use a regular expression that matches the log files that the web content filter logs generates. Configure this parameter if you select **Log File** in the **Protocol Configuration** list.

Configuring the Cisco IronPort to send syslog events

Configure Cisco IronPort to send syslog events to IBM Security QRadar.

Procedure

1. Log in to Cisco IronPort.
2. Select **System Administration > Log Subscriptions**.
3. Define a log subscription for each log type that you want to forward to QRadar:
   a. Click **Add Log Subscription**.
   b. From the **Log Type** list, select the type of log that you want to configure.
   c. In the **Log Name** field, type a name.

      The appliance uses this name for the directory that will contain the log file.
   d. If you are creating a subscription for access logs, select **Squid** from the **Log style** list and type `dst %k dstPort %p` in the **Custom Fields (optional)** field.
   e. From the **Retrieval Method** list, select **Syslog Push**.
   f. In the **Hostname** field, type the IP address or server name of your QRadar system.
   g. From the **Protocol** list, select UDP or TCP.
   h. From the **Facility** list, select the facility you want to use.

      Tip: You can use syslog only for text-based logs.
4. Save the subscription.

Chapter 13. Correlog Agent for IBM z/OS

The CorreLog Agent for IBM z/OS DSM for IBM Security QRadar can collect event logs from your IBM z/OS servers.

The following table identifies the specifications for the CorreLog Agent for IBM z/OS DSM:

Specification	Value
Manufacturer	CorreLog
DSM name	CorreLog Agent for IBM z/OS
RPM file name	`DSM-CorreLogzOSAgent_`*`qradar-version_build-number`*`.noarch.rpm`
Supported versions	7.1 7.2
Protocol	Syslog LEEF
QRadar recorded events	All events
Automatically discovered	Yes
Includes identity	No
Includes custom event properties	No
More information	Correlog website (https://correlog.com/solutions-and-services/sas-correlog-mainframe.html)

To integrate CorreLog Agent for IBM z/OS DSM with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent CorreLog Agent for IBM z/OS RPM on your QRadar Console.
2. For each CorreLog Agent instance, configure your CorreLog Agent system to enable communication with QRadar.
3. If QRadar does not automatically discover the DSM,, create a log source on the QRadar Console for each CorreLog Agent system you want to integrate. Configure all the required parameters, but use the following table for specific Correlog values:

Parameter	Description
Log Source Type	CorreLog Agent for IBM zOS
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your CorreLog Agent system for communication with QRadar

For the procedure to configure your Correlog Agent system for communication with QRadar, see the CZA - CorreLog Agent for z/OS manual that you received from CorreLog with your Agent for z/OS software distribution.

About this task

Use the following sections of the CZA - CorreLog Agent for z/OS manual:

- General considerations in **Section 1: Introduction**.
- Procedure in **Section 2: Installation**.
- Procedure in the **Section 3: Configuration**.

  Ensure that you complete the **Tailoring the Installation for a Proprietary Syslog Extension/IBM Security QRadar instructions**.

  When you start the CorreLog agent, if QRadar does not collect z/OS events, see the **Troubleshooting topic in Section 3**.
- If you want to customize the optional CorreLog Agent parameter file, review QRadar normalized event attributes in **Appendix G: Fields**.

Chapter 14. CloudPassage Halo

The CloudPassage Halo DSM for IBM Security QRadar can collect event logs from the CloudPassage Halo account.

The following table identifies the specifications for the CloudPassage Halo DSM:

Table 19. CloudPassage Halo DSM Specifications

Specification	Value
Manufacturer	CloudPassage
DSM name	CloudPassage Halo
RPM file name	DSM-CloudPassageHalo-*build_number*.noarch.rpm
Supported versions	All
Event format	Syslog, Log file
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	No
More information	CloudPassage website (www.cloudpassage.com)

To integrate CloudPassage Halo with QRadar, use the following steps:

1. If automatic updates are not enabled, download the latest versions of the following RPMs:
   - DSMCommon RPM
   - CloudPassage Halo RPM
2. Configure your CloudPassage Halo to enable communication with QRadar.
3. If QRadar does not automatically detect CloudPassage Halo as a log source, create a CloudPassage Halo log source on the QRadar Console.

Configuring CloudPassage Halo for communication with QRadar

To collect CloudPassage Halo events, download and configure the CloudPassage Halo Event Connector script to send syslog events to QRadar.

Before you begin

Before you can configure the Event Connector, you must create a read-only CloudPassage API key. To create a read-only key, log in to your CloudPassage Portal and click **Add New Key** on the Site Administration window.

About this task

The Event Connector script requires Python 2.6 or later to be installed on the host on which the Event Connector script runs. The Event Connector makes calls to the CloudPassage Events API, which is available to all Halo subscribers.

Note: You can configure the CloudPassage Halo Event Collect to write the events to file for QRadar to retrieve by using the Log File Protocol, however, this method is not recommended.

Procedure

1. Log in to the CloudPassage Portal.
2. Go to to **Settings > Site Administration**.
3. Click the **API Keys** tab.
4. Click **Show** for the key you want to use.
5. Copy the key ID and secret key into a text file.

   Ensure that the file contains only one line, with the key ID and the secret key separated by a vertical bar/pipe (|), for example, `your_key_id|your_secret_key`. If you want to retrieve events from multiple Halo accounts, add an extra line for each account.
6. Save the file as `haloEvents.auth`.
7. Download the Event Connector script and associated files from https://github.com/cloudpassage/halo-event-connector-python.
8. Copy the following files to a Linux or Windows system that has Python 2.6 (or later) installed:
   - haloEvents.py
   - cpapi.py
   - cputils.py
   - remote_syslog.py (use this script only if you deploy the Event Connector on Windows and you want to send events through syslog)
   - haloEvents.auth
9. Set the environment variables on the Linux or Windows system:
   - On Linux, include the full path to the Python interpreter in the PATH environment variable.
   - On Windows, set the following variables:
     - Set the PATH variable to include the location of haloEvents.py and the Python interpreter.
     - Set the PYTHONPATH variable to include the location of the Python libraries and the Python interpreter.
10. To send events through syslog with the Event Connector is deployed on a Windows system, run the haloEvents.py script with the **`--leefsyslog=<QRadar IP`**> switch:

    ```
    haloEvents.py --leefsyslog=1.2.3.4
    ```

    By default, the Event Connector retrieves existing events on initial connection and then retrieves onlynew events thereafter. To start event retrieval from a specific date, rather than retrieving all historical events on startup, use the **`--starting=<date>`** switch, where date is in the YYYY-MM-DD format:

    ```
    haloEvents.py --leefsyslog=1.2.3.4 --starting=2014-04-02
    ```
11. To send events through syslog and deploy the Event Connector on a Linux system, configure the local logger daemon.

    a. To check which logger the system uses, type the following command:

    ```
    ls -d /etc/*syslog*
    ```

    Depending on what Linus distribution you have, the following files might be listed:

    -

  - rsyslog.conf
  - syslog-ng.conf
  - syslog.conf

b. Edit the appropriate .conf file with relevant information for your environment.

   Example configuration for syslog-ng:

```
source s_src {
      file("/var/log/leefEvents.txt");
};
destination d_qradar {
     udp("qradar_hostname" port(514));
};
log {
     source(s_src); destination(d_qradar);
};
```

c. To run the `haloEvents.py` script with the **`leeffile=<filepath>`** switch, type the following command:

```
haloEvents.py --leeffile=/var/log/leefEvents.txt
```

   You can include **`--starting=YYYY-MM-DD`** switch to specify the date from which you want events to be collected for on initial startup.

   Note: As an alternative to using syslog, you can write events to a file for QRadar to retrieve by using the Log File protocol. For Windows or Linux to write the events to a file instead, use the **`--leeffile=<filename>`** switch to specify the file to write to.

Configuring a CloudPassage Halo log source in QRadar

To collect CloudPassage Halo events, configure a log source in QRadar.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the Log Source Type list, select **CloudPassage Halo**.
7. From the Protocol Configuration list, select **Syslog** or **Log File**.
8. Configure the remaining parameters:
9. Click **Save**.
10. On the Admin tab, click **Deploy Changes**.

Chapter 15. DG Technology MEAS

The IBM Security QRadar DSM for DG Technology MEAS can collect event logs from your DG Technology MEAS servers.

The following table identifies the specifications for the DG Technology MEAS DSM:

Table 20. DSM Specifications for DG Technology MEAS

Specification	**Value**
Manufacturer	DG Technology
Log source type	DG Technology MEAS
RPM file name	`DSM-DGTechnologyMEAS-`*`build_number`*`.noarch.rpm`
Supported versions	8.x
Protocol configuration	LEEF Syslog
Supported event types	Mainframe events
Automatically discovered?	Yes
Includes identity?	No
Includes custom event properties	No
More information	DG Technology website (http://www.dgtechllc.com)

To integrate DG Technology MEAS DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent DG Technology MEAS RPM on your QRadar Console.
2. For each instance of DG Technology MEAS, configure your DG Technology MEAS system to enable communication with QRadar.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your DG Technology MEAS system for communication with QRadar

To collect all audit logs and system events from DG Technology MEAS, you must specify QRadar as the syslog server.

Procedure

1. Log in to your DG Technology MEAS server.
2. Type the following command:

```
java meas/MeasServer 41000 m=qwl lo=IP_address_of_QRadar_host
```

Results

When QRadar receives events from your DG Technology MEAS, a log source is automatically created and listed on the Log Sources window.

Chapter 16. FireEye

The IBM Security QRadar DSM for The FireEye accepts syslog events in Log Event Extended Format (LEEF) and Common Event Format (CEF).

This DSM applies to FireEye CMS, MPS, EX, AX, NX, FX, and HX appliances. QRadar records all relevant notification alerts that are sent by FireEye appliances.

The following table identifies the specifications for the FireEye DSM.

Table 21. FireEye DSM specifications

Specification	Value
Manufacturer	FireEye
DSM name	FireEye MPS
Supported versions	CMS, MPS, EX, AX, NX, FX, and HX
RPM file name	DSM-FireEyeMPS-*QRadar_version-Build_number*.noarch.rpm
Protocol	Syslog
QRadar recorded event types	All relevant events
Auto discovered?	Yes
Includes identity?	No
More information	FireEye website (www.fireeye.com)

To integrate FireEye with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the DSM Common and FireEye MPS RPM on your QRadar Console.
2. For each instance of FireEye in your deployment, configure the FireEye system to forward events to QRadar.
3. For each instance of FireEye, create an FireEye log source on the QRadar Console.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your FireEye system for communication with QRadar

To enable FireEye to communicate with QRadar, you must configure your FireEye appliance to forward syslog events.

About this task

Procedure

1. Log in to the FireEye appliance by using the CLI.
2. To activate configuration mode, type the following commands:
   ```
   enable
   ```
   ```
   configure terminal
   ```
3. To enable rsyslog notifications, type the following command:
   ```
   fenotify rsyslog enable
   ```
4. To add QRadar as an rsyslog notification consumer, type the following command:
   ```
   fenotify rsyslog trap-sink QRadar
   ```
5. To specify the IP address for the QRadar system that you want to receive rsyslog trap-sink notifications, type the following command:
   ```
   fenotify rsyslog trap-sink QRadar address QRadar_IP_address
   ```
6. To define the rsyslog event format, type the following command:
   ```
   fenotify rsyslog trap-sink QRadar prefer message format leef
   ```
7. To save the configuration changes to the FireEye appliance, type the following command:
   ```
   write memory
   ```

Configuring a FireEye log source in QRadar

QRadar automatically creates a log source after your QRadar Console receives FireEye events. If QRadar does not automatically discover FireEye events, you can manually add a log source for each instance from which you want to collect event logs.

About this task

Procedure

1. Log in to QRadar
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **FireEye**.
7. Using the P**rotocol Configuration** list, select **Syslog**.
8. In the **Log Source Identifier** field, type the IP address or host name of the FireEye appliance.
9. Configure the remaining parameters.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

Chapter 17. FreeRADIUS

The IBM Security QRadar DSM for FreeRADIUS collects events from your FreeRADIUS device.

The following table lists the specifications for the FreeRADIUS DSM:

Table 22. FreeRADIUS DSM specifications

Specification	Value
Manufacturer	FreeRADIUS
DSM name	FreeRADIUS
RPM file name	`DSM-FreeRADIUS-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V2.x
Event format	Syslog
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	FreeRADIUS website (http://freeradius.org)

To send logs from FreeRADIUS to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the FreeRADIUS DSM RPM on your QRadar Console.
2. Configure your FreeRADIUS device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a FreeRADIUS log source on the QRadar Console. The following table describes the parameters that require specific values for FreeRADIUS event collection:

Table 23. FreeRADIUS log source parameters

Parameter	Value
Log Source type	FreeRADIUS
Protocol Configuration	Syslog

Configuring your FreeRADIUS device to communicate with QRadar

Configure FreeRADIUS to send logs to the syslog daemon of the host and configure the daemon to send events to QRadar.

Before you begin

You must have a working knowledge of syslog configuration and the Linux distribution.

About this task

FreeRADIUS has multiple distributions. Some files might not be in the same locations that are described in this procedure. For example, the location of the FreeRADIUS startup script is based on distribution. Conceptually, the configuration steps are the same for all distributions.

Procedure

1. Log in to the system that hosts FreeRADIUS.
2. Edit the `/etc/freeradius/radius.conf` file.
3. Change the text in the file to match the following lines:

   ```
   logdir = syslog
   Log_destination = syslog
   log{
       destination = syslog
       syslog_facility = daemon
       stripped_names = no
       auth = yes
       auth_badpass = no
       auth_goodpass = no
   }
   ```

4. Edit the `/etc/syslog.conf` file.
5. To configure log options, add the following text.

   # .=notice logs authentication messages (L_AUTH).

   ```
   # <facility_name>.=notice
   @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>
   ```

   # .=err logs module errors for FreeRADIUS.

   ```
   #<facility_name>.=err
   @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>
   ```

   # .* logs messages to the same target.

   ```
   # <facility_name>.*
   @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>
   ```

   An example syslog facility name is *local1*. You can rename it.

   To configure a log option, remove the comment tag (#) from one of the active lines that contains an `@` symbol.

6. If the configuration change does not load automatically, restart the syslog daemon. The method to restart the syslog daemon depends on the distribution that is used. The following table lists possible methods.

Operating system distribution	Command to restart daemon
Red Hat Enterprise Linux	service syslog restart
Debian Linux or Ubuntu Linux	`/etc/init.d/syslog` restart
FreeBSD operating system	`/etc/rc.d/syslogd` restart

7. Add the following options to the FreeRADIUS startup script:
   - `-l syslog`
   - `-g <facility_name>`

   The `-g` value must match the facility name in Step 5.

8. Restart FreeRADIUS.

Chapter 18. genua genugate

The IBM Security QRadar DSM for genua genugate collects events from a genua genugate device.

genua genugate produces logs from third-party software such as openBSD and sendMail. The genua genugate DSM provides basic parsing for the logs from these third-party devices. To achieve more specify parsing for these logs, install the specific DSM for that device.

The following table lists the specifications for the genua genugate DSM:

Table 24. genua genugate DSM specifications

Specification	Value
Manufacturer	genua
DSM name	genua genugate
RPM file name	`DSM-GenuaGenugate-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	8.2 and later
Protocol	Syslog
Recorded event types	General error messages High availability General relay messages Relay-specific messages genua programs/daemons EPSI Accounting Daemon - gg/src/acctd Configfw FWConfig ROFWConfig User-Interface Webserver
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	genua website (https://www.genua.de/en/solutions/high-resistance-firewall-genugate.html)

To send genua genugate events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - genua genugate DSM RPM
2. Configure your genua genugate device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a genua genugate log source on the QRadar Console. Configure all required parameters and use the following table to identify specific values for genua genugate:

Table 25. genua genugate log source parameters

Parameter	Value
Log Source type	genua genugate
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring genua genugate to send events to QRadar"
Configure genua genugate to send events to IBM Security QRadar.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring genua genugate to send events to QRadar

Configure genua genugate to send events to IBM Security QRadar.

Procedure

1. Log in to genua genugate.
2. Click **System > Sysadmin > Logging page**.
3. In the **IBM QRadar IP Address** field, type the IP address of your QRadar Console or Event Collector.
4. Select the **Accounting to External** check box.
5. Click **OK**.

Chapter 19. HyTrust CloudControl

The IBM Security QRadar DSM for HyTrust CloudControl collects events from HyTrust CloudControl devices.

The following table lists the specifications for the HyTrust CloudControl DSM:

Table 26. HyTrust CloudControl DSM specifications

Specification	**Value**
Manufacturer	Hytrust
DSM name	HyTrust CloudControl
RPM file name	`DSM-HyTrustCloudControl-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V3.0.2 through V3.6.0
Protocol	Syslog
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Hytrust web site (http://www.hytrust.com)

To collect HyTrust CloudControl events, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - HyTrust CloudControl DSM RPM
2. Configure your HyTrust CloudControl device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a HyTrust CloudControl log source on the QRadar Console. The following table describes the parameters that require specific values that are required for HyTrust CloudControl event collection:

Table 27. HyTrust CloudControl log source parameters

Parameter	**Value**
Log Source type	HyTrust CloudControl
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring HyTrust CloudControl to communicate with QRadar" on page 50
To collect HyTrust CloudControl events, you must configure your third-party device to send events to IBM Security QRadar

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source

to receive events from your network devices or appliances.

Configuring HyTrust CloudControl to communicate with QRadar

To collect HyTrust CloudControl events, you must configure your third-party device to send events to IBM Security QRadar

Procedure

1. Log in to HyTrust CloudControl.
2. From the HTA Management Console, select **Configuration** > **Logging**.
3. From the **HTA Logging Aggregation options**, select **External**.
4. From the **Logging Aggregation Template Type** options, select either **Proprietary** or **CEF**.
5. In the **HTA Syslog Servers** field, type the IP address for QRadar.

Chapter 20. IBM AIX DSMs

IBM Security QRadar provides the IBM AIX Audit and IBM AIX Server DSMs to collect and parse audit or operating system events from IBM AIX devices.

IBM AIX Server DSM overview

The IBM AIX Server DSM collects operating system and authentication events using syslog for users that interact or log in to your IBM AIX appliance.

The following table identifies the specifications for both IBM AIX DSM Server:

Table 28. IBM AIX Server DSM specifications

Specification	Value
Manufacturer	IBM
DSM names	IBM AIX Server
RPM file names	`DSM-IBMAIXServer-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V5.X, V6.X, and V7.X
Protocol type	Syslog
QRadar recorded event types	Login or logoff events Session opened or session closed events Accepted password and failed password events Operating system events
Automatically discovered?	Yes
Includes identity?	Yes
More information	IBM website (http://www.ibm.com/)

To integrate IBM AIX Server events with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the latest version of the IBM AIX Server DSM.
2. Configure your IBM AIX Server device to send syslog events to QRadar.
3. Configure a syslog-based log source for your IBM AIX Server device. Use the following protocol-specific parameters:

Parameter	Description
Log Source Type	IBM AIX Server
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring your IBM AIX Server device to send syslog events to QRadar"

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your IBM AIX Server device to send syslog events to QRadar

Procedure

1. Log in to your IBM AIX appliance as a root user.
2. Open the `/etc/syslog.conf` file.
3. To forward the system authentication logs to QRadar, add the following line to the file:

   ```
   auth.info @QRadar_IP_address
   ```

   A tab must separate auth.info and the IP address of QRadar. For example:

   ```
   ##### begin /etc/syslog.conf
   mail.debug /var/adm/maillog
   mail.none /var/adm/maillog
   auth.notice /var/adm/authlog
   lpr.debug /var/adm/lpd-errs
   kern.debug /var/adm/messages
   *.emerg;*.alert;*.crit;*.warning;*.err;*.notice;*.info /var/adm/messages
   auth.info            @<10.100.100.1>
   ##### end /etc/syslog.conf
   ```

4. Save and exit the file.
5. Restart the syslog service:

   ```
   refresh -s syslogd
   ```

IBM AIX Audit DSM overview

The IBM AIX Audit DSM collects detailed audit information for events that occur on your IBM AIX appliance.

The following table identifies the specifications for the IBM AIX Audit DSM:

Table 29. IBM AIX Audit DSM specifications

Specification	Value
Manufacturer	IBM
DSM names	IBM AIX Audit
RPM file names	`DSM-IBMAIXAudit-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V6.1 and V7.1
Protocol type	Syslog Log File Protocol
QRadar recorded event types	Audit events
Automatically discovered?	Yes
Includes identity?	No

Table 29. IBM AIX Audit DSM specifications (continued)

Specification	Value
More information	IBM website (http://www.ibm.com/)

To integrate IBM AIX Audit events with QRadar, complete the following steps:

1. Download the latest version of the IBM AIX Audit DSM.
2. For syslog events, complete the following steps:
   a. Configure your IBM AIX Audit device to send syslog events to QRadar. See "Configuring IBM AIX Audit DSM to send syslog events to QRadar" on page 54.
   b. If QRadar does not automatically discover the log source, add an IBM AIX Audit log source. Use the following IBM AIX Audit-specific values in the log source configuration:

Parameter	Value
Log Source Type	IBM AIX Audit
Protocol Configuration	Syslog

3. For log file protocol events, complete the following steps:
   a. Configure your IBM AIX Audit device to convert audit logs to the log file protocol format.
   b. Configure a log file protocol-based log source for your IBM AIX Audit device. Use the following protocol-specific values in the log source configuration:

Parameter	Value
Log Source Type	IBM AIX Audit
Protocol Configuration	Log File
Service Type	The protocol to retrieve log files from a remote server. **Important:** If you select the SCP and SFTP service type, ensure that the server that is specified in the **Remote IP or Hostname** parameter has the SFTP subsystem enabled.
Remote Port	If the host for your event files uses a non-standard port number for FTP, SFTP, or SCP, adjust the port value.
SSH Key File	If you select SCP or SFTP as the Service Type, use this parameter to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** parameter is ignored.
Remote Directory	The directory location on the remote host where the files are retrieved. Specify the location relative to the user account you are using to log in. **Restriction:** For FTP only. If your log files are in a remote user home directory, leave the remote directory blank to support operating systems where a change in the working directory (CWD) command is restricted.

Parameter	Value
FTP File Pattern	The FTP file pattern must match the name that you assigned to your AIX audit files with the **-n** parameter in the audit script. For example, to collect files that start with AIX_AUDIT and end with your time stamp value, type `AIX_Audit_*`.
FTP Transfer Mode	ASCII is required for text event logs that are retrieved by the log file protocol by using FTP.
Processor	NONE
Change Local Directory?	Leave this check box clear.
Event Generator	LineByLine The Event Generator applies more processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring IBM AIX Audit DSM to send syslog events to QRadar"
To collect syslog audit events from your IBM AIX Audit device, redirect your audit log output from your IBM AIX device to the IBM Security QRadar Console or Event Collector.

"Configuring IBM AIX Audit DSM to send log file protocol events to QRadar" on page 55
Configure the audit.pl script to run each time that you want to convert your IBM AIX audit logs to a readable event log format for QRadar.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring IBM AIX Audit DSM to send syslog events to QRadar

To collect syslog audit events from your IBM AIX Audit device, redirect your audit log output from your IBM AIX device to the IBM Security QRadar Console or Event Collector.

About this task

On an IBM AIX appliance, you can enable or disable classes in the audit configuration. The IBM AIX default classes capture a large volume of audit events. To prevent performance issues, you can tune your IBM AIX appliance to reduce the number of classes that are collected. For more information about audit classes, see your IBM AIX appliance documentation.

Procedure

1. Log in to your IBM AIX appliance.
2. Open the audit configuration file:

```
/etc/security/audit/config
```

3. Edit the Start section to disable the **binmode** element and enable the **streammode** element:

   ```
   binmode = off
   streammode = on
   ```

4. Edit the Classes section to specify which classes to audit.
5. Save the configuration changes.
6. Open the streamcmds file:

   ```
   /etc/security/audit/streamcmds
   ```

7. Add the following line to the file:

   ```
   /usr/sbin/auditstream | auditpr -h eclrRdi | /usr/bin/logger -p
   local0.debug
   ```

8. Save the configuration changes.
9. Edit the syslog configuration file to specify a debug entry and the IP address of the QRadar Console or Event Collector:

   ```
   *.debug @ip_address
   ```

   Tip: A tab must separate *.debug from the IP address.

10. Save the configuration changes.
11. Reload your syslog configuration:

    ```
    refresh -s syslogd
    ```

12. Start the audit script on your IBM AIX appliance:

    ```
    audit start
    ```

What to do next

The IBM AIX Audit DSM automatically discovers syslog audit events that are forwarded from IBM AIX to QRadar and creates a log source. If the events are not automatically discovered, you can manually configure a log source.

Configuring IBM AIX Audit DSM to send log file protocol events to QRadar

Configure the audit.pl script to run each time that you want to convert your IBM AIX audit logs to a readable event log format for QRadar.

Before you begin

To use the audit script, you are required to install a version of Perl 5.8 or above on your IBM AIX appliance

About this task

This procedure requires you to configure two files:

Audit configuration file

The audit configuration file identifies the event classes that are audited and the location of the event log file on your IBM AIX appliance. The IBM AIX default classes capture many audit events. To prevent performance issues, you can configure the classes in the audit configuration file. For more information about configuring audit classes, see your IBM AIX documentation.

Audit script

The audit script uses the audit configuration file to identify which audit logs to read and converts the binary logs to single-line events that QRadar can read. The log file protocol can then retrieve the event log from your IBM AIX appliance and import the events to QRadar. The audit script uses the audit.pr file to convert the binary audit records to event log files QRadar can read.

Run the audit script each time that you want to convert your audit records to readable events. You can use a cron job to automate this process. for example, you can add `0 * * * * /audit.pl` to allow the audit script to run hourly. For more information, see your system documentation.

Procedure

1. Log in to your IBM AIX appliance.
2. Configure the audit configuration file:
   a. Open the audit configuration file:
   ```
   etc/security/audit/config
   ```
   b. Edit the Start section to enable the **binmode** element.
   ```
   binmode = on
   ```
   c. In the Start section, edit the configuration to determine which directories contain the binary audit logs. The default configuration for IBM AIX auditing writes binary logs to the following directories:
   ```
   trail = /audit/trail
   bin1 = /audit/bin1
   bin2 = /audit/bin2
   binsize = 10240
   cmds = /etc/security/audit/bincmds
   ```
   In most cases, you do not have to edit the binary file in the bin1 and bin2 directories.

   d. In the Classes section, edit the configuration to determine which classes are audited. For information on configuring classes, see your IBM AIX documentation.

   e. Save the configuration changes.
3. Start auditing on your IBM AIX system:
   ```
   audit start
   ```
4. Install the audit script:
   a. Access the IBM Support website (http://www.ibm.com/support).

   b. Download the `audit.pl.gz` file.

   c. Copy the audit script to a folder on your IBM AIX appliance.

   d. Extract the file:
   ```
   tar -zxvf audit.pl.gz
   ```
   e. Start the audit script:
   ```
   ./audit.pl
   ```
   You can add the following parameters to modify the command:

Parameter	Description
-r	Defines the results directory where the audit script writes event log files for QRadar. If you do not specify a results directory, the script writes the events to the following `/audit/results/` directory. The results directory is used in the **Remote Directory** parameter in the log source configuration uses this value. To prevent errors, verify that the results directory exists on your IBM AIX system.
-n	Defines a unique name for the event log file that is generated by audit script. The **FTP File Pattern** parameter in the log source configuration uses this name to identify the event logs that the log source must retrieve in QRadar
-l	Defines the name of the last record file.
-m	Defines the maximum number of audit files to retain on your IBM AIX system. By default, the script retains 30 audit files. When the number of audit files exceeds the value of the **-m** parameter, the script deletes the audit file with the oldest time stamp.
-t	Defines the directory that contains the audit trail file. The default directory is `/audit/trail`.

What to do next

The IBM AIX Audit DSM automatically discovers log file protocol audit events that are forwarded from IBM AIX to QRadar and creates a log source. If the events are not automatically discovered, you can manually configure a log source.

Chapter 21. IBM AS/400 iSeries event collection

IBM Security QRadar has multiple options for how to collect events from an IBM AS/400 (or IBM OS/400) iSeries device.

You can use one of the following software products to configure QRadar to retrieve events from an IBM AS/400 (or IBM OS/400) iSeries device:

IBM AS/400 iSeries DSM
The IBM AS/400 iSeries DSM uses the DSPJRN command to write audit journal records to a database file. The database file is uploaded to an FTP server for QRadar to retrieve. QRadar uses the Log File protocol to retrieve the database file.

LogAgent for System i
The LogAgent for System i accepts all Common Event Format (CEF) formatted syslog messages. You can integrate an IBM OS/400 device and then use the LogAgent for System i software. After you configure your LogAgent for System i software, use the Log File protocol source to retrieve the syslog CEF messages.

For more information, see your *Patrick Townsend Security Solutions LogAgent for System i* documentation.

PowerTech Interact
PowerTech Interact accepts all Common Event Format (CEF) formatted syslog messages. After you configure your PowerTech Interact software, use the Log File protocol source to pull the syslog CEF messages.

Raz-Lee iSecurity DSM
You can also use the Raz-Lee iSecurity DSM to retrieve events from an IBM AS/400 (or IBM OS/400) iSeries device.

For more information, see the Frequently Asked Questions webpage on the IBM Support webpage.

Related concepts:

Chapter 22, "IBM AS/400 iSeries DSM," on page 61
The IBM Security QRadar DSM for IBM AS/400 iSeries collects audit records and event information from IBM AS/400 iSeries devices.

Chapter 22. IBM AS/400 iSeries DSM

The IBM Security QRadar DSM for IBM AS/400 iSeries collects audit records and event information from IBM AS/400 iSeries devices.

The following table identifies the specifications for the IBM AS/400 iSeries DSM:

Table 30. IBM AS/400 iSeries DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM AS/400 iSeries
Supported versions	V5R4 and later
RPM file name	`DSM-IBMiSeries-`*`Qradar_version-build_number`*`.noarch.rpm`
Protocol	Log File Protocol syslog
Recorded event types	Audit records and events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	IBM website (http://www.ibm.com/)

To collect events from IBM AS/400 iSeries devices, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM AS/400 iSeries DSM RPM on your QRadar Console.
2. Configure your IBM AS/400 iSeries device to communicate with QRadar.
3. Add an IBM AS/400 iSeries log source on the QRadar Console. Configure all the required parameters, but use the following table to configure the parameters that are required to collect IBM AS/400 iSeries events:

Table 31. IBM AS/400 iSeries log source parameters

Parameter	Value
Log Source Type	IBM AS/400 iSeries
Protocol Configuration	Log File **Note:** If you are using the PowerTech Interact or LogAgent for System i software to collect CEF formatted syslog messages, you must select the **Syslog** option
Service Type	Secure File Transfer Protocol (SFTP)

Related tasks:

"Configuring an IBM iSeries device to communicate with QRadar" on page 62
For IBM Security QRadar to be able to collect IBM iSeries events, you need to configure your IBM iSeries device to communicate with your QRadar device.

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM

RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring an IBM iSeries device to communicate with QRadar

For IBM Security QRadar to be able to collect IBM iSeries events, you need to configure your IBM iSeries device to communicate with your QRadar device.

About this task

The IBM AS/400 iSeries DSM uses an agent that manages, gathers, and transfers event information. The agent uses the DSPJRN command to write audit journal records to a database file. These records are reformatted and forwarded to an FTP server where QRadar can retrieve the records.

The IBM iSeries system records and writes security events in the Audit Journal and the QHST logs. QHST logs are stored in the Audit Journal as TYPE5 messages.

Procedure

1. From the IBM support website (http://www.ibm.com/support), download the AJLIB.SAVF file.
2. Copy the AJLIB.SAVF file to a computer or terminal that has FTP access to the IBM AS/400 iSeries device.
3. Using FTP on the computer or terminal, replace the iSeries generic SAVF file with the AJLIB.SAVF file. Type the following commands:

   ```
   cd qgpl
   quote site namefmt 1
   bin
   lcd c:\
   put ajlib.savf
   quit
   ```

   If you transfer your SAVF file from another iSeries device, send the file with the BINARY FTP subcommand mode before the GET or PUT statement.
4. To restore the AJLIB library on the IBM iSeries device, type the following command:

   ```
   RSTLIB SAVLIB(AJLIB) DEV(*SAVF) SAVF(AJLIB)
   ```
5. To restore the IFS directory, type the following command:

   ```
   RST DEV('/qsys.lib/ajlib.lib/ajifs.file') OBJ(('/ajlib'))
   ```
6. To configure the data collection start date and time for the Audit Journal Library (AJLIB), type the following command:

   ```
   ADDLIBLE AJLIB
   AJLIB/SETUP
   ```

   You are prompted for a user name and password. If you start the Audit Journal Collector, a failure message is sent to QSYSOPR. The setup function sets a default start date and time for data collection from the Audit Journal to 08:00:00 of the current day.

   Tip: To preserve your previous start date and time information for a previous installation, you must run AJLIB/DATETIME. Record the previous start date and time, and then type those values when you run AJLIB/SETUP command. The start date and time must contain a valid date and time in the six character system date and system time format. The end date and time must be a valid date and time or left blank.

7. If you changed the start date and time, type the following command to update the IBM AS/400 iSeries device:

   ```
   AJLIB/DATETIME
   ```

8. To launch the Audit Journal Collection program to gather and send records to your remote FTP server, type the following command:

   ```
   AJLIB/AUDITJRN
   ```

   The process Audit Journal Collection program is typically automated by an iSeries Job Scheduler to collect records periodically.

Results

If the FTP transfer is successful, the current date and time information is written into the start time for `AJLIB/DATETIME` to update the gather time and the end time is set to blank. If the FTP transfer fails, the export file is erased and no updates are made to the gather date or time and a message is sent to QSYSOPR.

Chapter 23. IBM Federated Directory Server

The IBM Security QRadar DSM collects events from IBM Federated Directory Server systems.

The following table identifies the specifications for the IBM Federated Directory Server DSM:

Table 32. IBM Federated Directory Server DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM Federated Directory Server
RPM file name	`DSM-IBMFederated DirectoryServer-` *`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V7.2.0.2 and later
Event format	LEEF
Recorded event types	FDS Audit
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Security Directory Server information in the IBM Knowledge Center ((http://www-01.ibm.com/support/knowledgecenter/SSVJJU/welcome)

To send events from IBM Federated Directory Server to QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - IBM Federated Directory Server DSM RPM
2. Configure QRadar monitoring on your IBM Federated Directory Server device.
3. If QRadar does not automatically detect the log source, add an IBM Federated Directory Server log source on the QRadar Console. The following table describes the parameters that require specific values for IBM Federated Directory Server event collection:

Table 33. IBM Federated Directory Serve log source parameters

Parameter	Value
Log Source type	IBM Federated Directory Server
Protocol Configuration	Syslog
Log Source Identifier	The source IP or host name of the IBM Federated Directory Server.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM

RPM manually.

"Configuring IBM Federated Directory Server to monitor security events"
Configure IBM Federated Directory Server to monitor security events, which are generated when an entry is added, modified, or deleted in the target

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring IBM Federated Directory Server to monitor security events

Configure IBM Federated Directory Server to monitor security events, which are generated when an entry is added, modified, or deleted in the target

Procedure

1. Log in to your IBM Federated Directory Server.
2. In the navigation pane, under **Common Settings**, click **Monitoring**.
3. On the Monitoring page, click the **QRadar** tab.
4. To indicate that you want to monitor security events, on the **QRadar** page, select **Enabled** .
5. Configure the parameters
6. In the **Map file** field, specify the path and file name of the map file that configures the various QRadar LEEF attributes for the event.
7. Click **Select** to browse for the map file. The default value points to the `LDAPSync/QRadar.map` file.
8. In the **Date format mask** field, specify a standard Java `SimpleDateFormat` mask to use for date values that are written in mapped LEEF attributes.

   This value controls both the value of the **devTimeFormat** attribute and the formatting of date values in the event. The default value is the ISO 8601 standard mask, `MMM dd yy HH:mm:ss`, which creates a string, `Oct 16 12 15:15:57`.

Chapter 24. IBM Fiberlink MaaS360

The IBM Fiberlink® MaaS360® DSM for IBM Security QRadar can collect event logs from the Fiberlink MaaS360 console.

The following table identifies the specifications for the IBM Fiberlink MaaS360 DSM:

Table 34. IBM Fiberlink MaaS360 DSM Specification

Specification	Value
Manufacturer	IBM
DSM name	IBM Fiberlink MaaS360
RPM file name	DSM-IBMFiberlinkMaaS360
Supported versions	N/A
Event format	LEEF
QRadar recorded event types	Compliance rule events
Automatically discovered?	No
Included identity?	No
More information	Fiberlink MaaS360 website (http://www.maas360.com/)

To integrate IBM Fiberlink MaaS360 with QRadar, use the following steps:

1. If automatic updates are not enabled, download the latest versions of the following RPMs:
   - DSMCommon RPM
   - IBM FiberLink REST API Protocol RPM
   - IBM Fiberlink MaaS360 RPM
2. Configure your Fiberlink MaaS360 instance to enable communication with QRadar.
3. Create an IBM Fiberlink MaaS360 log source on the QRadar Console.

Manually installing an RPM

If automatic updates are not enabled on your QRadar Console or if the Console is restricted from the Internet, you can download DSM, protocol, and scanner RPMs from the IBM support website. Then you can install the RPM by using the command-line interface. To uninstall an RPM, contact Customer Support.

Procedure

1. Access the IBM support website (http://www.ibm.com/support).
2. Download the RPM file to the system that hosts your QRadar Console.
3. Using SSH, log in to QRadar as the root user.
4. Go to the directory that includes the downloaded file.
5. Type the following command:
   ```
   rpm -Uvh filename
   ```
6. Log in to theQRadar user interface.

7. On the **Admin** tab, click **Deploy Changes**.

   Attention: For protocol RPM installations, follow the post installation steps that are provided on the Console output where the installation is run from.

Configuring your Fiberlink MaaS360 instance for communication with QRadar

To allow QRadar communication, you need to enable the REST API and copy the public certificate from the Fiberlink MaaS360 instance to the QRadar Console.

Procedure

1. To enable the REST API for your Fiberlink MaaS360 account, contact Fiberlink customer service.
2. Copy the public certificate from the Fiberlink login server to the `/opt/qradar/conf/trusted_certificates` directory on your QRadar Console.

   Ensure that the following conditions are met:
   - The certificate is DER encoded.
   - The file name extension is .DER. The extension is case-sensitive.

Configuring an IBM Fiberlink MaaS360 log source in QRadar

To collect IBM Fiberlink MaaS360 events, configure a log source in QRadar.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the Log Source Type list, select **IBM Fiberlink MaaS360**.
7. From the Protocol Configuration list, select **IBM Fiberlink REST API**.
8. Configure the following IBM Fiberlink REST API parameters:

Parameter	Description
Login URL	The URL for the Fiberlink MaaS login server.
Secret Key	The secret key that is provided by Fiberlink Customer Service when you enabled the REST API.
App ID	The App ID that was provided by Fiberlink Customer Service when you enabled the REST API.
Billing ID	The Billing ID for your Fiberlink MaaS360 account.
Platform	The platform version of the Fiberlink MaaS360 console.
App Version	The App Version of the application that corresponds to your REST API account.

9. Configure the remaining parameters.
10. Click **Save**.

11. On the Admin tab, click **Deploy Changes**.

Chapter 25. IBM Security Privileged Identity Manager

The IBM Security QRadar DSM for IBM Security Privileged Identity Manager collects events from IBM Security Privileged Identity Manager devices.

The following table identifies the specifications for the IBM Security Privileged Identity Manager DSM:

Table 35. IBM Security Privileged Identity Manager DSM specifications

Specification	**Value**
Manufacturer	IBM
DSM name	IBM Security Privileged Identity Manager
RPM file name	`DSM-IBMSecurityPrivilegedIdentityManager-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V2.0
Protocol	JDBC
Recorded event types	Audit Authentication System
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	IBM Security Privileged Identity Manager website (http://www-03.ibm.com/software/products/en/pim/)

To collect events from IBM Security Privileged Identity Manager, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - JDBC Protocol RPM
   - IBM Security Privileged Identity Manager DSM RPM
2. Collect information from the IBM Security Privileged Identity Manager web user interface.
3. Add an IBM Security Privileged Identity Manager log source on the QRadar Console. The following table describes the parameters that require specific values for IBM Security Privileged Identity Manager event collection:

Table 36. IBM Security Privileged Identity Manager log source parameters

Parameter	**Value**
Log Source type	IBM Security Privileged Identity Manager
Protocol Configuration	JDBC
Log Source Identifier	*<DATABASE@HOSTNAME>*
Database Type	DB2

Table 36. IBM Security Privileged Identity Manager log source parameters (continued)

Parameter	Value
Database Name	Must match the value in the **Database name** field in IBM Security Privileged Identity Manager.
IP or Hostname	Must match the value in the **Hostname** field in IBM Security Privileged Identity Manager.
Port	Must match the value in the **Port** field in IBM Security Privileged Identity Manager.
Username	Must match the value in the **Database administrator ID** field in IBM Security Privileged Identity Manager.
Predefined Query	None
Table Name	*DB2ADMIN*.V_PIM_AUDIT_EVENT Replace *DB2ADMIN* with the actual database schema name as identified in the Database Administrator ID parameter in IBM Security Privileged Identity Manager.
Select List	*
Compare Field	TIMESTAMP
Use Prepared Statements	Select this check box.
Start Date and Time	Initial date/time for the JDBC retrieval.
Polling Interval	10
EPS Throttle	20000

Configuring IBM Security Privileged Identity Manager

To configure a log source in IBM Security QRadar, you must record some information from IBM Security Privileged Identity Manager.

Before you begin

To communicate with QRadar, the IBM Security Privileged Identity Manager DB2 database must have incoming TCP connections enabled.

Procedure

1. Log in to IBM Security Privileged Identity Manager.
2. Click the **Configure Privileged Identity Manager** tab.
3. In the Manage External Entities pane, select **Database Server Configuration**.
4. Double-click the **Identity data store** row in the **Database Server Configuration** column.
5. Record the values for the following parameters:
   - Host name
   - Port
   - Database name
   - Database Administrator ID

6. To create a view in IBM Security Privileged Identity Manager DB2 database in the same schema as identified in the Database Administrator ID parameter, run the following SQL statement:

   ```
   CREATE view V_PIM_AUDIT_EVENT
   AS
   SELECT
   ae.ID, ae.itim_event_category as event_category, ae.ENTITY_NAME, service.NAME service_name,
   ae.ENTITY_DN, ae.ENTITY_TYPE,
   ae.ACTION, ae.INITIATOR_NAME, ae.INITIATOR_DN, ae.CONTAINER_NAME, ae.CONTAINER_DN,
   ae.RESULT_SUMMARY, ae.TIMESTAMP,
   lease.POOL_NAME, lease.LEASE_DN, lease.LEASE_EXPIRATION_TIME, lease.JUSTIFICATION,
   ae.COMMENTS, ae.TIMESTAMP2, ae.WORKFLOW_PROCESS_ID
   FROM AUDIT_EVENT ae
   LEFT OUTER JOIN AUDIT_MGMT_LEASE lease ON (ae.id = lease.event_id)
   LEFT OUTER JOIN SA_EVALUATION_CREDENTIAL cred ON (LOWER(ae.entity_dn) = LOWER(cred.DN))
   LEFT OUTER JOIN V_SA_EVALUATION_SERVICE service ON (LOWER(cred.service_dn) = LOWER(service.dn));
   ```

What to do next

"Adding a log source" on page 3

Chapter 26. IBM RACF

IBM Security QRadar includes two options for integrating event from IBM RACF.

See the following options:
- "Integrating IBM RACF with QRadar Using IBM Security zSecure"
- "Integrate IBM RACF with QRadar using audit scripts" on page 80

Integrating IBM RACF with QRadar Using IBM Security zSecure

The IBM RACF DSM allows you to integrate events from an IBM z/OS mainframe using IBM Security zSecure.

Using a zSecure process, events from the System Management Facilities (SMF) are recorded to an event file in the Log Enhanced Event format (LEEF). IBM Security QRadar retrieves the LEEF event log files using the log file protocol and processes the events. You can schedule to retrieve events on a polling interval, which allows QRadar to retrieve the events on the schedule you have defined.

To integrate IBM RACF LEEF events:
1. Confirm your installation meets any prerequisite installation requirements. For more information, see "Before You Begin."
2. Configure your IBM z/OS image to write events in LEEF format. For more information, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.
3. Create a log source in QRadar for IBM RACF to retrieve your LEEF formatted event logs. For more information, see "Create an IBM RACF log source" on page 76.
4. Optional. Create a custom event property for IBM RACF in QRadar. For more information, see the *IBM Security QRadar Custom Event Properties for IBM z/OS* technical note.

Before You Begin

Before you can configure the data collection process, you must complete the basic zSecure installation process.

The following prerequisites are required:
- You must ensure parmlib member IFAPRDxx is not disabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- You must configure an SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
- You must allow SFTP, FTP, or SCP traffic on firewalls located between QRadar and your z/OS image.

After installing the software, you must also perform the post-installation activities to create and modify the configuration. For instructions on installing and configuring zSecure, see the *IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide*.

Create an IBM RACF log source

The Log File protocol allows IBM Security QRadar to retrieve archived log files from a remote host.

About this task

Log files are transferred, one at a time, to QRadar for processing. The log file protocol can manage plain text event logs, compressed files, or archives. Archives must contain plain-text files that can be processed one line at a time. Multi-line event logs are not supported by the log file protocol. IBM RACF integrated with QRadar, using audit scripts, writes log files to a specified directory as plain text files. QRadar processes the events, which are written as one event per line in the file. QRadar extracts the archive and processes the events, which are written as one event per line in the file.

To retrieve these events, you must create a log source using the Log File protocol. QRadar requires credentials to log in to the system hosting your event files and a polling interval.

Procedure

1. Click the Admin tab.
2. Click the Log Sources icon.
3. Click Add.
4. In the **Log Source Name** field, type a name for the log source.
5. In the **Log Source Description** field, type a description for the log source.
6. From the Log Source Type list, select **IBM Resource Access Control Faclilty (RACF)**.
7. From the **Protocol Configuration** list, select **Log File**.
8. Configure the following values:

Table 37. IBM RACF log file protocol parameters

Parameter	Description
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow QRadar to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository containing all of your event logs, you should specify a name, IP address, or hostname for the image or location that uniquely identifies events for the IBM RACF log source. This allows events to be identified at the image or location level in your network that your users can identify.

Table 37. IBM RACF log file protocol parameters (continued)

Parameter	Description
Service Type	From the list, select the protocol you want to use when retrieving log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy The underlying protocol used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 to 65535. The options include: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value accordingly.
Remote User	Type the user name or userid necessary to log in to the host containing your event files. • If your log files are located on your IBM z/OS image, type the userid necessary to log in to your IBM z/OS. The userid can be up to 8 characters in length. • If your log files are located on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the Service Type, this parameter allows you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.

Table 37. IBM RACF log file protocol parameters (continued)

Parameter	Description
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. For FTP only. If your log files reside in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) required to filter the list of files specified in the Remote Directory. All matching files are included in the processing. The FTP file pattern you specify must match the name you assigned to your event files. For example, to collect files starting with zOS and ending with .gz, type the following: Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: *http://download.oracle.com/javase/tutorial/essential/regex/*
FTP Transfer Mode	This option only displays if you select FTP as the Service Type. From the list, select the transfer mode you want to apply to this log source: • **Binary** - Select Binary for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files. • **ASCII** - Select ASCII for log sources that require an ASCII FTP file transfer.
SCP Remote File	If you select SCP as the Service Type you must type the file name of the remote file.

Table 37. IBM RACF log file protocol parameters (continued)

Parameter	Description
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.
Processor	None.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. QRadar examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.

Table 37. IBM RACF log file protocol parameters (continued)

Parameter	**Description**
Change Local Directory?	Select this check box to define a local directory on your QRadar system for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

9. Click **Save**.
10. On the **Admin** tab, click **Deploy Changes**.

    The IBM RACF configuration is complete. If your IBM RACF requires custom event properties, see the *IBM Security QRadar Custom Event Properties for IBM z/OS* technical note.

Integrate IBM RACF with QRadar using audit scripts

The IBM Resource Access Control Facility (RACF) DSM for IBM Security QRadar allows you to integrate with an IBM z/OS mainframe using IBM RACF for auditing transactions.

QRadar records all relevant and available information from the event.

Note: zSecure integration is the only integration that provides custom events to the log source. Custom events may be displayed even when you collect events by using the Native QEXRACF integration.

To integrate the IBM RACF events into QRadar:

1. The IBM mainframe system records all security events as Service Management Framework (SMF) records in a live repository.
2. At midnight, the IBM RACF data is extracted from the live repository using the SMF dump utility. The RACFICE utility IRRADU00 (an IBM utility) creates a log file containing all of the events and fields from the previous day in a SMF record format.
3. The QEXRACF program pulls data from the SMF formatted file, as described above. The program only pulls the relevant events and fields for QRadar and writes that information in a condensed format for compatibility. The information is also saved in a location accessible by QRadar.
4. QRadar uses the log file protocol source to pull the QEXRACF output file and retrieves the information on a scheduled basis. QRadar then imports and process this file.

Configure IBM RACF to integrate with QRadar

You can integrate an IBM mainframe RACF with IBM Security QRadar:

Procedure

1. From the IBM support website (*http://www.ibm.com/support)*, download the following compressed file:

   `qexracf_bundled.tar.gz`
2. On a Linux-based operating system, extract the file:

   `tar -zxvf qexracf_bundled.tar.gz`

   The following files are contained in the archive:

   `qexracf_jcl.txt`

   `qexracfloadlib.trs`

   `qexracf_trsmain_JCL.txt`
3. Load the files onto the IBM mainframe using any terminal emulator file transfer method.

   Upload the `qexracf_trsmain_JCL.txt` and `qexracf_jcl.txt` files using the TEXT protocol.

   Upload the `QexRACF loadlib.trs` file using binary mode and append to a pre-allocated data set. The `QexRACF loadlib.trs` file is a tersed file containing the executable (the mainframe program QEXRACF). When you upload the .trs file from a workstation, pre-allocate a file on the mainframe with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL=1024, BLKSIZE=6144. The file transfer type must be binary mode and not text.
4. Customize the `qexracf_trsmain_JCL.txt` file according to your installation-specific requirements.

   The `qexracf_trsmain_JCL.txt` file uses the IBM utility Trsmain to uncompress the program stored in the `QexRACF loadlib.trs` file.

   An example of the `qexracf_trsmain_JCL.txt` file includes:

   ```
   //TRSMAIN   JOB (yourvalidjobcard),Q1labs,  //  MSGCLASS=V //DEL    EXEC
   PGM=IEFBR14 //D1    DD   DISP=(MOD,DELETE),DSN=<yourhlq>.QEXRACF.TRS //
         UNIT=SYSDA, //       SPACE=(CYL,(10,10)) //TRSMAIN EXEC
   PGM=TRSMAIN,PARM='UNPACK' //SYSPRINT  DD
   SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA) //INFILE    DD
   DISP=SHR,DSN=<yourhlq>.QEXRACF.TRS //OUTFILE   DD
   DISP=(NEW,CATLG,DELETE), //          DSN=<yourhlq>.LOAD,  //
   SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA //
   ```

   You must update the file with your installation specific information for parameters, such as, jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

   The .trs input file is an IBM TERSE formatted library and is extracted by running the JCL, which calls the TRSMAIN. This tersed file, when extracted, creates a PDS linklib with the QEXRACF program as a member.
5. You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in the LINKLST. The program does not require authorization.
6. After uploading, copy the program to an existing link listed library or add a STEPLIB DD statement with the correct dataset name of the library that will contain the program.

7. The qexracf_jcl.txt file is a text file containing a sample JCL deck to provide you with the necessary JCL to run the IBM IRRADU00 utility. This allows QRadar to obtain the necessary IBM RACF events. Configure the job card to meet your local standards.

   An example of the qexracf_jcl.txt file includes:

```
//QEXRACF JOB (<your valid jobcard>),Q1LABS, // MSGCLASS=P, //
REGION=0M               //* //*QEXRACF JCL version 1.0 April 2009
//*
//************************************************************** //*
Change below               dataset names to sites specific datasets
names *
//************************************************************** //SET1
SET               SMFOUT='<your hlq>.CUSTNAME.IRRADU00.OUTPUT', //
SMFIN='<your SMF dump ouput               dataset>', // QRACFOUT='<your
hlq>.QEXRACF.OUTPUT'
//************************************************************** //*
Delete old               datasets *
//************************************************************** //DEL
EXEC               PGM=IEFBR14 //DD2 DD DISP=(MOD,DELETE),DSN=&QRACFOUT,
// UNIT=SYSDA, //               SPACE=(TRK,(1,1)), //
DCB=(RECFM=FB,LRECL=80)
//************************************************************** //*
Allocate new               dataset *
//************************************************************** //ALLOC
EXEC               PGM=IEFBR14 //DD1 DD DISP=(NEW,CATLG),DSN=&QRACFOUT,
//               SPACE=(CYL,(1,10)),UNIT=SYSDA, //
DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//************************************************************** //*
Execute IBM               IRRADU00 utility to extract RACF smf records
*
//**************************************************************
//IRRADU00 EXEC               PGM=IFASMFDP //SYSPRINT DD SYSOUT=*
//ADUPRINT DD SYSOUT=* //OUTDD DD               DSN=
&SMFOUT,SPACE=(CYL,(100,100)),DISP=(,CATLG), //
DCB=(RECFM=FB,LRECL=8192,BLKSIZE=40960), // UNIT=SYSALLDA //SMFDATA
DD               DISP=SHR,DSN=&SMFIN //SMFOUT DD DUMMY //SYSIN DD
*                    INDD(SMFDATA,OPTIONS(DUMP))
     OUTDD(SMFOUT,TYPE(30:83))                    ABEND(NORETRY)
     USER2(IRRADU00)      USER3(IRRADU86) /*               //EXTRACT EXEC
PGM=QEXRACF,DYNAMNBR=10, // TIME=1440 //*STEPLIB DD
DISP=SHR,DSN=<the loadlib containing the QEXRACF program if not in
LINKLST>               //SYSTSIN DD DUMMY //SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=* //RACIN DD               DISP=SHR,DSN=&SMFOUT
//RACOUT DD DISP=SHR,DSN=&QRACFOUT //
//************************************************************** //* FTP
Output file               from C program (Qexracf) to an FTP server *
//* QRadar will go to that               FTP Server to get file
           * //* Note you need to replace               <user>,
<password>,<serveripaddr>* //*               <THEIPOFTHEMAINFRAMEDEVICE>
and <QEXRACFOUTDSN>           *
//************************************************************** //*FTP
EXEC               PGM=FTP,REGION=3800K //*INPUT DD *
//*<FTPSERVERIPADDR> //*<USER>               //*<PASSWORD> //*ASCII
```

```
//*PUT '<QEXRACFOUTDSN>'              /<THEIPOFTHEMAINFRAMEDEVICE>/
<QEXRACFOUTDSN> //*QUIT //*OUTPUT DD SYSOUT=*             //*SYSPRINT
DD SYSOUT=* //* //*
```

8. After the output file is created, you must send this file to an FTP server. This ensures that every time you run the utility, the output file is sent to a specific FTP server for processing at the end of the above script. If the z/OS platform is configured to serve files through FTP or SFTP, or allow SCP, then no interim server is required and QRadar can pull those files directly from the mainframe. If an interim FTP server is needed, QRadar requires a unique IP address for each IBM RACF log source or they will be joined as one system.

Chapter 27. IBM Privileged Session Recorder

The IBM Security QRadar DSM for IBM Privileged Session Recorder can collect event logs from your IBM Privileged Session Recorder device.

The following table lists the specifications for the IBM Privileged Session Recorder DSM.

Table 38. IBM Privileged Session Recorder specifications

Specification	Value
Manufacturer	IBM
DSM name	Privileged Session Recorder
RPM filename	DSM-IBMPrivilegedSessionRecorder
Protocol	JDBC
QRadar recorded event types	Command Execution Audit Events
Automatically discovered?	No
Includes identity?	No
More information	IBM website (http://www.ibm.com/)

To collect IBM Privileged Session Recorder events, use the following procedures:

1. If automatic updates are not enabled, download and install the following RPMs on your QRadar Console:
   - Protocol-JDBC RPM
   - IBM Privileged Session Recorder DSM RPM
2. On the IBM Security Privileged Identity Manager dashboard, obtain the database information for the Privileged Session Recorder data store and configure your IBM Privileged Session Recorder DB2 database to allow incoming TCP connections.
3. For each instance of IBM Privileged Session Recorder, create an IBM Privileged Session Recorder log source on the QRadar Console. Use the following table to define the Imperva SecureSphere parameters:

Table 39. IBM Privileged Session Recorder log source parameters

Parameter	Description
Log Source Type	IBM Privileged Session Recorder
Protocol Configuration	JDBC
Log Source Identifier	*DATABASE@HOSTNAME*
Database Type	DB2
Database Name	The Session Recorder data store name that you configured on the IBM Privileged Identity Manager dashboard.
IP or Hostname	The Session Recorder database server address.
Port	The port that is specified on IBM Privileged Identity Manager dashboard.

Table 39. IBM Privileged Session Recorder log source parameters (continued)

Parameter	Description
Username	The DB2 database user name
Password	The DB2 database password
Predefined Query	IBM Privileged Session Recorder
Use Prepared Statements	This option must be selected.
Start Date and Time	The initial date and time for the JDBC retrieval.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring IBM Privileged Session Recorder to communicate with QRadar"
Before you can configure a log source in IBM Privileged Session Recorder for IBM Security QRadar, obtain the database information for the Privileged Session Recorder data store. You must also configure your IBM Privileged Session Recorder DB2 database to allow incoming TCP connections from QRadar.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring IBM Privileged Session Recorder to communicate with QRadar

Before you can configure a log source in IBM Privileged Session Recorder for IBM Security QRadar, obtain the database information for the Privileged Session Recorder data store. You must also configure your IBM Privileged Session Recorder DB2 database to allow incoming TCP connections from QRadar.

IBM Privileged Session Recorder is a component of IBM Security Privileged Identity Manager.

Procedure

1. Log in to the IBM Security Privileged Identity Manager web user interface.
2. Select the **Configure Privileged Identity Manager** tab.
3. Select **Database Server Configuration** in the **Manage External Entities** section.
4. In the table, double-click the **Session Recording data store** row in the **Database Server Configuration** column.
5. 5. Record the following parameters to use when you configure a log source in QRadar:

IBM Privileged Session Recorder Field	QRadar Log Source Field
Hostname	IP or Hostname
Port	Port
Database name	Database Name
Database administrator ID	Username

Chapter 28. IBM Security Network IPS

The IBM Security Network IPS DSM for IBM Security QRadar collects LEEF-based events from IBM Security Network IPS appliances by using the syslog protocol.

The following table identifies the specifications for the IBM Security Network IPS DSM:

Parameter	**Value**
Manufacturer	IBM
DSM	Security Network IPS
RPM file name	DSM-IBMSecurityNetworkIPS-*QRadar_version-Build_number*.noarch.rpm
Supported versions	v4.6 and later (UDP) v4.6.2 and later (TCP)
Protocol	syslog (LEEF)
QRadar recorded events	Security alerts (including IPS and SNORT) Health alerts System alerts IPS events (Including security, connection, user defined, and OpenSignature policy events)
Automatically discovered?	Yes
Includes identity?	No

To integrate the IBM Security Network IPS appliance with QRadar, use the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM Security Network IPS RPMs on your QRadar Console.
2. For each instance of IBM Security Network IPS, configure your IBM Security Network IPS appliance to enable communication with QRadar.
3. If QRadar does not automatically discover the log source, create a log source for each instance of IBM Security Network IPS on your network.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your IBM Security Network IPS appliance for communication with QRadar

To collect events with QRadar, you must configure your IBM Security Network IPS appliance to enable syslog forwarding of LEEF events.

Before you begin

Ensure that no firewall rules block the communication between your IBM Security Network IPS appliance and QRadar.

Procedure

1. Log in to your IPS Local Management Interface.
2. From the navigation menu, select **Manage System Settings** > **Appliance** > **LEEF Log Forwarding**.
3. Select the **Enable Local Log** check box.
4. In the **Maximum File Size** field, configure the maximum file size for your LEEF log file.
5. From the Remote Syslog Servers pane, select the **Enable** check box.
6. In the **Syslog Server IP/Host** field, type the IP address of your QRadar Console or Event Collector.
7. In the **TCP Port** field, type `514` as the port for forwarding LEEF log events.

   Note: If you use v4.6.1 or earlier, use the **UDP Port** field.
8. From the event type list, enable any event types that are forwarded to QRadar.
9. If you use a TCP port, configure the **`crm.leef.fullavp`** tuning parameter:
   a. From the navigation menu, select **Manage System Settings** > **Appliance** > **Tuning Parameters**.
   b. Click **Add Tuning Parameters**.
   c. In the **Name** field, type `crm.leef.fullavp`.
   d. In the **Value** field, type `true`.
   e. Click **OK**.

Configuring an IBM Security Network IPS log source in QRadar

QRadar automatically discovers and creates a log source for syslog events from IBM Security Network IPS appliances. However, you can manually create a log source for QRadar to receive syslog events.

About this task

Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Click **Add**.
4. In the **Log Source Name** field, type a name for your log source.
5. From the **Log Source Type** list, select **IBM Security Network IPS (GX)**.
6. Using the **Protocol Configuration** list, select **Syslog**.
7. Configure the parameters:

Parameter	Description
Log Source Identifier	The IP address or host name for the log source as an identifier for events from your IBM Security Network IPS appliance.
Credibility	The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event.
Coalescing Events	Enables the log source to coalesce (bundle) events.
Incoming Event Payload	The incoming payload encoder for parsing and storing the logs.

8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.

Chapter 29. IBM SmartCloud Orchestrator

The IBM Security QRadar DSM for IBM SmartCloud Orchestrator collects audit logs from the SmartCloud Orchestrator system.

The following table identifies specifications for the IBM SmartCloud Orchestrator DSM.

Table 40. IBM SmartCloud Orchestrator specifications

Specification	Value
Manufacturer	IBM
DSM name	SmartCloud Orchestrator
RPM file name	`DSM-IBMSmartCloudOrchestrator-`*`Qradar_version_build number`*`.noarch.rpm`
Supported versions	V2.3 FP1 and later
Protocol type	IBM SmartCloud Orchestrator REST API
QRadar recorded event types	Audit Records
Log source type in the QRadar UI	IBM SmartCloud Orchestrator
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties	No
More information	http://ibm.com

To integrate IBM SmartCloud Orchestrator with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMS on your QRadar Console:
   - IBM SmartCloud Orchestrator RPM
   - IBM SmartCloud Orchestrator RESTAPI protocol RPM
2. Create an IBM SmartCloud Orchestrator log source on the QRadar Console. Use the following values for the SmartCloud-specific parameters:

Parameter	Description
Log Source Type	IBM SmartCloud Orchestrator.
Protocol Configuration	IBM SmartCloud Orchestrator REST API
IP or Hostname	The IP address or server name of the SmartCloud Orchestrator.

No action is required on the IBM SmartCloud Orchestrator system. After you create the log source, QRadar starts collecting logs from IBM SmartCloud Orchestrator.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM

RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Installing IBM SmartCloud Orchestrator

Integrate SmartCloud Orchestrator with IBM Security QRadar

Procedure

1. Download and install the latest DSMCommon RPM on your QRadar Console. If automatic updates are configured to install DSM updates, this step is not necessary.
2. Download and install the latest IBM SmartCloud Orchestrator RESTAPI Protocol RPM on to your QRadar Console.
3. Download and install the latest IBM SmartCloud Orchestrator RPM on your QRadar Console. If automatic updates are configured to install DSM updates, this step is not necessary.

Configuring an IBM SmartCloud Orchestrator log source in QRadar

To enable IBM SmartCloud Orchestrator integration with IBM Security QRadar, add a log source.

Procedure

1. Log in to QRadar.
2. Select the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon and then click **Add**.
5. From the **Log Source Type** list, select **IBM SmartCloud Orchestrator**.
6. From the **Protocol Configuration** list, select **IBM SmartCloud Orchestrator REST API**.
7. Configure the parameters:

Option	Description
IP or Hostname	The IP address or server name of the SmartCloud Orchestrator.
Username	The user name of the SmartCloud Orchestrator console user.
Password	The password of the SmartCloud Orchestrator console user.
Confirm Password	This option confirms that the password was entered correctly.
EPS Throttle	The maximum number of events per second for this log source (default 5000).
Recurrence	How often this log source attempts to obtain data. Can be in Minutes, Hours, Days (default 5 minutes).

Chapter 30. IBM Tivoli Endpoint Manager

The IBM Security QRadar DSM for IBM Tivoli Endpoint Manager retrieves system events in Log Extended Event Format (LEEF). QRadar uses the IBM Tivoli Endpoint Manager SOAP protocol to retrieve events in 30-second intervals.

The following table lists the specifications for the IBM Tivoli Endpoint Manager DSM:

Table 41. IBM Tivoli Endpoint Manager specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM Tivoli Endpoint Manager

RPM file name	`DSM-IBMTivoliEndpointManager-`
	`Qradar_version-build_number``.noarch.rpm`

Supported versions	8.2.x and later Use the most current version that is available.
Protocol	SOAP
Recorded event types	System events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	IBM website (http://www.ibm.com)

To collect events from IBM Tivoli Endpoint Manager events, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM Tivoli Endpoint Manager RPM on your QRadar Console.
2. Configure your Tivoli Endpoint Manager server to communicate with QRadar:
   a. Install the Web Reports application on the Tivoli Endpoint Manager server.
   b. Create a user account that QRadar can use to access the Relevance database in the Web Reports application.

   Note: For more information, see your IBM Tivoli Endpoint Manager documentation.
3. Create a log source on the QRadar Console. Use the following table to help you configure the parameters that are specific to IBM Tivoli Endpoint Manager:

Table 42. IBM Tivoli Endpoint Manager log source parameters

Parameter	Description
Log Source Type	IBM Tivoli Endpoint Manager
Protocol Configuration	IBM Tivoli Endpoint Manager SOAP
Port	Use Port 80. If you use HTTPS, use port 443.

Table 42. IBM Tivoli Endpoint Manager log source parameters (continued)

Parameter	Description
Use HTTPS	If certificates are required, copy them to the `/opt/qradar/conf/trusted_certificates` directory on your QRadar Console or Event Collector. QRadar supports certificates that have the following file extensions: `.crt`, `.cert`, or `.der`.
Username	The user account must have access to the Relevance database in the Web Reports application.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Chapter 31. IBM Security Trusteer Apex Advanced Malware Protection

The IBM Security Trusteer Apex Advanced Malware Protection DSM collects event data from a Trusteer Apex Advanced Malware Protection system.

IBM Security QRadar can either collect:

- Syslog events directly from the Trusteer Apex Advanced Malware Protection system.
- Log files from an intermediary server that hosts flat feed files from the Trusteer Apex Advanced Malware Protection system.

The following table lists the specifications for the IBM Security Trusteer Apex Advanced Malware Protection DSM:

Table 43. IBM Security Trusteer Apex Advanced Malware Protection DSM specifications

Specification	**Value**
Manufacturer	IBM
DSM name	IBM Security Trusteer Apex Advanced Malware Protection
RPM file name	`DSM-TrusteerApex-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	Apex Local Manager V2.0.34 and later for the syslog/LEEF event collection. The LEEF version is `ver_1303.1` and later V1 and later for Flat File Feed
Protocol	Syslog/LEEF Log File
Recorded event types	Malware Detection Exploit Detection Data Exfiltration Detection Lockdown for Java Event File Inspection Event Apex Stopped Event Apex Uninstalled Event Policy Changed Event ASLR Violation Event ASLR Enforcement Event Password Protection Event
Automatically discovered?	Yes
Includes identity?	No

Table 43. IBM Security Trusteer Apex Advanced Malware Protection DSM specifications (continued)

Specification	Value
Includes custom properties?	No
More information	IBM Security Trusteer Apex Advanced Malware Protection website (http://www-03.ibm.com/software/products/en/trusteer-apex-adv-malware)

To configure IBM Security Trusteer Apex Advanced Malware Protection event collection, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - Log File Protocol RPM
   - IBM Security Trusteer Apex Advanced Malware Protection DSM RPM
2. Choose one of the following options:
   - To send syslog events to QRadar, see "Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar" on page 98.
   - To collect log files from IBM Security Trusteer Apex Advanced Malware Protection through an intermediary server, see "Configuring a Flat File Feed service" on page 98.
3. If QRadar does not automatically discover the log source, add an IBM Security Trusteer Apex Advanced Malware Protection log source on the QRadar Console.

   The following table describes the parameters that require specific values for IBM Security Trusteer Apex Advanced Malware Protection syslog event collection:

Table 44. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for syslog

Parameter	Value
Log Source type	**IBM Security Trusteer Apex Advanced Malware Protection**
Protocol Configuration	**Syslog**
Log Source Identifier	The IP address or host name from in syslog header. If the syslog header does not contain an IP address or host name, use the packet IP address.

The following table describes the parameters that require specific values for IBM Security Trusteer Apex Advanced Malware Protection Log File collection:

Table 45. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Log File Protocol

Parameter	Value
Log Source type	**IBM Security Trusteer Apex Advanced Malware Protection**
Protocol Configuration	**Log File**

Table 45. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Log File Protocol (continued)

Parameter	**Value**
Log Source Identifier	The IP address or host name of the server that hosts the flat feed files.
Service Type	**SFTP**
Remote IP or Hostname	The IP address or host name of the server that hosts the flat feed files..
Remote Port	`22`
Remote User	The user name that you created for QRadar on the server that hosts the flat feed files.
SSH Key File	If you use a password, you can leave this field blank.
Remote Directory	The log file directory where the flat feed files are stored.
Recursive	Do not select this option.
FTP File Pattern	`"trusteer_feeds_.*?_[0-9]{8}_[0-9]*?\.csv"`
Start Time	The time that you want your log file protocol to start log file collection.
Recurrence	The polling interval for log file retrieval.
Run On Save	Must be enabled.
Processor	**None**
Ignore Previously Processed Files	Must be enabled.
Event Generator	**LINEBYLINE**
File Encoding	**UTF-8**

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar" on page 98
Configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to IBM Security QRadar.

"Configuring a Flat File Feed service" on page 98
For IBM Security QRadar to retrieve log files from IBM Security TrusteerApex Advanced Malware Protection, you must set up a flat file feed service on an intermediary SFTP-enabled server. The service enables the intermediary server to host the flat files that it receives from IBM Security TrusteerApex Advanced Malware Protection and allows for connections from external devices so that QRadar can retrieve the log files.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar

Configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to IBM Security QRadar.

Before you begin

Install an Apex Local Manager on your Trusteer Management Application (TMA).

For more information about configuring your IBM Security Trusteer Apex Advanced Malware Protection to communicate with QRadar, use the following documentation from the IBM Knowledge Center:

- *IBM Security Trusteer Apex Advanced Malware Protection Local Manager - Hybrid Solution Reference Guide*
- *IBM Security Trusteer Apex Advanced Malware Protection Feeds Reference Guide*

SSL/TLS authentication is not supported.

Procedure

1. Log in to Trusteer Management Application (TMA).
2. Select **Apex Local Manager & SIEM Settings**.
3. Optional: If the Apex Local Manager wizard does not automatically display, click **Add**.
4. Type the name of the Apex Local Manager.
5. Check the **Enable** box and click **Next**.
6. Type the server settings for QRadar and click **Next**.
7. Optional: If you use a separate syslog server for the Apex Local Manager system events, type the settings.
8. Click **Finish**.

Configuring a Flat File Feed service

For IBM Security QRadar to retrieve log files from IBM Security TrusteerApex Advanced Malware Protection, you must set up a flat file feed service on an intermediary SFTP-enabled server. The service enables the intermediary server to host the flat files that it receives from IBM Security TrusteerApex Advanced Malware Protection and allows for connections from external devices so that QRadar can retrieve the log files.

To configure IBM Security TrusteerApex Advanced Malware Protection to send flat file feed to the intermediary server, contact IBM Trusteer support.

Before you begin

About this task

Flat File Feeds use a CSV format. Each feed item is written to the file on a separate line, which contains several comma-separated fields. Each field contains data that describes the feed item. The first field in each feed line contains the feed type.

Procedure

1. Enable an SFTP-enabled server and ensure that external devices can reach it.
2. Log on to the SFTP-enabled server.
3. Create a user account on the server for IBM Security Trusteer Apex Advanced Malware Protection.
4. Create a user account for QRadar.
5. Optional: Enable SSH key-based authentication.

What to do next

After you set up the intermediary server, record the following details:

- Target SFTP server name and IP addresses
- SFTP server port (standard port is 22)
- The file path for the target directory
- SFTP user name if SSH authentication is not configured
- Upload frequency (from 1 minute to 24 hours)
- SSH public key in RSA format

IBM Trusteer support uses the intermediary server details when they configure IBM Security TrusteerApex Advanced Malware Protection to send flat feel files..

Chapter 32. IBM WebSphere DataPower

The IBM Security QRadar DSM collects event logs from your IBM WebSphere DataPower system.

The following table identifies the specifications for the IBM WebSphere DataPower DSM.

Table 46. IBM WebSphere DataPower DSM specifications

Specification	Value
Manufacturer	IBM
DSM Name	WebSphere DataPower
RPM file name	`DSM-IBMWebSphereDataPower-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	FirmwareV6 and V7
Protocol	Syslog
QRadar recorded event types	All Events
Log source type in QRadar UI	IBM WebSphere DataPower
Auto discovered?	Yes
Includes identity?	No
Includes custom properties?	No
For more information	IBM web page (http://www.ibm.com/)

To send events from IBM WebSphere DataPower to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM WebSphere DataPower DSM on your QRadar Console.
2. For each instance of IBM WebSphere DataPower, configure the IBM WebSphere DataPower system to communicate with QRadar.
3. If QRadar does not automatically discover IBM WebSphere DataPower, create a log source for each instance of IBM WebSphere DataPower on the QRadar Console. Use the following IBM Websphere DataPower specific values:

Parameter	Value
Log Source Type	IBM WebSphere DataPower
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring IBM WebSphere DataPower to communicate with QRadar" on page 102
To collect IBM WebSphere DataPower events, configure your third-party system to send events to IBM Security QRadar.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring IBM WebSphere DataPower to communicate with QRadar

To collect IBM WebSphere DataPower events, configure your third-party system to send events to IBM Security QRadar.

Before you begin

Review the DataPower logging documents to determine which logging configuration changes are appropriate for your deployment. See IBM Knowledge Center (http://www-01.ibm.com/support/knowledgecenter/SS9H2Y_7.0.0/com.ibm.dp.xi.doc/logtarget_logs.html?lang=en).

Procedure

1. Log in to your IBM WebSphere DataPower system.
2. In the search box on the left navigation menu, type `Log Target`.
3. Select the matching result.
4. Click **Add**.
5. In the **Main** tab, type a name for the log target.
6. From the **Target Type** list, select **syslog**.
7. In the **Local Identifier** field, type an identifier to be displayed in the **Syslog event payloads** parameter on the QRadar user interface.
8. In the **Remote Host** field, type the IP address or host name of your QRadar Console or Event Collector.
9. In the **Remote Port** field, type `514`.
10. Under **Event Subscriptions**, add a base logging configuration with the following parameters:

Parameter	Value
Event Category	`all`
Minimum Event Priority	`warning` **Important:** To prevent a decrease in system performance, do not use more than one word for the **Minimum Event Priority** parameter.

11. Apply the changes to the log target.
12. Review and save the configuration changes.

Chapter 33. Kaspersky Security Center

The IBM Security QRadar DSM for Kaspersky Security Center can retrieve events directly from a database on your Kaspersky Security Center appliance or receive events from the appliance by using syslog.

The following table identifies the specifications for the Kaspersky Security Center DSM:

Table 47. Kaspersky Security Center DSM specifications

Specification	**Value**
Manufacturer	Kaspersky
DSM name	Kaspersky Security Center
RPM file name	`DSM-KasperskySecurityCenter-`*`Qradar_version-build_number`*`.noarch.rpm`
Protocol	JDBC: Versions 9.2-10.1 Syslog LEEF: Version 10.1 and later
Recorded event types	Antivirus Server Audit
Automatically discovered?	No, if you use the JDBC protocol Yes, if you use the syslog protocol
Includes identity?	Yes
Includes custom properties?	No
More information	Kaspersky website (http://www.kaspersky.com)

To send Kaspersky Security Center events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - Kaspersky Security Center DSM
2. Choose one of the following options:
   - If you use syslog, configure your Kaspersky Security Center to forward events to QRadar.
   - If you use the JDBC protocol, create a database view on your Kaspersky Security Center device.
3. Create a Kaspersky Security Center log source on the QRadar Console. Configure all required parameters, and use the following tables to configure the specific values that are required for Kaspersky Security Center event collection.
   - If you use syslog, configure the following parameters:

Table 48. Kaspersky Security Center syslog log source parameters

Parameter	Value
Log Source type	Kaspersky Security Center
Protocol Configuration	Syslog

- If you use JDBC, configure the following parameters:

Table 49. Kaspersky Security Center JDBC log source parameters

Parameter	Value
Log Source type	Kaspersky Security Center
Protocol Configuration	JDBC
Log Source Identifier	Use the following format: `<Kaspersky_Database>@<Server_Address>` Where the <*Server_Address*> is the IP address or host name of the Kaspersky database server.
Database Type	MSDE
Database Name	KAV
IP or Hostname	The IP address or host name of the SQL server that hosts the Kaspersky Security Center database.
Port	The default port for MSDE is 1433. You must enable and verify that you can communicate by using the port you specified in the **Port** field. The JDBC configuration port must match the listener port of the Kaspersky database. To be able to communicate with QRadar, the Kaspersky database must have incoming TCP connections enabled . If you define a database instance that uses MSDE as the database type, you must leave the **Port** parameter blank in your configuration.
Table Name	dbo.events

For more information about the JDBC protocol parameters, see the *Log Sources User Guide*

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Exporting syslog to QRadar from Kaspersky Security Center" on page 106
Configure Kaspersky Security Center to forward syslog events to your IBM Security QRadar Console or Event Collector.

"Creating a database view for Kaspersky Security Center for JDBC event collection" on page 105
To use the JDBC protocol to collect audit event data, you must create a database view on your Kaspersky server that IBM Security QRadar can access.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Creating a database view for Kaspersky Security Center for JDBC event collection

To use the JDBC protocol to collect audit event data, you must create a database view on your Kaspersky server that IBM Security QRadar can access.

Before you begin

Create a Kaspersky Security Center user for QRadar who can poll the database for events.

Ensure that QRadar can poll the database for events on TCP port 1433 or the port that is configured for your log source. Protocol connections are often disabled on databases by default and extra configuration steps might be required to allow connections for event polling. Configure any firewalls that are located between Kaspersky Security Center and QRadar to allow traffic for event polling.

Procedure

1. Download the `klsql2.zip` file from the Kaspersky Labs (http://support.kaspersky.com/9284) website.
2. Copy the `klsql2.zip` file to your Kaspersky Security Center Administration Server.
3. Extract the `klsql2.zip` file to a directory.
4. In any text editor, edit the `src.sql` file to clear the contents.
5. Type the following statement to create the database view:

   Tip: If you copy and paste this statement, ensure that you remove any line breaks from your pasted text.

   ```
   create view dbo.events as select e.nId, e.strEventType as 'EventId',
   e.wstrDescription as 'EventDesc', e.tmRiseTime as 'DeviceTime', h.nIp as
   'SourceInt', e.wstrPar1, e.wstrPar2, e.wstrPar3, e.wstrPar4, e.wstrPar5,
   e.wstrPar6, e.wstrPar7, e.wstrPar8, e.wstrPar9 from dbo.v_akpub_ev_event
   e, dbo.v_akpub_host h where e.strHostname = h.strName;
   ```
6. Save the `src.sql` file.
7. Go to the directory that contains the `klsql2` files.
8. To create the database view on your Kaspersky Security Center appliance, type the following command:

   ```
   klsql2 -i src.sql -o result.xml
   ```

Results

The database view is named `dbo.events`. You will use this value when you configure a Kaspersky Security Center log source in QRadar.

Related tasks:

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Exporting syslog to QRadar from Kaspersky Security Center

Configure Kaspersky Security Center to forward syslog events to your IBM Security QRadar Console or Event Collector.

About this task

Kaspersky Security Center can forward events that are registered on the Administration Server, Administration Console, and Network Agent appliances.

Procedure

1. Log in to Kaspersky Security Center.
2. In the console tree, expand the **Reports and notifications** folder.
3. Right-click **Events** and select **Properties**.
4. In the Exporting events pane, select the **Automatically export events to SIEM system database** check box.
5. In the **SIEM system** list, select **QRadar**.
6. Type the IP address and port for the QRadar Console or Event Collector.
7. Optional: To forward historical data to QRadar, click **Export archive** to export historical data.
8. Click **OK**.

Chapter 34. Kisco Information Systems SafeNet/i

The IBM Security QRadar DSM for Kisco Information Systems SafeNet/i collects event logs from IBM iSeries systems.

The following table identifies the specifications for the Kisco Information Systems SafeNet/i DSM:

Table 50. Kisco Information Systems SafeNet/i DSM specifications

Specification	Value
Manufacturer	Kisco Information Systems
DSM name	Kisco Information Systems SafeNet/i
RPM file name	`DSM-KiscoInformationSystemsSafeNetI-` *`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V10.11
Protocol	Log File
Recorded event types	All events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Kisco Information Systems website (http://www.kisco.com/safenet/summary.htm)

To collect Kisco Information Systems SafeNet/i events, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - Log File Protocol RPM
   - Kisco Information Systems SafeNet/i DSM RPM
2. Configure your Kisco Information Systems SafeNet/i device to communicate with QRadar.
3. Add a Kisco Information Systems SafeNet/i log source on the QRadar Console. The following table describes the parameters that require specific values for Kisco Information Systems SafeNet/i event collection:

Table 51. Kisco Information Systems SafeNet/i log source parameters

Parameter	Value
Log Source type	Kisco Information Systems SafeNet/i
Protocol Configuration	Log File
Service Type	FTP
Remote IP or Hostname	The IP or host name of Kisco Information systems SafeNet/i device.
Remote Port	21

Table 51. Kisco Information Systems SafeNet/i log source parameters (continued)

Parameter	Value
Remote User	The iSeries User ID that you created for QRadar in Kisco Information Systems SafeNet/i.
Remote Directory	Leave this field empty.
FTP File Pattern	`.*`
FTP Transfer Mode	BINARY
Processor	NONE
Event Generator	LINEBYLINE
File Encoding	US-ASCII

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring Kisco Information Systems SafeNet/i to communicate with QRadar"
To collect SafeNet/i events, configure your IBM iSeries system to accept FTP GET requests from your QRadar through Kisco Information Systems SafeNet/i.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring Kisco Information Systems SafeNet/i to communicate with QRadar

To collect SafeNet/i events, configure your IBM iSeries system to accept FTP GET requests from your QRadar through Kisco Information Systems SafeNet/i.

About this task

Use the following table when you configure the FTP access settings:

Table 52. FTP access settings

Parameter	Value
Initial Name Format	*PATH
Initial List Format	*UNIX
Initial Library	*USRPRF
Initial Home Directory Path	The IFS directory

Procedure

1. Create an IFS directory on your IBM iSeries system.
   a. Log in to your IBM iSeries system.
   b. Create an IFS Directory to hold the Kisco Information Systems SafeNet/i QRadar alert files.

      Example: `/SafeNet/QRadar/`
   c. Set up a user profile for QRadar to use to FTP into the IFS Directory through SafeNet/i.

Example: QRADARUSER

2. Configure FTP access for the QRadar user profile.
   a. Log in to Kisco Information Systems SafeNet/i.
   b. Type **GO SN7** and select **Work with User to Server Security**.
   c. Type the user profile name that you created for QRadar, for example, QRADARUSER.
   d. Type 1 for the **FTP Server Request Validation *FTPSERVER** and **FTP Server Logon *FTPLOGON3** servers.
   e. Press F3 and select **Work with User to FTP Statement Security** and type the user profile name again.
   f. Type 1 for the **List Files** and **Receiving Files** FTP operations.
   g. Press F4 and configure FTP access parameters for the user. See Table 52 on page 108.
   h. Press F3 and select **Work with User to Long Paths**.
   i. Press F6 and provide the path to the IFS directory.

      Ensure that the path is followed by an asterisk, for example, /SafeNet/QRadar/*
   j. Type X under the **R** column.
   k. Press F3 to exit.
3. Type CHGRDRSET and then press F4.
4. Configure the following parameters:

Paramter	Value
Activate QRADAR Integration	Yes
This Host Identifier	The IP address or host name of the IBM iSeries device.
IFS Path to QRADAR Alert File	Use the following format: /SafeNet/QRadar/

5. Type CHGNOTIFY and press F4.
6. Configure the following parameters:

Parameter	Value
Alert Notification Status	On
Summarized Alerts?	Yes

Chapter 35. Lastline Enterprise

The IBM Security QRadar DSM for Lastline Enterprise receives anti-malware events from Lastline Enterprise systems.

The following table identifies the specifications for the Lastline Enterprise DSM:

Table 53. Lastline Enterprise DSM specifications

Specification	Value
Manufacturer	Lastline
DSM name	Lastline Enterprise
RPM file name	`DSM-LastlineEnterprise-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	6.0
Protocol	LEEF
Recorded event types	Anti-malware
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Lastline website (http://www.lastline.com/platform/enterprise)

To send Lastline Enterprise events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - Lastline Enterprise DSM RPM
2. Configure your Lastline Enterprise device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Lastline Enterprise log source on the QRadar Console. The following table describes the parameters that require specific values that are required for Lastline Enterprise event collection:

Table 54. Lastline Enterprise log source parameters

Parameter	Value
Log Source type	Lastline Enterprise
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring Lastline Enterprise to communicate with QRadar" on page 112
On the Lastline Enterprise system, use the SIEM settings in the notification interface to specify a SIEM appliance where Lastline can send events.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring Lastline Enterprise to communicate with QRadar

On the Lastline Enterprise system, use the SIEM settings in the notification interface to specify a SIEM appliance where Lastline can send events.

Procedure

1. Log in to your Lastline Enterprise system.
2. On the sidebar, click **Admin**.
3. Click **Reporting > Notifications**.
4. To add a notification, click the **Add a notification** (+) icon.
5. From the **Notification Type** list, select **SIEM**.
6. In the SIEM Server Settings pane, configure the parameters for your QRadar Console or Event Collector. Ensure that you select **LEEF** from the **SIEM Log Format** list.
7. Configure the triggers for the notification:
   a. To edit existing triggers in the list, click the **Edit trigger** icon, edit the parameters, and click **Update Trigger**.
   b. To add a trigger to the list, click the **Add Trigger** (+) icon, configure the parameters, and click **Add Trigger**.
8. Click **Save**.

Chapter 36. McAfee ePolicy Orchestrator

The IBM Security QRadar for McAfee ePolicy Orchestrator can collect event logs from your McAfee ePolicy Orchestrator device.

The following table identifies the specifications for the McAfee ePolicy Orchestrator DSM:

Table 55. McAfee ePolicy Orchestrator

Specification	Value
Manufacturer	McAfee
DSM name	McAfee ePolicy Orchestrator
RPM file name	DSM-McAfeeEpo-*QRadar_version-build_number*.noarch.rpm
Supported versions	V3.5 to V5.x
Protocol type	JDBC SNMPv2 SNMPv3
QRadar recorded event types	AntiVirus events
Automatically discovered?	No
Included identity?	No
More information	http://www.mcafee.com (http://www.mcafee.com)

To integrate McAfee ePolicy Orchestrator with QRadar, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the McAfee ePolicy Orchestrator DSM RPM.
2. Configure your McAfee ePolicy Orchestrator DSM device to enable communication with QRadar. Use one of the following options:
   - To integrate
3. Create an McAfee ePolicy Orchestrator DSM log source on the QRadar Console.

Configuring a McAfee ePO log source by using the JDBC protocol

Configure QRadar to access the ePO database by using the JDBC protocol.

Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Click **Add**.
4. In the **Log Source Name** field, type a name for your McAfee ePolicy Orchestrator log source.
5. From the **Log Source Type** list, select **McAfee ePolicy Orchestrator**.
6. From the Protocol Configuration list, select **JDBC**.

7. Configure the following log source parameters:

Option	Description

Log Source Identifier	The identifier for the log source in the following format:
	`<McAfee ePO Database>@`
	`<McAfee ePO Database Server IP or Host Name>`
	When you define a name for your log source identifier, you must use the values of the McAfee ePO Database and Database Server IP address or hostname from the ePO Management Console.

Database Type	MSDE
Database Name	The name of the McAfee ePolicy Orchestrator database.
IP or Hostname	The IP address or host name of the McAfee ePolicy Orchestrator SQL Server.
Port	The port number that the database server uses The port must match the listener port of the McAfee ePolicy Orchestrator database. The McAfee ePolicy Orchestrator database must have incoming TCP connections enabled to communicate with QRadar. If you select MSDE from the Database Type list, leave the Port parameter blank.
Authentication Domain	If you select MSDE from the Database Type list and the database is configured for Windows, you must define this parameter. Otherwise, leave this parameter blank.
Authentication Domain	If you select MSDE from the Database Type list and the database is configured for Windows, you must define this parameter. Otherwise, leave this parameter blank.
Database Instance	Optional. The database instance, if you have multiple SQL server instances on your database server. If you use a non-standard port in your database configuration, or have blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.
Table Name	Type a table or view that includes the event records as follows: • For ePO 3.x, type Events. • For ePO 4.x, type EPOEvents. • For ePO 5.x, type EPOEvents
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if required for your configuration. The list must contain the field defined in the Compare Field parameter.
Compare Field	To identify new events added between queries to the table, type AutoID.

Option	Description
Start Date and Time	Optional. Type the start date and time for database polling in the following format: yyyy-MM-dd HH:mm with HH specified using a 24 hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Prepared statements allow the JDBC protocol source to set up the SQL statement once, and then run the SQL statement many times with different parameters. For security and performance reasons, use prepared statements. If you clear this check box, use an alternative query method that does not use pre-compiled statements.
Polling Interval	The polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. To define a longer polling interval, append H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values entered without an H or M 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	Clear the Use Named Pipe Communications check box.
Database Cluster Name	If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

8. Click Save.
9. On the Admin tab, click Deploy Changes.

Configuring ePO to forward SNMP events

To configure ePO to forward SNMP events, you must configure your McAfee ePolicy Orchestrator device to send SNMP trap notifications and QRadar to receive them.

About this task

Procedure

1. Add a registered server.
2. Configure the SNMP trap notifications on your ePO device.
3. Configure the log source and protocol in QRadar.
4. Optional: Install the Java Cryptography Extension for high-level SNMP decryption algorithms.

Adding a registered server to McAfee ePO

To configure ePO to forward SNMP events, you must add a registered server to McAfee EPO.

Procedure

1. Log in to your McAfee ePolicy Orchestrator console.
2. Select **Menu** > **Configuration** > **Registered Servers**.

3. Click **New Server**.
4. From the **Server Type** menu, select **SNMP Server**.
5. Type the name and any additional notes about the SNMP server, click **Next**.
6. From the **Address** list, select the type of server address that you are using and type the name or IP address.
7. From the **SNMP Version** list, select the SNMP version to use:
   - If you use SNMPv2c, you must provide the Community name.
   - If you use SNMPv3, you must provide the SNMPv3 Security details.
8. To verify the SNMP configuration, click **Send Test Trap**.
9. Click **Save**.

Configuring ePO to forward SNMP events

To configure ePO to forward SNMP events, you must configure your McAfee ePolicy Orchestrator device to send SNMP trap notifications and QRadar to receive them.

About this task

Procedure

1. Add a registered server.
2. Configure the SNMP trap notifications on your ePO device.
3. Configure the log source and protocol in QRadar.
4. Optional: Install the Java Cryptography Extension for high-level SNMP decryption algorithms.

Configuring a McAfee ePO log source by using the SNMP protocol

Configure QRadar to access the ePO database by using the SNMP protocol.

Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Click **Add**.
4. In the **Log Source Name** field, type a name for your McAfee ePolicy Orchestrator log source.
5. From the **Log Source Type** list, select **McAfee ePolicy Orchestrator**.
6. From the **Protocol Configuration** list, select either **SNMPv2** or **SNMPv3**.
7. If you chose SNMPv2, configure the following log source parameters:

Option	Description
Log Source Identifier	The unique IP address for the log source.
Community	The SNMP community string for the SNMPv2 protocol, such as Public.
Include OIDs in Event Payload	Select this check box to allow the McAfee ePO event payloads to be constructed by using name-value pairs instead of the standard event payload format.

8. If you chose SNMPv3, configure the following log source parameters:

Option	Description
Log Source Identifier	The unique IP address for the log source.
Authentication Protocol	The algorithm that you want to use to authenticate SNMPv3 traps: • **SHA** uses Secure Hash Algorithm (SHA) as your authentication protocol. • **MD5** uses Message Digest 5 (MD5) as your authentication protocol.
Include OIDs in Event Payload	Select this check box to allow the McAfee ePO event payloads to be constructed by using name-value pairs instead of the standard event payload format.
Authentication Password	The password to authenticate SNMPv3. Your authentication password must include a minimum of 8 characters.
Decryption Protocol	The algorithm to decrypt the SNMPv3 traps: • DES • AES128 • AES192 • AES256 If you select AES192 or AES256 as your decryption algorithm, you must install the Java Cryptography Extension. For more information, see Installing the Java Cryptography Extension.
Decryption Password	The password to decrypt SNMPv3 traps. Your decryption password must include a minimum of 8 characters.
User	The user access for this protocol.
Include OIDs in Event Payload	Select this check box to allow the McAfee ePO event payloads to be constructed as name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events for McAfee ePO.

9. Click **Save**.
10. On the **Admin** tab, click **Deploy Changes**.

Installing the Java Cryptography Extension on McAfee ePO

The Java™ Cryptography Extension (JCE) is a Java framework that is required for QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your McAfee ePO appliance.

Procedure

1. Download the latest version of the JavaTM Cryptography Extension from the following website:

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

   The JavaTM Cryptography Extension version must match the version of the Java™ installed on your McAfee ePO appliance.

2. Copy the JCE compressed file to the following directory on your McAfee ePO appliance:

   ```
   <installation path to McAfee ePO>/jre/lib/security
   ```

Installing the Java Cryptography Extension on QRadar

The Java™ Cryptography Extension (JCE) is a Java framework that is required for QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your QRadar appliance.

Procedure

1. Download the latest version of the JavaTM Cryptography Extension from the following website:

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

   The JavaTM Cryptography Extension version must match the version of the Java™ installed on QRadar.
2. Extract the JCE file.

   The following Java archive (JAR) files are included in the JCE download:
   - local_policy.jar
   - US_export_policy.jar
3. Log in to your QRadar Console or Event Collector as a root user.
4. Copy the JCE jar files to the following directory on your QRadar Console or Event Collector:

   ```
   /usr/java/latest/jre/lib/
   ```

Results

The JCE jar files are only copied to the system that receives the AES192 or AE256 encrypted files from McAfee ePolicy Orchestrator.

Supported parameters for event detection

The following event detection parameters are available, based on your version of McAfee ePolicy Orchestrator.

Table 56. Supported event detection parameters

Available Types	Selected Types	ePO version
Detected UTC	{lisOfDetectedUTC}	4.5
Received UTC	{listOfReceivedUTC}	4.5
Detecting Prodcut IPv4 Address	{listOfAnalyzerIPV4}	4.5
Detecting Product IPV6 Address	{listOfAnalyzerIPV6}	4.5
Detecting Product MAC Address	{listOfAnalyzerMAC}	4.5
Source PV4 Address	{listOfSourceIPV4}	4.5
Source IPv6 Address	{listOfSourceIPV6}	4.5
Source MAC Address	{listOfSourceMAC}	4.5
Source User Name	{listOfSoureUserName}	4.5

Table 56. Supported event detection parameters (continued)

Available Types	Selected Types	ePO version
Target IPv4 Address	{listOfTargetIPV4}	4.5
Target IPv6 Address	{listOfTargetIPV6}	4.5
Target MAC	{listOfTargetMAC}	4.5
Target Port	{listOfTargetPort}	4.5
Threat Event ID	{listOfThreatEventID}	4.5
Threat Severity	{listOfThreatSeverity}	4.5
SourceComputers		4.0
AffectedComputerIPs		4.0
EventIDs		4.0
TimeNotificationSent		4.0

Chapter 37. LOGbinder EX event collection from Microsoft Exchange Server

The IBM Security QRadar DSM for Microsoft Exchange Server can collect LOGbinder EX V2.0 events.

The following table identifies the specifications for the Microsoft Exchange Server DSM when the log source is configured to collect LOGbinder EX events:

Table 57. LOGbinder for Microsoft Exchange Server

Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft Exchange Server
RPM file name	DSM-MicrosoftExchange-*QRadar_version-build_number*.noarch.rpm
Supported versions	LOGbinder EX V2.0
Protocol type	Syslog LEEF
QRadar recorded event types	Admin Mailbox
Automatically discovered?	Yes
Included identity?	No
More information	Microsoft Exchange website (http://www.office.microsoft.com/en-us/exchange/)

The Microsoft Exchange Server DSM can collect other types of events. For more information on how to configure for other Microsoft Exchange Server event formats, see the Microsoft Exchange Server topic in the *DSM Configuration Guide*.

To collect LOGbinder events from Microsoft Exchange Server, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs:
   - DSMCommon RPM
   - Microsoft Exchange Server DSM RPM
2. Configure your LOGbinder EX system to send Microsoft Exchange Server event logs to QRadar.
3. If the log source is not automatically created, add a Microsoft Exchange Server DSM log source on the QRadar Console. The following table describes the parameters that require specific values that are required for LOGbinder EX event collection:

Table 58. Microsoft Exchange Server log source parameters for LOGbinder event collection

Parameter	Value
Log Source type	Microsoft Exchange Server
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your LOGbinder EX system to send Microsoft Exchange event logs to QRadar

To collect Microsoft Exchange LOGbinder events, you must configure your LOGbinder EX system to send events to IBM Security QRadar.

Before you begin

Configure LOGbinder EX to collect events from your Microsoft Exchange Server. For more information, see your LOGbinder EX documentation.

Procedure

1. Open the LOGbinder EX Control Panel.
2. Double-click **Output** in the Configure pane.
3. Choose one of the following options:
   - Configure for Syslog-Generic output:
     a. In the Outputs pane, double-click **Syslog-Generic**.
     b. Select the **Send output to Syslog-Generic** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
   - Configure for Syslog-LEEF output:
     a. In the Outputs pane, double-click **Syslog-LEEF**.
     b. Select the **Send output to Syslog-LEEF** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
4. Click **OK**.
5. To restart the LOGbinder service, click the **Restart** icon.

Chapter 38. LOGbinder SP event collection from Microsoft SharePoint

The IBM Security QRadar DSM for Microsoft SharePoint can collect LOGbinder SP events.

The following table identifies the specifications for the Microsoft SharePoint DSM when the log source is configured to collect LOGbinder SP events:

Table 59. LOGbinder for Microsoft SharePoint specifications

Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft SharePoint
RPM file name	`DSM-MicrosoftSharePoint-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	LOGbinder SP V4.0
Protocol type	Syslog LEEF
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	No
More information	*http://office.microsoft.com/en-sg/sharepoint/* (http://office.microsoft.com/en-sg/sharepoint/) *http://www.logbinder.com/products/logbindersp/* (http://www.logbinder.com/products/logbindersp/)

The Microsoft SharePoint DSM can collect other types of events. For more information about other Microsoft SharePoint event formats, see the Microsoft SharePoint topic in the *DSM Configuration Guide*.

To collect LOGbinder events from Microsoft SharePoint, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs:
   - DSMCommon RPM
   - Microsoft SharePoint DSM RPM
2. Configure your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar.
3. If the log source is not automatically created, add a Microsoft SharePoint DSM log source on the QRadar Console. The following table describes the parameters that require specific values that are required for LOGbinder event collection:

Table 60. Microsoft SharePoint log source parameters for LOGbinder event collection

Parameter	Value
Log Source type	Microsoft SharePoint
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar"
To collect Microsoft SharePoint LOGbinder events, you must configure your LOGbinder SP system to send events to IBM Security QRadar.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar

To collect Microsoft SharePoint LOGbinder events, you must configure your LOGbinder SP system to send events to IBM Security QRadar.

Procedure

1. Open the LOGbinder SP Control Panel.
2. Double-click **Output** in the Configure pane.
3. Choose one of the following options:
   - Configure for Syslog-Generic output:
     a. In the Outputs pane, double-click **Syslog-Generic**.
     b. Select the **Send output to Syslog-Generic** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
   - Configure for Syslog-LEEF output:
     a. In the Outputs pane, double-click **Syslog-LEEF**.
     b. Select the **Send output to Syslog-LEEF** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
4. Click **OK**.
5. To restart the LOGbinder service, click the **Restart** icon.

Chapter 39. LOGbinder SQL event collection from Microsoft SQL Server

The IBM Security QRadar DSM for Microsoft SQL Server can collect LOGbinder SQL events.

The following table identifies the specifications for the Microsoft SQL Server DSM when the log source is configured to collect LOGbinder SQL events:

Table 61. LOGbinder for Microsoft SQL Server specifications

Specification	Value
Manufacturer	Microsoft
DSM name	Microsoft SQL Server
RPM file name	`DSM-MicrosoftSQL-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	LOGBinder SQL V2.0
Protocol type	Syslog
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	Yes
More information	LogBinder SQL website (http://www.logbinder.com/products/logbindersql/) Microsoft SQL Server website (http://www.microsoft.com/en-us/server-cloud/products/sql-server/)

The Microsoft SQL Server DSM can collect other types of events. For more information about other Microsoft SQL Server event formats, see the Microsoft SQL Server topic in the *DSM Configuration Guide*.

To collect LOGbinder events from Microsoft SQL Server, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs:
   - DSMCommon RPM
   - Microsoft SQL Server DSM RPM
2. Configure your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar.
3. If the log source is not automatically created, add a Microsoft SQL Server DSM log source on the QRadar Console. The following table describes the parameters that require specific values that are required for LOGbinder event collection:

Table 62. Microsoft SQL Server log source parameters for LOGbinder event collection

Parameter	Value
Log Source type	Microsoft SQL Server

Table 62. Microsoft SQL Server log source parameters for LOGbinder event collection (continued)

Parameter	Value
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar

To collect Microsoft SQL Server LOGbinder events, you must configure your LOGbinder SQL system to send events to IBM Security QRadar.

Before you begin

Configure LOGbinder SQL to collect events from your Microsoft SQL Server. For more information, see your LOGbinder SQL documentation.

Procedure

1. Open the LOGbinder SQL Control Panel.
2. Double-click **Output** in the Configure pane.
3. Choose one of the following options:
   - Configure for Syslog-Generic output:
     a. In the Outputs pane, double-click **Syslog-Generic**.
     b. Select the **Send output to Syslog-Generic** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
   - Configure for Syslog-LEEF output:
     a. In the Outputs pane, double-click **Syslog-LEEF**.
     b. Select the **Send output to Syslog-LEEF** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
4. Click **OK**.
5. To restart the LOGbinder service, click the **Restart** icon.

Chapter 40. Microsoft Exchange Server

The IBM Security QRadar DSM for Microsoft Exchange Server collects Exchange events by polling for event log files.

The following table identifies the specifications for the Microsoft Exchange Server DSM:

Table 63. Microsoft Exchange Server

Specification	Value
Manufacturer	Microsoft
DSM name	Exchange Server
RPM file name	DSM-MicrosoftExchange-*QRadar_version-build_number*.noarch.rpm
Supported versions	Microsoft Exchange 2003 Microsoft Exchange 2007 Microsoft Exchange 2010
Protocol type	WinCollect for Microsoft Exchange 2003 Microsoft Exchange protocol for Microsoft Exchange 2007 and 2010
QRadar recorded event types	Outlook Web Access events (OWA) Simple Mail Transfer Protocol events (SMTP) Message Tracking Protocol events (MSGTRK)
Automatically discovered?	No
Included identity?	No
More information	Microsoft website (http://www.microsoft.com)

To integrate Microsoft Exchange Server with QRadar, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the Microsoft Exchange Server DSM RPM.
2. Configure your Microsoft Exchange Server DSM device to enable communication with QRadar.
3. Create an Microsoft Exchange Server DSM log source on the QRadar Console.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring Microsoft Exchange Server to communicate with QRadar

Before you begin

Ensure that the firewalls that are located between the Exchange Server and the remote host allow traffic on the following ports:

- TCP port 13 for Microsoft Endpoint Mapper.
- UDP port 137 for NetBIOS name service.
- UDP port 138 for NetBIOS datagram service.
- TCP port 139 for NetBIOS session service.
- TCP port 445 for Microsoft Directory Services to transfer files across a Windows share.

Procedure

1. Configure OWA logs.
2. Configure SMTP logs.
3. Configure MSGTRK logs.

Configuring OWA logs on your Microsoft Exchange Server

To prepare your Microsoft Exchange Server to communicate with IBM Security QRadar, configure Outlook Web Access (OWA) event logs.

Procedure

1. Log into your Microsoft Internet Information System (IIS) Manager.
2. On the desktop, select **Start** > **Run**.
3. Type the following command:
   ```
   inetmgr
   ```
4. Click **OK**.
5. In the menu tree, expand **Local Computer**.
6. If you use IIS 6.0 Manager for Microsoft Server 2003, complete the following steps:
   a. Expand **Web Sites**.
   b. Right-click **Default Web Site** and select **Properties**.
   c. From the **Active Log Format** list, select **W3C**.
   d. Click **Properties**.
   e. Click the **Advanced** tab.
   f. From the list of properties, select the **Method (cs-method)** and **Protocol Version (cs-version)** check boxes
   g. Click **OK**.
7. If you use IIS 7.0 Manager for Microsoft Server 2008 R2, complete the following steps:
   a. Click **Logging**.
   b. From the **Format** list, select **W3C**.
   c. Click **Select Fields**.
   d. From the list of properties, select the **Method (cs-method)** and **Protocol Version (cs-version)** check boxes
   e. Click **OK**.

Enabling SMTP logs on your Microsoft Exchange Server

To prepare your Microsoft Exchange Server 2007 and 2010 to communicate with IBM Security QRadar, enable SMTP event logs.

Procedure

1. Start the Exchange Management Console.
2. To configure your *receive connector*, choose one of the following options:
   - For edge transport servers, select **Edge Transport** in the console tree and click the **Receive Connectors** tab.
   - For hub transport servers, select **Server Configuration** > **Hub Transport** in the console tree, select the server, and then click the **Receive Connectors** tab.
3. Select your receive connector and click **Properties**.
4. Click the **General** tab.
5. From the **Protocol logging level** list, select **Verbose**.
6. Click **Apply**.
7. Click **OK**.
8. To configure your *send connector*, choose one of the following options:
   - For edge transport servers, select **Edge Transport** in the console tree and click the **Send Connectors** tab.
   - For hub transport servers, select **Organization Configuration** > **Hub Transport** in the console tree, select your server, and then click the **Send Connectors** tab.
9. Select your send connector and click **Properties**.
10. Click the **General** tab.
11. From the **Protocol logging level** list, select **Verbose**.
12. Click **Apply**.
13. Click **OK**.

Configuring a log source for Microsoft Exchange

IBM Security QRadar does not automatically discover Microsoft Exchange events. To integrate Microsoft Exchange event data, you must create a log source for each instance from which you want to collect event logs.

Before you begin

If a log folder path on the Exchange Server contains an administrative share (C$), ensure that users with NetBIOS access have local or domain administrator permissions.

About this task

The folder path fields for OWA, SNMP, and MSGTRK define the default file path with a drive letter and path information. If you changed the location of the log files on the Microsoft Exchange Server, ensure that you provide the correct file paths in the log source configuration. The Microsoft Exchange Protocol can read subdirectories of the OWA, SMTP, and MSGTRK folders for event logs.

Directory paths can be specified in the following formats:

- Correct - `c$/LogFiles/`

- Correct - `LogFiles/`
- Incorrect - `c:/LogFiles`
- Incorrect - `c$\LogFiles`

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **Log Sources** icon.
4. In the **Log Source Name** field, type a name for the log source.
5. In the **Log Source Description** field, type a description for the log source.
6. From the **Log Source Type** list, select **Microsoft Exchange Server**.
7. From the **Protocol Configuration** list, select **Microsoft Exchange**.
8. Configure the following parameters:

Option	Description
Log Source Identifier	The IP address or host name to identify the Windows Exchange event source in the QRadar user interface.
Server Address	The IP address of the Microsoft Exchange server.
SMTP Log Folder Path	The directory path to access the SMTP log files. Use one of the following directory paths: • For Microsoft Exchange 2003, use `c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/` . • For Microsoft Exchange 2007, use `c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/`. • For Microsoft Exchange 2010, use `c$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/ProtocolLog/`.
OWA Log Folder Path	The directory path to access the OWA log files. Use one of the following directory paths: • For Microsoft Exchange 2003, use `c$/WINDOWS/system32/LogFiles/W3SVC1/` . • For Microsoft Exchange 2007, use `c$/WINDOWS/system32/LogFiles/W3SVC1/` . • For Microsoft Exchange 2010, use `c$/inetpub/logs/LogFiles/W3SVC1/` .
MSGTRK Log Folder Path	The directory path to access message tracking log files. Message tracking is only available on Microsoft Exchange 2007 servers assigned the Hub Transport, Mailbox, or Edge Transport server role. Use one of the following directory paths: • For Microsoft Exchange 2007, use `c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/MessageTracking/`. • For Microsoft Exchange 2010, use `c$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/MessageTracking/`.
Force File Read	Forces the protocol to read the log file. By default, the check box is selected. If the check box is cleared, the log file is read when the log file modified time or file size attributes change.

9. Configure the remaining parameters.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

Chapter 41. Microsoft SQL Server

The IBM Security QRadar DSM for Microsoft SQL Server collect SQL events by using the syslog, WinCollect Microsoft SQL, or JDBC protocol.

The following table identifies the specifications for the Microsoft SQL Server DSM:

Table 64. Microsoft SQL Server DSM

Specification	Value
Manufacturer	Microsoft
DSM name	SQL Server
RPM file name	DSM-MicrosoftSQL-*QRadar-version-Build_number*.noarch.rpm
Supported versions	2008, 2012, and 2014 (Enterprise editions only)
Event format	syslog, JDBC, WinCollect
QRadar recorded event types	SQL error log events
Automatically discovered?	Yes
Includes identity?	Yes
More information	Microsoft website (http://www.microsoft.com/en-us/server-cloud/products/sql-server/)

You can integrate Microsoft SQL Server with QRadar by using one of the following methods:

JDBC Microsoft SQL Server Enterprise can capture audit events by using the JDBC protocol. The audit events are stored in a table view. Audit events are only available in Microsoft SQL Server 2008, 2012, and 2014 Enterprise.

WinCollect
You can integrate Microsoft SQL Server 2000, 2005, 2008, 2012, and 2014 with QRadar by using WinCollect to collect ERRORLOG messages from the databases that are managed by your Microsoft SQL Server. For more information, see your WinCollect documentation.

To integrate the Microsoft SQL Server DSM with QRadar, use the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Microsoft SQL Server RPM on your QRadar Console.
2. For each instance of Microsoft SQL Server, configure your Microsoft SQL Server appliance to enable communication with QRadar.
3. If QRadar does not automatically discover the Microsoft SQL Server log source, create a log source for each instance of Microsoft SQL Server on your network.

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source

to receive events from your network devices or appliances.

Microsoft SQL Server preparation for communication with QRadar

To prepare Microsoft SQL Server for communication with QRadar, you must create an audit object, audit specification, and database view.

Creating a Microsoft SQL Server auditing object

Create an auditing object to store audit events.

Procedure

1. Log in to your Microsoft SQL Server Management Studio.
2. From the navigation menu, select **Security** > **Audits**.
3. Right-click **Audits** and select **New Audit**.
4. In the **Audit name** field, type a name for the new audit file.
5. From the **Audit destination** list, select **File**.
6. From the **File path** field, type the directory path for your Microsoft SQL Server audit file.
7. Click **OK**.
8. Right-click your audit object and select **Enable Audit**.

Creating a Microsoft SQL Server audit specification

Create an audit specification to define the level of auditing events that are written to an audit file.

Before you begin

You must create an audit object. See "Creating a Microsoft SQL Server auditing object."

About this task

You can create an audit specification at the server level or at the database level. Depending on your requirements, you might require both a server and database audit specification.

Procedure

1. From the Microsoft SQL Server Management Studio navigation menu, select one of the following options:
   - **Security** > **Server Audit Specifications**
   - **<Database>** > **Security** > `Database Audit Specifications`
2. Right-click **Server Audit Specifications**, and then select one of the following options:
   - **New Server Audit Specifications**
   - **New Database Audit Specifications**
3. In the **Name** field, type a name for the new audit file.
4. From the **Audit** list, select the audit object that you created.
5. In the **Actions** pane, add actions and objects to the server audit.
6. Click **OK**.

7. Right-click your server audit specification and select one of the following options:
   - **Enable Server Audit Specification**
   - **Enable Database Audit Specification**

Creating a Microsoft SQL Server database view

Create the dbo.AuditData database view to allow QRadar to poll for audit events from a database table by using the JDBC protocol. The database view contains the audit events from your server audit specification and database audit specification.

Procedure

1. From the Microsoft SQL Server Management Studio toolbar, click **New Query**.
2. Type the following Transact-SQL statement:

   ```
   create view dbo.AuditData as
        SELECT * FROM sys.fn_get_audit_file
        ('<Audit File Path and Name>',default,default);
        GOa
   ```

   For example:

   ```
   create view dbo.AuditData as
        SELECT * FROM sys.fn_get_audit_file
        ('C:\inetpub\logs\SQLAudits*',default,default);
        GO
   ```
3. From the Standard toolbar, click **Execute**.

Configuring a Microsoft SQL Server log source

Use this procedure if your QRadar Console did not automatically discover the Microsoft Windows Security Event log source.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **Log Sources** icon.
4. Click the **Add** button.
5. From the **Log Source Type** list, select **Microsoft SQL Server**.
6. From the **Protocol Configuration** list, select **JDBC** or **WinCollect**.
7. `Optional`. If you want to configure events for **JDBC**, configure the following Microsoft SQL Server log source parameters:

Parameter	Description
Log Source Identifier	Type the identifier for the log source in the following format: `<SQL Database>@<SQL DB Server IP or Host Name>` Where: `<SQL Database>` is the database name, as entered in the **Database Name** parameter. <SQL DB Server IP or Host Name> is the hostname or IP address for this log source, as entered in the **IP or Hostname** parameter.
Database Type	From the list, select **MSDE**.
Database Name	Type `Master` as the name of the Microsoft SQL database.
IP or Hostname	Type the IP address or host name of the Microsoft SQL server.
Port	Type the port number that is used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft SQL database. The Microsoft SQL database must have incoming TCP connections that are enabled to communicate with QRadar. **Important:** If you define a **Database Instance** when you are using MSDE as the **Database Type**, you must leave the **Port** parameter blank in your configuration.
Username	Type the user name to access the SQL database.
Password	Type the password to access the SQL database.
Confirm Password	Type the password to access the SQL database.
Authentication Domain	If you select MSDE as the **Database Type** and the database is configured for Windows, you must define a **Window Authentication Domain**. Otherwise, leave this field blank.
Database Instance	**Optional:** If you have multiple SQL server instances on your database server, type the database instance. **Important:** If you have 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.

Parameter	Description
Table Name	Type dbo.AuditData as the name of the table or view that includes the audit event records.
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views. The list must contain the field that is defined in the **Compare Field** parameter. The comma-separated list can be a maximum of 255 characters. You can include the special characters, dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).
Compare Field	Type event_time in the **Compare Field** parameter. The **Compare Field** identifies new events that are added between queries, in the table.
Start Date and Time	**Optional:** Type the start date and time for database polling. The **Start Date and Time** parameter must be formatted as yyyy-MM-dd HH:mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select this check box to use prepared statements Prepared statements allow the JDBC protocol source to set up the SQL statement, and then run the SQL statement many times with different parameters. For security and performance reasons, you might want to use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Polling Interval	You can type a polling interval number. The polling interval is the amount of time between queries to the event table. The default polling interval is 10 seconds. 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 that are entered without an H or M, poll in seconds.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.

Parameter	Description
Use Named Pipe Communication	Clear the **Use Named Pipe Communications** check box. If you use a **Named Pipe** connection, the user name and password must be the appropriate Windows authentication user name and password, and not the database user name and password. Also, you must use the default **Named Pipe**.
Database Cluster Name	If you select the **Use Named Pipe Communication** check box, the **Database Cluster Name** parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name.

8. Optional. If you want to configure events for **WinCollect**, see the *IBM Security WinCollect User Guide*.
9. Click **Save**.
10. On the **Admin** tab, click **Deploy Changes**.

Chapter 42. Microsoft Windows Security Event Log

The IBM Security QRadar DSM for Microsoft Windows Security Event Log accepts syslog events from Microsoft Windows systems.

For event collection from Microsoft operating systems, QRadar supports the following protocols:

- MSRPC (Microsoft Security Event Log over MSRPC)
- Syslog (Intended for Snare, BalaBit, and other third-party Windows solutions)
  – Common Event Format (CEF) is also supported.
- WMI (Microsoft Security Event Log). This is a legacy protocol.
- WinCollect. See the WinCollect User Guide (http://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.4/QRadar/EN/b_wincollect.pdf)

Related tasks:

"Enabling MSRPC on Windows hosts"
To enable communication between your Windows host and QRadar over MSRPC, configure the Remote Procedure Calls (RPC) settings on the Windows host for the Microsoft Remote Procedure Calls (MSRPC) protocol.

"Enabling a Snare Agent on Windows hosts" on page 142
To enable communication between your Windows host and IBM Security QRadar, you can use a Snare Agent to forward Windows events.

"Enabling WMI on Windows hosts" on page 143
To enable communication between your Windows host and IBM Security QRadar, you can use Windows Management Instrumentation (WMI).

Enabling MSRPC on Windows hosts

To enable communication between your Windows host and QRadar over MSRPC, configure the Remote Procedure Calls (RPC) settings on the Windows host for the Microsoft Remote Procedure Calls (MSRPC) protocol.

Before you begin

You must be a member of the administrators group to enable communication over MSRPC between your Windows host and the QRadar appliance.

About this task

Based on performance tests on an IBM Security QRadar Event Processor 1628 appliance with 132 GB of RAM and 40 cores (Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80 GHz), a rate of 8500 events per second (eps) was achieved successfully, while simultaneously receiving and processing logs from other non-Windows systems. The log source limit is 500.

Specification	Value
Manufacturer	Microsoft
Protocol type	Microsoft Security Event Log over MSRPC

Specification	Value
Supported versions	Windows Server 2003 (most recent) Windows Server 2008 (most recent) Windows 2012 (most recent) Windows 7 Windows 8 Windows 8.1 Windows Vista
Intended application	Agentless event collection for Windows operating systems that can support 100 EPS per log source.
Maximum number of supported log sources	500 MSRPC protocol log sources for each managed host (16xx or 18xx appliance)
Maximum overall EPS rate of MSRPC	8500 EPS for each managed host
Special features	Supports encrypted events by default.
Required permissions	The log source user must be a member of the **Event Log Readers** group. If this group is not configured, then domain admin privileges are required in most cases to poll a Windows event log across a domain. In some cases, the **Backup operators** group can also be used depending on how Microsoft Group Policy Objects are configured. Windows XP and 2003 operating systems users require read access to the following registry keys: • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language • HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
Supported event types	Application System Security DSN Server File Replication Directory Service logs Directory Service logs
Windows service requirements	For Windows Vista and later: Remote Procedure Call (RPC) and RPC Endpoint Mapper. For Windows 2003: Remote Registry and Server.

Specification	Value
Windows port requirements	Ensure that external firewalls between the Windows host and the QRadar appliance are configured to allow incoming and outgoing TCP connections on the following ports: For Windows Vista and later: • TCP port 135 • TCP port that is dynamically allocated for RPC, above 49152 For Windows 2003: • TCP port 445 • TCP port 139
Automatically discovered?	No, manual log source creation is required.
Includes identity?	Yes
Includes custom properties?	A security content pack with Windows custom event properties is available on IBM Fix Central.

Required RPM files	`PROTOCOL-WindowsEventRPC-`*`QRadar_release-Build_number`*`.noarch.rpm`
	`DSM-MicrosoftWindows-`*`QRadar_release-Build_number`*`.noarch.rpm`
	`DSM-DSMCommon-`*`QRadar_release-Build_number`*`.noarch.rpm`

More information	Microsoft support (support.microsoft.com/)
Troubleshooting tools available	Yes, an MSRPC test tool is available through IBM support.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. From the **Log Source Type** list, select **Microsoft Windows Security Event Log**.
5. From the **Protocol Configuration** list, select **Microsoft Security Event Log over MSRPC**.
6. From the **Log Source Identifier** list, type the IP address or the host name of the Windows system that you intend to poll for events. Host names must be entered as fully qualified domain names (FQDN), such as `myhost.example.com`.
7. From the **Domain** field, type the domain of the Windows system.
8. Configure the log source user name and password parameters.
9. Optional: Configure the **Polling Interval** field.

   Note: The **Polling Interval (Sec)** field does not tune log source performance like with WinCollect log sources. To poll low event rate systems with limited bandwidth, you can increase the polling interval to reduce network usage.
10. Configure the **Event Throttle** field.
11. Select at least one of the **Standard Log Types** check boxes.

Important: If you use the **Microsoft Security Event Log** or **Microsoft Security Event Log over MSRPC** protocol, select only the log types that are supported on the target Windows host.

12. Select at least one of the **Event Types** check boxes.
13. Click **Save**.
14. On the **Admin** tab, click **Deploy Changes**.

Enabling a Snare Agent on Windows hosts

To enable communication between your Windows host and IBM Security QRadar, you can use a Snare Agent to forward Windows events.

About this task

Syslog collection of Windows events can come from a number of different sources. The instructions provided in this guide outline configuration for the free version of Snare by Intersect Alliance. Several other third-party products can use the Syslog protocol.

Specification	Value
Manufacturer	Microsoft
Protocol type	Syslog
Supported versions	See your vendor documentation.
Products that commonly use this DSM	Snare Adaptive Log Exporter BalaBit Forwarded Splunk events Snare Epilogue
Supported event types	Security System, Application DNS Server File Replication Directory Service
Intended application	Agent solution for parsing and collection of Windows events from partner and third-party products.
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	A security content pack with Windows custom event properties is available on IBM Fix Central.

Required RPM files	`DSM-MicrosoftWindows-`*`QRadar_release-Build_number`*`.noarch.rpm`
	`DSM-DSMCommon-`*`QRadar_release-Build_number`*`.noarch.rpm`

Specification	Value
More information	Microsoft support (support.microsoft.com/)
Troubleshooting tools available	You can use `tcpdump` utility on the QRadar appliance to confirm that events are being received.

Procedure

1. Log in to your Windows host.
2. Download and install the Snare Agent from the Snare website (http://www.intersectalliance.com/SnareWindows/index.html).
3. On the navigation menu, select **Network Configuration**.
4. In the **Destination Snare Server** address field, type the IP address of the QRadar system.
5. Select the **Enable SYSLOG Header** check box.
6. Click **Change Configuration**.
7. On the navigation menu, select **Objectives Configuration**.
8. In the **Identify the event types to be captured** field, select check boxes to define the event types to forward to QRadar.

   Tip: The DSM for Microsoft Windows Event Log supports Informational, Warning, Error, Success Audit, and Failure Audit event types.
9. In the **Identify the event logs** field, select the check boxes to define the event logs to forward to QRadar.

   Tip: The Microsoft Windows Event Log DSM supports Security, System, Application, DNS Server, File Replication, and Directory Service log types.
10. Click **Change Configuration**.
11. On the navigation menu, select **Apply the Latest Audit Configuration**.
12. Record the value in the **override host name detection with** field. The value must match the IP address or host name that is assigned to the device that is configured in the QRadar log source.

Results

After QRadar receives approximately 35 events, a log source is automatically created and events are displayed on the **Log Activity** tab.

Enabling WMI on Windows hosts

To enable communication between your Windows host and IBM Security QRadar, you can use Windows Management Instrumentation (WMI).

Before you begin

You must be a member of the administrators group on the remote computer to configure WMI/DCOM Windows host and the QRadar appliance.

About this task

The Microsoft Security Event Log protocol (WMI) is not recommended for event collection where more than 50 EPS is required or for servers over slow network connections, such as satellite or slow WAN networks. Network delays that are created by slow connections decrease the EPS throughput available to remote servers. Faster connections can use MSRPC as an alternative. If it is not possible to decrease your network round-trip delay time, we recommend that you use an agent, such as WinCollect.

Specification	**Value**
Manufacturer	Microsoft
DSM name	Windows Security Event Log
Supported versions	Windows Server 2003 (most recent) Windows Server 2008 (most recent) Windows 2012 (most recent) Windows 7 Windows 8 (64-bit versions) Windows Vista Windows XP
Special features	Supports encrypted events by default.
Intended application	Agentless event collection for Windows operating systems over WMI that is capable of 50 EPS per log source. **Important:** This is a legacy protocol. In most cases, new log sources should be configured by using the Microsoft Security Event Log over MSRPC protocol.
Special configuration instructions	Configuring DCOM and WMI to Remotely Retrieve Windows 7 Events (http://www.ibm.com/support/docview.wss?uid=swg21678809) Configuring DCOM and WMI to Remotely Retrieve Windows 8 and Windows 2012 Events (http://www.ibm.com/support/docview.wss?uid=swg21681046)
Windows port requirements	You must ensure that external firewalls between the Windows host and the QRadar appliance are configured to allow incoming and outgoing TCP connections on the following ports: • TCP port 135 (all operating system versions) • TCP port that is dynamically allocated above 49152 (required for Vista and above operating systems) • TCP port that is dynamically allocated above 1024 (required for Windows XP & 2003) • TCP port 445 (required for Windows XP & 2003) • TCP port 139 (required for Windows XP & 2003)

Specification	Value
Windows service requirements	The following services must be configured to start automatically: • Remote Procedure Call (RPC) • Remote Procedure Call (RPC) Locator • RPC Endpoint Mapper • Remote Registry • Server • Windows Management Instrumentation
Log source permissions	The log source user must be a member of the **Event Log Readers** group. If this group is not configured, then domain admin privileges are required in most cases to poll a Windows event log across a domain. In some cases, the **Backup operators** group can also be used depending on how Microsoft Group Policy Objects are configured. The log source user must have access to following components: • Window event log protocol DCOM components • Windows event log protocol name space • Appropriate access to the remote registry keys
Supported event types	Application System Security DNS Server File Replication Directory Service logs
Automatically discovered?	No, manual log source creation is required
Includes identity?	Yes
Includes custom properties?	A security content pack with Windows custom event properties is available on IBM Fix Central.

Required RPM files	`PROTOCOL-WinCollectWindowsEventLog-`*`QRadar_release-Build_number`*`.noarch.rpm`
	`DSM-MicrosoftWindows-`*`QRadar_release-Build_number`*`.noarch.rpm`
	`DSM-DSMCommon-`*`QRadar_release-Build_number`*`.noarch.rpm`

More information	Microsoft support (support.microsoft.com/)
Troubleshooting tools available	Yes, a WMI test tool is available in `/opt/qradar/jars`.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. From the **Log Source Type** list, select **Microsoft Windows Security Event Log**.
5. From the **Protocol Configuration** list, select **Microsoft Security Event Log**.
6. From the **Log Source Identifier** list, type the IP address or the host name of the Windows system that you intend to poll for events. Host names must be entered as fully qualified domain names (FQDN), such as `myhost.example.com`.
7. From the **Domain** field, type the domain of the Windows system.
8. Configure the log source user name and password parameters.
9. Select at least one of the **Standard Log Types** check boxes.

   Important: If you use the **Microsoft Security Event Log** or **Microsoft Security Event Log over MSRPC** protocol, select only the log types that are supported on the target Windows host.
10. Select at least one of the **Event Types** check boxes.
11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

Chapter 43. Netskope Active

The IBM Security QRadar DSM for Netskope Active collects events from your Netskope Active servers.

The following table identifies the specifications for the Netskope Active DSM:

Table 65. Netskope Active DSM specifications

Specification	Value
Manufacturer	Netskope
DSM name	Netskope Active
RPM file name	`DSM-NetskopeActive-`*`Qradar_version-build_number`*`.noarch.rpm`
Protocol	Netskope Active REST API
Recorded event types	Alert, All
Automatically discovered?	No
Includes identity?	Yes
More information	Netskope Active website (www.netskope.com)

To integrate Netskope Active DSM with QRadar complete the following steps:

Note: If multiple DSM RPMs are required, the integration sequence must reflect the DSM RPM dependency.

1. If automatic updates are not enabled, download and install the most recent version of the following DSMs on your QRadar Console.
   - Netskope Active DSM RPM
   - Netskope Active REST API Protocol RPM
   - PROTOCOL-Common RPM
2. Configure the required parameters, and use the following table for the Netskope Active log source specific parameters:

Table 66. Netskope Active log source parameters

Parameter	Value
Log Source type	Netskope Active
Protocol Configuration	Netskope Active REST API

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring QRadar to collect events from your Netskope Active system" on page 148
To collect all audit logs and system events from Netskope Active servers, you must configure QRadar to collect audit logs and system events from your Netskope Active system.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring QRadar to collect events from your Netskope Active system

To collect all audit logs and system events from Netskope Active servers, you must configure QRadar to collect audit logs and system events from your Netskope Active system.

About this task

The following table describes the parameters that are required to collect Netskope Active events:

Table 67. Netskope Active DSM log source parameters

Parameter	Description
IP or Hostname	`partners.goskope.com`
Authentication Token	The authentication token is generated in the Netskope WebUI and is the only credential that is required for **Netskope Active REST API** usage. To access the token generation option in the Netskope WebUI, select **Settings** > **REST API**.
Automatically Acquire Server Certificates	If you choose **Yes** from the drop-down list, QRadar automatically downloads the certificate and begins trusting the target server. The correct server must be entered in the **IP or Hostname** field.
Throttle	The maximum number of events per second. The default is 5000.
Recurrence	You can specify when the log source attempts to obtain data. The format is M/H/D for Months/Hours/Days. The default is 1 M.
Collection Type	**All Events** Select to collect all events. **Alerts Only** Select to collect only alerts.

Procedure

1. Log in to QRadar.
2. Click **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **Netskope Active**.
7. From the **Protocol Configuration** list, select **Netskope Active REST API**.
8. Configure the parameters.
9. Click **Save**.

10. On the **Admin** tab, click **Deploy Changes**.

Chapter 44. OpenStack

The IBM Security QRadar DSM for OpenStack collects event logs from your OpenStack device.

The following table identifies the specifications for the OpenStack DSM:

Table 68. OpenStack DSM specifications

Specification	Value
Manufacturer	OpenStack
DSM name	OpenStack
RPM file name	`DSM-OpenStackCeilometer-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	v 2014.1
Protocol	HTTP Receiver
Recorded event types	Audit event
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	OpenStack website (http://www.openstack.org/)

To send events from OpenStack to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - PROTOCOL-HTTPReceiver RPM
   - OpenStack DSM RPM
2. Add an OpenStack log source on the QRadar Console. The following table describes the parameters that are required to collect OpenStack events:

Table 69. OpenStack log source parameters

Parameter	Value
Log Source type	**OpenStack**
Protocol Configuration	**HTTPReceiver**
Communication Type	**HTTP**
Listen Port	The port number that OpenStack uses to communicate with QRadar. **Important:** Use a non-standard port. Make note of this port because it is required to configure your OpenStack device.
Message Pattern	`^\{"typeURI`

3. Configure your OpenStack device to communicate with QRadar.

Related tasks:

"Configuring OpenStack to communicate with QRadar" on page 152
To collect OpenStack events, you must configure your OpenStack device to allow

connections from QRadar.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

Configuring OpenStack to communicate with QRadar

To collect OpenStack events, you must configure your OpenStack device to allow connections from QRadar.

Important: OpenStack is an open source product with many different distributions that can be set up on many different operating systems. This procedure might vary in your environment.

Procedure

1. Log in to your OpenStack device.
2. Edit the `/etc/nova/api-paste.ini` file.
3. At the end of the file, add the following text:
```
[filter:audit]
paste.filter_factory = pycadf.middleware.audit:AuditMiddleware.factory
audit_map_file = /etc/nova/api_audit_map.conf
```
4. Review the `[composite:openstack_compute_api_v2]` settings and verify that the values match the following sample:
```
[composite:openstack_compute_api_v2]
use = call:nova.api.auth:pipeline_factory
noauth = faultwrap sizelimit noauth ratelimit osapi_compute_app_v2
keystone = faultwrap sizelimit authtoken keystonecontext ratelimit audit osapi_compute_app_v2
keystone_nolimit = faultwrap sizelimit authtoken keystonecontext audit osapi_compute_app_v2
```
5. Copy the `api_audit_map.conf` file to the `/etc/nova/` directory.
6. Restart the api service.

   The command to restart the API service depends on what operating system your OpenStack node is hosted on. On Redhat Enterprise Linux systems, the command is `service openstack-nova-api restart`.
7. Open the `entry_points.txt` file in the `egg-info` subdirectory of your OpenStack installation directory.

   For PackStack installations, the file path resembles the following path: `/usr/lib/python2.7/site-packages/ceilometer-2014.2-py2.7.egg-info/entry_points.txt`.
8. Add the http dispatcher to the `[ceilometer.dispatcher]` section.
```
[ceilometer.dispatcher]
file = ceilometer.dispatcher.file:FileDispatcher
database = ceilometer.dispatcher.database:DatabaseDispatcher
http = ceilometer.dispatcher.http:HttpDispatcher
```
9. Copy the supplied `http.py` script to the dispatcher subdirectory of the Ceilometer installation directory.

   The exact location depends on your operating system and OpenStack distribution. On the Redhat Enterprise Linux Distribution of OpenStack, the directory is `/usr/lib/python2.7/site-packages/ceilometer/dispatcher/`.
10. Edit the `/etc/ceilometer/ceilometer.conf` file.
11. Under the `[default]` section, add `dispatcher=http`.

12. At the bottom of the file, add this section:

    ```
    [dispatcher_http]
    target = http://<QRadar-IP>:<QRadar-Port>
    cadf_only = True
    ```

    Use the port that you configured for OpenStack when you created the log source on your QRadar system.

13. Restart the ceilometer collector and notification services.

    The command to restart the ceilometer collector and notification services depends on what operating system your OpenStack device is hosted on. On devices that use the Redhat Enterprise Linux operating system, use the following commands:

    ```
    service openstack-ceilometer-collector restart
    service openstack-ceilometer-notification restart
    ```

Chapter 45. Oracle Enterprise Manager

The IBM Security QRadar DSM for Oracle Enterprise Manager collects events from an Oracle Enterprise Manager device. The Real-time Monitoring Compliance feature of Oracle Enterprise Manager generates the events.

The following table lists the specifications for the Oracle Enterprise Manager DSM:

Table 70. Oracle Enterprise Manager DSM specifications

Specification	Value
Manufacturer	Oracle
DSM name	Oracle Enterprise Manager

RPM file name	`DSM-OracleEnterpriseManager-`*`Qradar_version-`*
	`Buildbuild_number``.noarch.rpm`

Supported versions	Oracle Enterprise Manager Cloud Control 12c
Protocol	JDBC
Recorded event types	Audit Compliance
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Oracle Enterprise Manager (http://www.oracle.com/us/products/enterprise-manager/index.html) The original format of the events are rows in an Oracle Enterprise Manager database view (`sysman.mgmt$ccc_all_observations`). QRadar polls this view for new rows and uses them to generate events. For more information, see Compliance Views (http://docs.oracle.com/cd/E24628_01/doc.121/e57277/ch5_complianceviews.htm#BABBIJAA)

To collect events from Oracle Enterprise Manager, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Oracle Enterprise Manager DSM RPM on your QRadar Console.
2. Ensure that the Oracle Enterprise Manager system is configured to accept connections from external devices.
3. Add an Oracle Enterprise Manager log source on the QRadar Console. The following table describes the parameters that require specific values for Oracle Enterprise Manager event collection:

Table 71. Oracle Enterprise Manager log source parameters

Parameter	Description
Log Source type	Oracle Enterprise Manager
Protocol Configuration	JDBC
Database Type	Oracle
Database Name	The Service Name of Oracle Enterprise Manager database. To view the available service names, run the `lsnrctl status` command on the Oracle host.
IP or Hostname	The IP address or host name of host for Oracle Enterprise Manager database.
Port	The port that is used by the Oracle Enterprise Manager database.
Username	The user name of the account that has right to access the `sysman.mgmt$ccc_all_observations` table.
Predefined Query	none
Table Name	`sysman.mgmt$ccc_all_observations`
Select List	*
Compare Field	ACTION_TIME
Use Prepared Statements	True

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Chapter 46. Palo Alto Networks

Use the IBM Security QRadar SIEM DSM for Palo Alto PA Series to collect events from Palo Alto PA Series devices.

The following table identifies the specifications for the Palo Alto PA Series DSM:

Table 72. DSM specifications for Palo Alto PA Series

Specification	Value
Manufacturer	Palo Alto Networks
DSM name	Palo Alto PA Series
RPM file name	`DSM-PaloAltoPaSeries-`*`build_number`*`.noarch.rpm`
Supported versions	PanOS v3.0 and later
Event format	Syslog LEEF
QRadar recorded event types	All events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Palo Alto Networks website (http://www.paloaltonetworks.com)

To send events from Palo Alto PA Series to QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the Palo Alto PA Series DSM RPM.
2. Configure your Palo Alto PA Series device to communicate with QRadar. You must create a syslog destination and forwarding policy on the Palo Alto PA Series device.
3. If QRadar does not automatically detect Palo Alto PA Series as a log source, create a Palo Alto PA Series log source on the QRadar Console. Use the following Palo Alto values to configure the log source parameters:

Parameter	Description
Log Source Identifier	The IP address or host name of the Palo Alto PA Series device.
Log Source Type	Palo Alto PA Series
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Creating a syslog destination on your Palo Alto device" on page 158
Before you can send Palo Alto events to IBM Security QRadar, create a syslog destination on the Palo Alto PA Series device.

"Creating a forwarding policy on your Palo Alto device" on page 159
If your IBM Security QRadar Console or Event Collector is in a different security zone than your Palo Alto PA Series device, create a forwarding policy rule.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Creating a syslog destination on your Palo Alto device

Before you can send Palo Alto events to IBM Security QRadar, create a syslog destination on the Palo Alto PA Series device.

Procedure

1. Log in to the Palo Alto Networks interface.
2. Click the **Device** tab.
3. Click **Server Profiles** > **Syslog**.
4. Click **Add**.
5. Create a syslog destination:
   a. In the **Syslog Server Profile** dialog box, click **Add**.
   b. Specify the name, server IP address, port, and facility of the QRadar system that you want to use as a syslog server:
   c. Click **OK**.
6. Configure LEEF events:

   Attention: The line breaks in these examples will cause this configuration to fail. For each of the substeps, copy the code blocks into a text editor, remove the line breaks, and paste as a single line in the **Custom Format** column.

   a. Click the **Custom Log Format** tab.
   b. Copy the following text and paste it in the **Custom Format** column for the **Config** log type.

   ```
   LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$result|cat=$type|
   usrName=$admin|src=$host|devTime=$cef-formatted-receive_time|client=$client|
   sequence=$seqno|serial=$serial|msg=$cmd
   ```

   c. Copy the following text and paste it in the **Custom Format** column for the **System** log type.

   ```
   LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$eventid|cat=$type
   |subtype=$subtype|devTime=$cef-formatted-receive_time|sev=$severity
   |Severity=$number-of-severity|msg=$opaque|Filename=$object
   ```

   d. Copy the following text and paste it in the **Custom Format** column for the **Threat** log type.

   ```
   LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$threatid|cat=$type
   |subtype=$subtype|src=$src|dst=$dst|srcPort=$sport|dstPort=$dport|proto=$proto
   |usrName=$srcuser|SerialNumber=$serial|srcPostNAT=$natsrc|dstPostNAT=$natdst
   |RuleName=$rule|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app
   |VirtualSystem=$vsys|SourceZone=$fromDestinationZone=$to|IngressInterface=$inbound_if
   |EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid
   |RepeatCount=$repeatcnt|srcPostNATPort=$natsport|dstPostNATPort=$natdport
   |Flags=$flags|URLCategory=$category|sev=$severity|Severity=$number-of-severity
   |Direction=$direction|ContentType=$contenttype|action=$action|Miscellaneous=$misc
   ```

   e. Copy the following text and paste it in the **Custom Format** column for the **Traffic** log type.

   ```
   LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$action|cat=$type|src=$src
   |dst=$dst|srcPort=$sport|dstPort=$dport|proto=$proto|usrName=$srcuser| SerialNumber=
   $serial|Type=$type|Subtype=$subtype|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=
   $rule|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app| VirtualSystem=
   $vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if
   |EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
   ```

```
RepeatCount=$repeatcnt|srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=$flags
|totalBytes=$bytes|totalPackets=$packets|ElapsedTime=$elapsed|URLCategory=$category
|dstBytes=$bytes_received|srcBytes=$bytes_sent|action=$action
```

7. Click **OK**.
8. Specify the severity of events that are contained in the syslog messages:
   a. Click **Log Setting** > **System** and click **Edit**.
   b. Select the check box for each event severity level that you want contained in the syslog message.
   c. Type the name of the syslog destination.
   d. Click **OK**.
9. Click the **Device** tab and click **Commit**.

What to do next

To allow communication between your Palo Alto Networks device and QRadar, create a forwarding policy. See "Creating a forwarding policy on your Palo Alto device."

Related concepts:

Chapter 46, "Palo Alto Networks," on page 157
Use the IBM Security QRadar SIEM DSM for Palo Alto PA Series to collect events from Palo Alto PA Series devices.

Creating a forwarding policy on your Palo Alto device

If your IBM Security QRadar Console or Event Collector is in a different security zone than your Palo Alto PA Series device, create a forwarding policy rule.

Procedure

1. Log in to Palo Alto Networks.
2. On the dashboard, click the **Policies** tab.
3. Click **Policies** > **Policy Based Forwarding**.
4. Click **New**.
5. Configure the parameters. For descriptions of the policy-based forwarding values, see your *Palo Alto Networks Administrator's Guide*.

Related concepts:

Chapter 46, "Palo Alto Networks," on page 157
Use the IBM Security QRadar SIEM DSM for Palo Alto PA Series to collect events from Palo Alto PA Series devices.

Chapter 47. RSA Authentication Manager

An RSA Authentication Manager DSM allows you to integrate IBM Security QRadar with an RSA Authentication Manager using syslog or the log file protocol.

Before you configure QRadar to integrate with RSA Authentication Manager, select your configuration preference:

- “Configuring syslog for RSA”
- “Configuring the log file protocol for RSA” on page 162

Note: You must apply the most recent hot fix on RSA Authentication Manager 7.1 primary, replica, node, database and radius installations before configuring syslog.

Configuring syslog for RSA

The procedure to configure your RSA Authentication Manager v6.x, v7.x and v8.x using syslog depends on the operating system version for your RSA Authentication Manager or SecureID 3.0 appliance:

If you are using RSA Authentication Manager on Linux, see “Configuring Linux.”

If you are using RSA Authentication Manager on Windows, see “Configuring Windows” on page 162.

Configuring Linux

You can configure RSA Authentication Manager for syslog on Linux-based operating systems:

Procedure

1. Log in to the RSA Security Console command-line interface (CLI).
2. Open the following file for editing based on your operating system:
   ```
   /usr/local/RSASecurity/RSAAuthenticationManager/utils/resources
   /ims.properties
   ```
3. Add the following enteries to the ims.properties file:
   ```
   ims.logging.audit.admin.syslog_host       = <IP address>
   ims.logging.audit.admin.use_os_logger     = true
   ims.logging.audit.runtime.syslog_host     = <IP address>
   ims.logging.audit.runtime.use_os_logger   = true
   ims.logging.system.syslog_host            = <IP address>
   ims.logging.system.use_os_logger          = true
   ```
   Where <IP address> is the IP address or hostname of QRadar.
4. Save the ims.properties files.
5. Open the following file for editing:
   ```
   /etc/syslog.conf
   ```
6. Type the following command to add QRadar as a syslog entry:
   ```
   *.* @<IP address>
   ```
   Where <IP address> is the IP address or hostname of QRadar.
7. Type the following command to restart the syslog services for Linux.

```
service syslog restart
```

8. You are now ready to configure the log sources and protocol in QRadar: To configure QRadar to receive events from your RSA Authentication Manager:
   a. From the Log Source Type list, select the RSA Authentication Manager option.

      For more information, see the IBM Security QRadar Log Sources User Guide. For more information on configuring syslog forwarding, see your RSA Authentication Manager documentation.

Configuring Windows

To configure RSA Authentication Manager for syslog using Microsoft Windows:

Procedure

1. Log in to the system hosting your RSA Security Console.
2. Open the following file for editing based on your operating system:

   ```
   /Program Files/RSASecurity/RSAAuthenticationManager/utils/
   resources/ims.properties
   ```
3. Add the following enteries to the `ims.properties` file:

   ```
   ims.logging.audit.admin.syslog_host       = <IP address>
   ims.logging.audit.admin.use_os_logger     = true
   ims.logging.audit.runtime.syslog_host     = <IP address>
   ims.logging.audit.runtime.use_os_logger   = true
   ims.logging.system.syslog_host            = <IP address>
   ims.logging.system.use_os_logger          = true
   ```

   Where `<IP address>` is the IP address or hostname of QRadar.
4. Save the `ims.properties` files.
5. Restart RSA services.
6. You are now ready to configure the log source in QRadar.

   To configure QRadar to receive events from your RSA Authentication Manager:
   a. From the Log Source Type list, select the RSA Authentication Manager option.

      For more information, see the IBM Security QRadar Log Sources User Guide. For more information on configuring syslog forwarding, see your RSA Authentication Manager documentation.

Configuring the log file protocol for RSA

The log file protocol allows QRadar to retrieve archived log files from a remote host. The RSA Authentication Manager DSM supports the bulk loading of log files using the log file protocol source.

The procedure to configure your RSA Authentication Manager using the log file protocol depends on the version of RSA Authentication Manager:

- If you are using RSA Authentication Manager v7.x, see “Configuring RSA Authentication Manager 7.x.”
- If you are using RSA Authentication Manager v6.x, see “Configuring RSA Authentication Manager 6.x” on page 163.

Configuring RSA Authentication Manager 7.x

You can configure your RSA Authentication Manager v7.x device.

Procedure

1. Log in to the RSA Security Console.
2. Click **Administration** > **Log Management** > **Recurring Log Archive Jobs**.
3. In the Schedule section, configure values for the `Job Starts`, `Frequency`, `Run Time`, and `Job Expires` parameters.
4. For the **Operations** field, select **Export Only** or **Export and Purge** for the following settings: **Administration Log Settings**, **Runtime Log Settings**, and **System Log Settings**.

   Note: The **Export and Purge** operation exports log records from the database to the archive and then purges the logs form the database. The **Export Only** operation exports log records from the database to the archive and the records remain in the database.
5. For **Administration**, **Runtime**, and **System**, configure an `Export` Directory to which you want to export your archive files.

   Ensure that you can access the Administration Log, Runtime Log, and System Log by using FTP before you continue.
6. For Administration, Runtime, and System parameters, set the Days Kept Online parameter to 1. Logs older than 1 day are exported. If you selected **Export and Purge**, the logs are also purged from the database.
7. Click **Save**.
8. You are now ready to configure the log sources and protocol within QRadar:
   a. To configure QRadar to receive events from an RSA device, you must select the **RSA Authentication Manager** option from the **Log Source Type** list.
   b. To configure the log file protocol, you must select the **Log File** option from the **Protocol Configuration** list.

      For more information about configuring log sources and protocols, see the *IBM Security QRadar Log Sources User Guide*.

Configuring RSA Authentication Manager 6.x

You can configure your RSA Authentication Manager v6.x device:

Procedure

1. Log in to the RSA Security Console.
2. Log in to the RSA Database Administration tool:
   a. Click the Advanced tool.

      The system prompts you to login again.
3. Click Database Administration.

   For complete information on using SecurID, see your vendor documentation.
4. From the Log list, select Automate Log Maintenance.

   The Automatic Log Maintenance window is displayed.
5. Select the Enable Automatic Audit Log Maintenance check box.
6. Select Delete and Archive.
7. Select Replace files.
8. Type an archive filename.
9. In the Cycle Through Version(s) field, type a value.

   For example, 1.
10. Select Select all Logs.

11. Select a frequency.
12. Click OK.
13. You are now ready to configure the log sources and protocol in QRadar:
    a. To configure QRadar to receive events from a RSA device, you must select the RSA Authentication Manager option from the Log Source Type list.
    b. To configure the log file protocol, you must select the Log File option from the Protocol Configuration list.

       For more information on configuring log sources and protocols, see the IBM Security QRadar Log Sources User Guide.

Chapter 48. Riverbed SteelCentral NetProfiler (Cascade Profiler) Alert

The IBM Security QRadar DSM for Riverbed SteelCentral NetProfiler collects alert logs from your Riverbed SteelCentral NetProfiler system. This product is also known as *Cascade Profiler*.

The following table identifies the specifications for the Riverbed SteelCentral NetProfiler DSM:

Table 73. Riverbed SteelCentral NetProfiler specifications

Specification	**Value**
Manufacturer	Riverbed
DSM name	SteelCentral NetProfiler

RPM file name	`DSM-RiverbedSteelCentralNetProfiler-`
	`Qradar_version-build_number``.noarch.rpm`

Event format	JDBC
Recorded event types	Alert Events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Riverbed website (http://www.riverbed.com/)

To integrate Riverbed SteelCentral NetProfiler with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console.
   - Protocol-JDBC RPM
   - Riverbed SteelCentral NetProfiler RPM
2. Configure your Riverbed SteelCentral NetProfiler system to enable communication with QRadar.
3. Create a log source on the QRadar Console. Use the following table to define the Riverbed-specific parameters:

Table 74. Riverbed SteelCentral NetProfiler log source parameters

Parameter	**Description**
Log Source Type	**Riverbed SteelCentral NetProfiler**
Protocol Configuration	**JDBC**
Database Name	You must type the actual name of the Riverbed database. For most configurations, the database name is `mazu`. **Tip:** Confirm the actual name of the Riverbed database.
Table Name	`events.export_csv_view`

Table 74. Riverbed SteelCentral NetProfiler log source parameters (continued)

Parameter	Description
Username	The user name for the account that is configured to access the PostgreSQL database on the Riverbed SteelCentral NetProfiler system.
Comparable Field	`start_time`
Polling Interval	**5M**

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your Riverbed SteelCentral NetProfiler system to enable communication with QRadar

To collect Riverbed SteelCentral NetProfiler alert events, you must configure your Riverbed SteelCentral NetProfiler system to allow QRadar to retrieve events from the PostgreSQL database.

Procedure

1. Log in to your Riverbed SteelCentral NetProfiler host user interface.
2. Select **Configuration** > **Appliance Security** > **Security Compliance**.
3. Check the **Enable ODBC Access** check box.
4. Select **Configuration** > **Account Management** > **User Accounts**.
5. Add an account that QRadar can use to access to the PostgreSQL database.

Chapter 49. Salesforce Security Auditing

The IBM Security QRadar DSM for Salesforce Security Auditing can collect Salesforce Security Auditing audit trail logs that you copy from the cloud to a location that QRadar can access.

The following table identifies the specifications for the Salesforce Security Auditing DSM:

Table 75. Salesforce Security Auditing DSM specifications

Specification	**Value**
Manufacturer	Salesforce
DSM	Salesforce Security Auditing
RPM file name	DSM-SalesforceSecurityAuditing-*QRadar_Version-Build_Number*.noarch.rpm
Protocol	Log File
QRadar recorded events	Setup Audit Records
Automatically discovered	No
Includes identity	No
More information	Salesforce web site (http://www.salesforce.com/)

Salesforce Security Auditing DSM integration process

To integrate Salesforce Security Auditing DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console:
   - Log File Protocol RPM
   - Salesforce Security Auditing RPM
2. Download the Salesforce audit trail file to a remote host that QRadar can access.
3. For each instance of Salesforce Security Auditing, create a log source on the QRadar Console.

Downloading the Salesforce audit trail file

To collect Salesforce Security Auditing events, you must download the Salesforce audit trail file to a remote host that QRadar can access.

About this task

You must use this procedure each time that you want to import an updated set of audit data into QRadar. When you download the audit trail file, you can overwrite the previous audit trail CSV file. When QRadar retrieves data from the audit trail file, QRadar processes only audit records that were not imported before.

Procedure

1. Log in to your Salesforce Security Auditing server.
2. Go to the **Setup** section.
3. Click **Security Controls**.
4. Click **View Setup Audit Trail**.
5. Click **Download setup audit trail for last six months (Excel.csv file)**.
6. Copy the downloaded file to a location that QRadar can reach by using Log File Protocol.

Configuring a Salesforce Security Auditing log source in QRadar

To collect Salesforce Security Auditing events, configure a log source in QRadar.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **Salesforce Security Auditing**.
7. From the **Protocol Configuration** list, select **Log File**.
8. Configure the following Salesforce Security Auditing parameters:

Parameter	Description
Event Generator	RegEx Based Multiline
Start Pattern	(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} \w+)
End Pattern	Ensure that this parameter remains empty.
Date Time RegEx	(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} \w+)
Date Time Format	dd/MM/yyyy hh:mm:ss z

   Attention: These values are based on the Winter 2015 version of Salesforce Security Auditing. For previous versions, use the following regex statements:

   - For the **Start Pattern** parameter, use the following statement:

     `(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} [APM]{2} \w+)`
   - For the **Date Time RegEx** parameter, use the following statement:

     `(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} \w{2} \w+)`
   - For the **Date Time Format** parameter, use `MM/dd/yyyy hh:mm:ss aa z`

9. Configure the remaining parameters.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

Chapter 50. Salesforce Security Monitoring

The IBM Security QRadar DSM for Salesforce Security Monitoring can collect event logs from your Salesforce console by using a RESTful API in the cloud.

The following table identifies the specifications for the Salesforce Security Salesforce Security Monitoring DSM:

Table 76. Salesforce Security Salesforce Security Monitoring DSM specifications

Specification	Value
Manufacturer	Salesforce
DSM	Salesforce Security Monitoring
RPM file name	DSM-SalesforceSecurityMonitoring-QRadar_Version-Build_Number.noarch.rpm
Protocol	Salesforce REST API Protocol
QRadar recorded events	Login History, Account History, Case History, Entitlement History, Service Contract History, Contract Line Item History, Contract History, Contact History, Lead History, Opportunity History, Solution History
Automatically discovered	No
Includes identity	Yes
More information	Salesforce website (http://www.salesforce.com/)

Salesforce Security Monitoring DSM integration process

To integrate Salesforce Security Monitoring DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console.
   - DSMCommon RPM
   - SalesforceRESTAPI Protocol RPM
   - Salesforce Security Monitoring RPM
2. Configure the Salesforce Security Monitoring server to communicate with QRadar.
3. Obtain and install a certificate to enable communication between Salesforce Security Monitoring and QRadar. The certificate must be in the /opt/QRadar/conf/trusted_certificates/ folder and be in .DER format.
4. For each instance of Salesforce Security Monitoring, create a log source on the QRadar Console.

Configuring the Salesforce Security Monitoring server to communicate with QRadar

To allow QRadar communication, you need to configure Connected App on the Salesforce console and collect information that the Connected App generates. This information is required for when you configure the QRadar log source.

Before you begin

If the RESTful API is not enabled on your Salesforce server, contact Salesforce support.

Procedure

1. Log in to your Salesforce Security Monitoring server.
2. From the **Setup** menu, click **Create > Apps > New**.
3. Type the name of your application.
4. Type the contact email information.
5. Select **Enable OAuth Settings**.
6. From the **Selected OAuth Scopes** list, select **Full Access**.
7. In the **Info URL** field, type a URL where the user can go for more information about your application.
8. Configure the remaining optional parameters.
9. Click **Save**.

What to do next

The Connected App generates the information that is required for when you to configure a log source on QRadar. Record the following information:

Consumer Key

Use the **Consumer Key** value to configure the **Client ID** parameter for the QRadar log source.

Consumer Secret

You can click the link to reveal the consumer secret. Use the **Consumer Secret** value to configure the **Secret ID** parameter for the QRadar log source.

Important: The **Consumer Secret** value is confidential. Do not store the consumer secret as plain text.

Security token

A security token is sent by email to the email address that you configured as the contact email.

Configuring a Salesforce Security Monitoring log source in QRadar

To collect Salesforce Security Monitoring events, configure a log source in QRadar.

Before you begin

When you configured a Connected App on the Salesforce Security Monitoring server, the following information was generated:

- Consumer Key

- Consumer Secret
- Security token

This information is required to configure a Salesforce Security Monitoring log source in QRadar.

Ensure that the trusted certificate from the Salesforce Security Monitoring instance is copied to the `/opt/qradar/conf/trusted_certificates/` folder in .DER format on QRadar system.

Procedure

1. Log in toQRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **Salesforce Security Monitoring**.
7. From the **Protocol Configuration** list, select **Salesforce Rest API**.
8. Configure the following values:

Parameter	Description
Login URL	The URL of the Salesforce security console.
Username	The user name of the Salesforce security console.
Security Token	The security token that was sent to the email address configured as the contact email for the Connected App on the Salesforce security console.
Client ID	The Consumer Key that was generated when you configured the Connected App on the Salesforce security console.
Secret ID	The Consumer Secret that was generated when you configured the Connected App on the Salesforce security console.
Use Proxy	When a proxy is configured, all traffic for the log source travels through the proxy for QRadar to access the Salesforce Security buckets. Configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.

9. Click **Save**.
10. On the Admin tab, click **Deploy Changes**.

Chapter 51. Configuring Sun Solaris Sendmail to communicate with QRadar

The IBM Security QRadar DSM for Sun Solaris Sendmail accepts Solaris authentication events using syslog and records all relevant sendmail events.

About this task

To collect events from Sun Solaris Sendmail, you must configure syslog to forward events to QRadar.

Procedure

1. Log in to the Sun Solaris command-line interface.
2. Open the `/etc/syslog.conf` file.
3. To forward system authentication logs to QRadar, add the following line to the file:

   ```
   mail.*; @<IP address>
   ```

   Where `<IP address>` is the IP address of your QRadar. Use tabs instead of spaces to format the line.

   Note: Depending on the version of Solaris you are running, you might need to add additional log types to the file. Contact your system administrator for more information.
4. Save and exit the file.
5. Type the following command:

   ```
   kill -HUP 'cat /etc/syslog.pid'
   ```

   You are now ready to configure the log source QRadar.

Configuring a Sun Solaris Sendmail log source

IBM Security QRadar automatically discovers and creates a log source for syslog events from Sun Solaris Sendmail appliances.

About this task

The following configuration steps are optional.

Sendmail logs from Proofpoint 7.5 and 8.5 are supported.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. In the **Log Source Name** field, type a name for your log source.
7. In the **Log Source Description** field, type a description for the log source.

8. From the Log Source Type list, select **Solaris Operating System Sendmail Logs**.
9. If you want to configure the **Syslog** protocol, select it from the **Protocol Configuration** list and configure the following values:

Table 77. Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from Sun Solaris Sendmail installations. For Each additional log source that you create when you have multiple installations, include a unique identifier, such as an IP address or host name

10. If you want to configure a **Log File** protocol, select it from the **Protocol Configuration** list and configure the following values:

Table 78. Log file parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source. The log source identifier must be unique for the log source type.
Service Type	From the list, select the protocol that you want to use when retrieving log files from a remove server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service types requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the Sun Solaris Sendmail system.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. If you configure the Service Type as FTP, the default is 21. If you configure the Service Type as SFTP or SCP, the default is 22. The valid range is 1 - 65535.
Remote User	Type the user name necessary to log in to your Sun Solaris system. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to your Sun Solaris system.
Confirm Password	Confirm the Remote Password to log in to your Sun Solaris system.

Table 78. Log file parameters (continued)

Parameter	Description
SSH Key File	If you select SCP or SFTP from the **Service Type** field you can define a directory path to an SSH private key file. The SSH Private Key File allows you to ignore the **Remote Password** field.
Remote Directory	Type the directory location on the remote host from which the files are retrieved.
Recursive	Select this check box if you want the file pattern to also search sub folders. The Recursive parameter is not used if you configure SCP as the Service Type. By default, the check box is clear.
FTP File Pattern	If you select SFTP or FTP as the Service Type, this option allows you to configure the regular expression (regex) that is required to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing. Another example, if you want to retrieve all syslog files with the keyword "_maillog" in the file name, use the following entry: `.*_maillog.*\.syslog`. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website:http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option only appears if you select FTP as the Service Type. The FTP Transfer Mode parameter allows you to define the file transfer mode when you retrieve log files over FTP. From the list, select the transfer mode that you want to apply to this log source: • Binary - Select Binary for log sources that require binary data files or compressed .zip, .gzip, .tar, or .tar+gzip archive files. • ASCII - Select ASCII for log sources that require an ASCII FTP file transfer. You must select **NONE** for the **Processor** field and **LINEBYLINE** the **Event Generator** field when you are using ASCII as the transfer mode.
SCP Remote File	If you select SCP as the Service Type, you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.

Table 78. Log file parameters (continued)

Parameter	Description
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type `2H` if you want the directory to be scanned every 2 hours. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click Save. After the **Run On Save** completes, the log file protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the **Ignore Previously Processed File(s)** parameter.
EPS Throttle	Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.
Processor	If the files on the remote host are stored in a .zip, .gzip, .tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents that are processed.
Ignore Previously Processed File(s)	Select this check box to track files that have already been processed and you do not want the files to be processed a second time. This applies to FTP and SFTP Service Types only.
Change Local Directory?	Select this check box to define the local directory on your QRadar system that you want to use for storing downloaded files during processing. We recommend that you leave the check box clear. When the check box is selected, the **Local Directory** field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select **LINEBYLINE**.

11. Click **Save**.
12. On the Admin tab, click **Deploy Changes**.

    The log source is added to QRadar. Events that are forwarded toQRadar by Solaris Sendmail are displayed on the **Log Activity** tab.

Chapter 52. SSH CryptoAuditor

The IBM Security QRadar DSM for SSH CryptoAuditor collects logs from an SSH CryptoAuditor.

The following table identifies the specifications for the SSH CryptoAuditor DSM.

Table 79. SSH CryptoAuditor DSM specifications

Specification	Value
Manufacturer	SSH Communications Security
Product	CryptoAuditor
DSM Name	SSH CryptoAuditor
RPM filename	`DSM-SSHCryptoAuditor-`*`QRadar_release-Build_number`*`.noarch.rpm`
Supported versions	1.4.0 or later
Event format	Syslog
QRadar recorded event types	Audit, Forensics
Log source type in QRadar UI	SSH CryptoAuditor
Auto discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	SSH Communications Security website (http://www.ssh.com/)

To send events from SSH CryptoAuditor to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - SSH CryptoAuditor RPM
2. For each instance of SSH CryptoAuditor, configure your SSH CryptoAuditor system to communicate with QRadar.
3. If QRadar does not automatically discover SSH CryptoAuditor, create a log source on the QRadar Console for each instance of SSH CryptoAuditor. Use the following SSH CryptoAuditor specific parameters:

Parameter	Value
Log Source Type	SSH CryptoAuditor
Protocol Configuration	Syslog

Related tasks:

"Configuring an SSH CryptoAuditor appliance to communicate with QRadar" on page 178
To collect SSH CryptoAuditor events, you must configure your third-party appliance to send events to IBM Security QRadar.

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM

RPM manually.

Configuring an SSH CryptoAuditor appliance to communicate with QRadar

To collect SSH CryptoAuditor events, you must configure your third-party appliance to send events to IBM Security QRadar.

Procedure

1. Log in to SSH CryptoAuditor.
2. Go to the syslog settings in **Settings** > **External Services** > **External Syslog Servers**.
3. To create server settings for QRadar, click **Add Syslog Server**.
4. Type the QRadar server settings: address (IP address or FQDN) and port in which QRadar collects log messages.
5. To set the syslog format to Universal LEEF, select the **Leef format** check box.
6. To save the configuration, click **Save**.
7. Configure SSH CryptoAuditor alerts in **Settings** > **Alerts**. The SSH CryptoAuditor alert configuration defines which events are sent to external systems (email or SIEM/syslog).
   a. Select an existing alert group, or create new alert group by clicking **Add alert group**.
   b. Select the QRadar server that you defined earlier in the **External Syslog Server** drop box.
   c. If you created a new alert group, click **Save**. Save the group before binding alerts to the group.
   d. Define which alerts are sent to QRadar by binding alerts to the alert group. Click **[+]** next to the alert that you want to collect in QRadar, and select the alert group that has QRadar as external syslog server. Repeat this step for each alert that you want to collect in QRadar.
   e. Click **Save**.
8. Apply the pending configuration changes. The saved configuration changes do not take effect until you apply them from pending state.

Chapter 53. STEALTHbits StealthINTERCEPT

IBM Security QRadar collects audit logs from a STEALTHbits StealthINTERCEPT server by using the STEALTHbits StealthINTERCEPT DSM.

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT DSM:

Table 80. STEALTHbits StealthINTERCEPT DSM specifications

Specification	Value
Manufacturer	STEALTHbits Technologies
DSM name	STEALTHbits StealthINTERCEPT
RPM file name	`DSM-STEALTHbitsStealthINTERCEPT-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	3.3
Protocol	Syslog LEEF
Recorded event types	Active Directory Audit Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	StealthINTERCEPT (http://www.stealthbits.com/products/stealthintercept)

To integrate STEALTHbits StealthINTERCEPT with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - `DSMCommon` RPM
   - `STEALTHbitsStealthINTERCEPT` RPM
2. Configure your STEALTHbits StealthINTERCEPT device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a STEALTHbits StealthINTERCEPT log source on the QRadar Console. The following table describes the parameters that require specific values for STEALTHbits StealthINTERCEPT event collection:

Table 81. STEALTHbits StealthINTERCEPT log source parameters

Parameter	Value
Log Source type	STEALTHbits StealthINTERCEPT
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring your STEALTHbits StealthINTERCEPT system for communication with QRadar"
To collect all audit logs and system events from STEALTHbits StealthINTERCEPT, you must specify IBM Security QRadar as the syslog server and configure the message format.

Configuring your STEALTHbits StealthINTERCEPT system for communication with QRadar

To collect all audit logs and system events from STEALTHbits StealthINTERCEPT, you must specify IBM Security QRadar as the syslog server and configure the message format.

Procedure

1. Log in to your STEALTHbits StealthINTERCEPT server.
2. Start the Administration Console.
3. Click **Configuration** > **Syslog Server**.
4. Configure the following parameters:

Parameter	Description
Host Address	The IP address of the QRadar Console
Port	514

5. Click **Import mapping file**.
6. Select the `SyslogLeefTemplate.txt` file and press Enter.
7. Click **Save**.
8. On the Administration Console, click **Actions**.
9. Select the mapping file that you imported, and then select the **Send to Syslog** check box.

   Tip: Leave the **Send to Events DB** check box selected. StealthINTERCEPT uses the events database to generate reports.
10. Click **Add**.

Adding a STEALTHbits StealthINTERCEPT log source in QRadar

To collect STEALTHbits StealthINTERCEPT events, configure a log source in IBM Security QRadar.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the Log Source Type list, select **STEALTHbits StealthINTERCEPT**.
7. From the **Protocol Configuration** list, select **Syslog**.
8. Configure the remaining parameters.
9. Click **Save**.
10. On the **Admin** tab, click **Deploy Changes**.

Chapter 54. STEALTHbits StealthINTERCEPT Alerts

IBM Security QRadar collects alerts logs from a STEALTHbits StealthINTERCEPT server by using STEALTHbits StealthINTERCEPT Alerts DSM

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT Alerts DSM:

Table 82. STEALTHbits StealthINTERCEPT Alerts DSM specifications

Specification	Value
Manufacturer	STEALTHbits Technologies
DSM name	STEALTHbits StealthINTERCEPT Alerts
RPM file name	`DSM-STEALTHbitsStealthINTERCEPTAlerts-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	3.3
Protocol	Syslog LEEF
Recorded event types	Active Directory Alerts Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	StealthINTERCEPT (http://www.stealthbits.com/products/stealthintercept)

To integrate STEALTHbits StealthINTERCEPT with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - `DSMCommon` RPM
   - `STEALTHbitsStealthINTERCEPT` RPM
   - `STEALTHbitsStealthINTERCEPTAlerts` RPM
2. Configure your STEALTHbits StealthINTERCEPT device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a STEALTHbits StealthINTERCEPT Alerts log source on the QRadar Console. The following table describes the parameters that require specific values for STEALTHbits StealthINTERCEPT Alerts event collection:

Table 83. STEALTHbits StealthINTERCEPT Alerts log source parameters

Parameter	Value
Log Source type	STEALTHbits StealthINTERCEPT Alerts
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM

RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Collecting alerts logs from STEALTHbits StealthINTERCEPT

To collect all alerts logs from STEALTHbits StealthINTERCEPT, you must specify IBM Security QRadar as the syslog server and configure the message format.

Procedure

1. Log in to your STEALTHbits StealthINTERCEPT server.
2. Start the Administration Console.
3. Click **Configuration** > **Syslog Server**.
4. Configure the following parameters:

Parameter	**Description**
Host Address	The IP address of the QRadar Console
Port	514

5. Click **Import mapping file**.
6. Select the `SyslogLeefTemplate.txt` file and press Enter.
7. Click **Save**.
8. On the Administration Console, click **Actions**.
9. Select the mapping file that you imported, and then select the **Send to Syslog** check box.

   Tip: Leave the **Send to Events DB** check box selected. StealthINTERCEPT uses the events database to generate reports.
10. Click **Add**.

Chapter 55. STEALTHbits StealthINTERCEPT Analytics

IBM Security QRadar collects analytics logs from a STEALTHbits StealthINTERCEPT server by using STEALTHbits StealthINTERCEPT Analytics DSM.

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT Analytics DSM:

Table 84. STEALTHbits StealthINTERCEPT Analytics DSM specifications

Specification	Value
Manufacturer	STEALTHbits Technologies
DSM name	STEALTHbits StealthINTERCEPT Analytics
RPM file name	`DSM-STEALTHbitsStealthINTERCEPTAnalytics-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	3.3
Protocol	Syslog LEEF
Recorded event types	Active Directory Analytics Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	StealthINTERCEPT (http://www.stealthbits.com/products/stealthintercept)

To integrate STEALTHbits StealthINTERCEPT with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - `DSMCommon` RPM
   - `STEALTHbitsStealthINTERCEPT` RPM
   - `STEALTHbitsStealthINTERCEPTAnalytics` RPM
2. Configure your STEALTHbits StealthINTERCEPT device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a STEALTHbits StealthINTERCEPT Analytics log source on the QRadar Console. The following table describes the parameters that require specific values for STEALTHbits StealthINTERCEPT Analytics event collection:

Table 85. STEALTHbits StealthINTERCEPT Analytics log source parameters

Parameter	Value
Log Source type	STEALTHbits StealthINTERCEPT Analytics
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Collecting analytics logs from STEALTHbits StealthINTERCEPT"
To collect all analytics logs from STEALTHbits StealthINTERCEPT, you must specify IBM Security QRadar as the syslog server and configure the message format.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Collecting analytics logs from STEALTHbits StealthINTERCEPT

To collect all analytics logs from STEALTHbits StealthINTERCEPT, you must specify IBM Security QRadar as the syslog server and configure the message format.

Procedure

1. Log in to your STEALTHbits StealthINTERCEPT server.
2. Start the Administration Console.
3. Click **Configuration** > **Syslog Server**.
4. Configure the following parameters:

Parameter	Description
Host Address	The IP address of the QRadar Console
Port	514

5. Click **Import mapping file**.
6. Select the `SyslogLeefTemplate.txt` file and press Enter.
7. Click **Save**.
8. On the Administration Console, click **Actions**.
9. Select the mapping file that you imported, and then select the **Send to Syslog** check box.

   Tip: Leave the **Send to Events DB** check box selected. StealthINTERCEPT uses the events database to generate reports.
10. Click **Add**.

Chapter 56. Symantec Critical System Protection

The IBM Security QRadar DSM for Symantec Critical System Protection can collect event logs from Symantec Critical System Protection systems.

The following table identifies the specifications for the Symantec Critical System Protection DSM.

Table 86. Symantec Critical System Protection DSM specifications

Specification	**Value**
Manufacturer	Symantec
DSM Name	Critical System Protection
RPM file name	`DSM-SymantecCriticalSystemProtection-`*`Qradar_version_build number`*`.noarch.rpm`
Supported versions	5.1.1
Event format	DB Entries
QRadar recorded event types	All events from the 'CSPEVENT_VW´ view
Log source type in QRadar UI	Symantec Critical System Protection
Auto discovered?	No
Includes identity?	No
Includes custom properties	No
For more information	Symantec Web Page (http://www.symantec.com/)

To integrate Symantec Critical System Protection with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most current version of the following RPMs on your QRadar Console:
   - Protocol-JDBC RPM
   - Symantec Critical System Protection RPM
2. For each Symantec Critical System Protection instance, configure Symantec Critical System Protection to enable communication with QRadar.

   Ensure that QRadar can poll the database for events by using TCP port 1433 or the port that is configured for your log source. Protocol connections are often disabled on databases and extra configuration steps are required in certain situations to allow connections for event polling. Configure firewalls that are located between Symantec Critical System Protection and QRadar to allow traffic for event polling.
3. If QRadar does not automatically discover Symantec Critical System Protection, create a log source for each Symantec Critical System Protection instance on the QRadar Console. Use the following values for the required log source parameters:

Parameter	**Description**
Log Source Type	Symantec Critical System Protection
Protocol Configuration	JDBC

Parameter	Description
Database Type	MSDE
Instance	SCSP
Database Name	SCSPDB
Table Name	CSPEVENT_VW
Compare Field	EVENT_ID

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Chapter 57. Sourcefire Defense Center (DC)

The IBM Security QRadar DSM for Sourcefire Defense Center accepts Sourcefire Defense Center events by using the eStreamer API service

QRadar supports Sourcefire Defense Center v4.8.0.2 to v5.2.0.4.

You must download and install one of the following patches from the Sourcefire website to collect Sourcefire Defense Center 5.x events in QRadar:

- `Sourcefire_hotfix-v5.1.0-0-build_1.tar`
- `Sourcefire_hotfix-v5.1.1-0-build_1.tar`

For more information about patches for your Sourcefire appliance, see the Sourcefire website.

Configuration overview

To integrate with Sourcefire Defense Center, you must create certificates in the Sourcefire Defense Center interface, and then add the certificates to the QRadar appliances that receive eStreamer event data.

If your deployment includes multiple Sourcefire Defense Center appliances, you must copy the certificate for each appliance that receives eStreamer events. The certificate allows the Sourcefire Defense Center appliance and the QRadarConsole or Event Collector to communicate by using the eStreamer API to collect events.

To integrate QRadar with Sourcefire Defense Center, use the following steps:

1. Create the eStreamer certificate on your Sourcefire Defense Center appliance.
2. Add the Sourcefire Defense Center certificate files to QRadar.
3. Configure a log source in QRadar for your Sourcefire Defense Center appliances.

Supported event types

QRadar supports the following event types from Sourcefire Defense Center:

- Intrusion events and extra data

  Intrusion events that are categorized by the Sourcefire Defense Center DSM in QRadar use the same QRadar Identifiers (QIDs) as the Snort DSM. To ensure that all intrusion events are categorized properly.

  Intrusion events in the 1,000,000 - 2,000,000 range are user-defined rules in Sourcefire Defense Center. User-defined rules that generate events are added as an Unknown event in QRadar, and include additional information that describes the event type. For example, a user-defined event can identify as Unknown:Buffer Overflow for Sourcefire Defense Center.
- Correlation events
- Metadata events
- Discovery events
- Host events
- User events

Creating Sourcefire 4.x certificates

QRadar requires a certificate for every Sourcefire Defense Center appliance in your deployment. Certificates are generated in pkcs12 format and must be converted to keystore and truststore files, which are usable by QRadar appliances.

Procedure

1. Log in to your Sourcefire Defense Center interface.
2. Select **Operations** > **Configuration** > **eStreamer**.
3. Click the **eStreamer** tab.
4. Click **Create Client**.
5. Select check boxes for the event types Sourcefire Defense Center provides to QRadar.
6. Click **+ Create Client** in the upper right-side of the interface.
7. In the **Hostname** field, type the IP address or host name.
   - If you use a QRadar Console or use an All-in-one appliance to collect eStreamer events, type the IP address or host name of your QRadar Console.
   - If you use a remote Event Collector to collect eStreamer events, type the IP address or host name for the remote Event Collector.
   - If you use High Availability (HA), type the virtual IP address.
8. In the **Password** field, leave the password field blank or type a password for your certificate and click **Save**.

   The new client is added to the **Streamer Client** list and the host is allowed to communicate with the eStreamer API on port 8302.
9. From the **Certificate Location** column, click the client that you created to save the pkcs12 certificate to a file location and click **OK**.

What to do next

You are now ready to import your Sourcefire Defense Center certificate to your QRadar appliance.

Creating Sourcefire 5.x certificates

Certificates are created by Sourcefire Defense Center appliances in your deployment.

About this task

QRadar requires a certificate for every Sourcefire Defense Center appliance in your deployment. Certificates are generated in pkcs12 format and must be converted to a keystore and truststore file, which are usable by QRadar appliances.

Procedure

1. Log in to your Sourcefire Defense Center interface.
2. Select **System** > **Local** > **Registration**.
3. Click the **eStreamer** tab.
4. Select check boxes for the event types Sourcefire Defense Center provides to QRadar and click **Save**.

   Important: For Sourcefire Defense Center 5.x, you must clear the **Impact Flag Alerts** check box.

5. Click **+ Create Client** in the upper right-side of the interface.
6. In the **Hostname** field, type the IP address or host name.
   - If you use QRadar Console or use an All-in-one appliance to collect eStreamer events, type the IP address or host name of your QRadar Console.
   - If you use an Event Collector to collect eStreamer events, type the IP address or host name for the Event Collector.
   - If you use High Availability (HA), type the virtual IP address.
7. In the **Password** field, type a password for your certificate or leave the field blank and click **Save**.

   The new client is added to the Streamer Client list and the host is allowed to communicate with the eStreamer API on port 8302.
8. Click the download arrow for your host to save the pkcs12 certificate to a file location.
9. Click **OK** to download the file.

What to do next

You are now ready to import your Sourcefire Defense Center certificate to your QRadar appliance.

Importing a Sourcefie certificate to QRadar

The estreamer-cert-import.pl script for QRadar converts your pkcs12 certificate file to a keystore and truststore file and places the certificates in the proper directory on your QRadar appliance. Repeat this procedure for each Sourcefire Defense Center pcks12 certificate you need to import to your QRadar Console or Event Collector.

Before you begin

You must have `root` or `su - root` privileges to run the `estreamer-cert-import.pl` import script.

About this task

The `estreamer-cert-import.pl` script is stored on your QRadar appliance when you install the Sourcefire Defense Center protocol.

The script converts and imports one pkcs12 file at a time. You are required only to import a certificate for the QRadar appliance that manages the Sourcefire Defense Center log source. For example, after the Sourcefire event is categorized and normalized by an Event Collector in a QRadar deployment, it is forwarded to the QRadar Console. In this scenario, you would import a certificate to the Event Collector.

When you import a new certificate, existing Sourcefire Defense Center certificates on the QRadar appliance are renamed to `estreamer.keystore.old` and `estreamer.truststore.old`.

Procedure

1. Log in to your QRadar Console or Event Collector as the root user.
2. Copy the pkcs12 certificate from your Sourcefire Defense Center appliance to the following directory:

```
/opt/qradar/bin/
```

3. To import your pkcs12 file, type the following command and any extra parameters

   ```
   /opt/qradar/bin/estreamer-cert-import.pl -f pkcs12_file_name options
   ```

   Extra parameters are described in the following table:

Parameter	Description
-f	Identifies the file name of the pkcs12 files to import.
-o	Overrides the default estreamer name for the keystore and truststore files. Use the -o parameter when you integrate multiple Sourcefire Defense Center devices. For example, /opt/qradar/bin/estreamer-cert-import.pl -f *<file name>* -o 192.168.1.100 The import script creates the following files: • /opt/qradar/conf/192.168.0.100.keystore • /opt/qradar/conf/192.168.0.100.truststore
-d	Enables verbose mode for the import script. Verbose mode is intended to display error messages for troubleshooting purposes when pkcs12 files fail to import properly.
-p	Specifies a password if a password was accidentally provided when you generated the pkcs12 file.
-v	Displays the version information for the import script.
-h	Displays a help message on using the import script.

Results

The import script creates a keystore and truststore file in the following locations:

- /opt/qradar/conf/estreamer.keystore
- /opt/qradar/conf/estreamer.truststore

Configuring a log source for Sourcefire Defense Center events

You must configure a log source because QRadar does not automatically discover Sourcefire Defense Center events.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the Log Source Type list, select **Sourcefire Defense Center**.

7. From the Protocol Configuration list, select **Sourcefire Defense Center Estreamer**.
8. Configure the following parameters:

Parameter	Description
Server Address	The IP address or host name of the Sourcefire Defense Center device.
Server Port	The port number QRadar uses to receive Sourcefire Defense Center Estreamer events.
Keystore Filename	The directory path and file name for the keystore private key and associated certificate.
Truststore Filename	The directory path and file name for the truststore files. The truststore file that contains the certificates that are trusted by the client.
Request Extra Data	Select this option to request extra data from Sourcefire Defense Center Estreamer, for example, extra data includes the original IP address of an event.
Use Extended Requests	Select this option to use an alternative method for retrieving events from an eStreamer source. Extended Requests are supported on Sourcefire DefenseCenter Estreamer version 5.0 or later.

Chapter 58. Sourcefire Intrusion Sensor

The Sourcefire Intrusion Sensor DSM for IBM Security QRadar accepts Snort based intrusion and prevention syslog events from Sourcefire devices.

Configuring Sourcefire Intrusion Sensor

To configure your Sourcefire Intrusion Sensor, you must enable policy alerts and configure your appliance to forward the event to QRadar.

Procedure

1. Log in to your Sourcefire user interface.
2. On the navigation menu, select **Intrusion Sensor** > **Detection Policy** > **Edit**.
3. Select an active policy and click **Edit**.
4. Click **Alerting**.
5. In the **State** field, select on to enable the syslog alert for your policy.
6. From the Facility list, select **Alert**.
7. From the Priority list, select **Alert**.
8. In the **Logging Host** field, type the IP address of the QRadar Console or Event Collector.
9. Click **Save**.
10. On the navigation menu, select **Intrusion Sensor** > **Detection Policy** > **Apply**.
11. Click **Apply**.

What to do next

You are now ready to configure the log source in QRadar.

Configuring a log source for Sourcefire Defense Center events

You must configure a log source because QRadar does not automatically discover Sourcefire Defense Center events.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the Log Source Type list, select **Sourcefire Defense Center**.
7. From the Protocol Configuration list, select **Sourcefire Defense Center Estreamer**.
8. Configure the following parameters:

Parameter	Description
Server Address	The IP address or host name of the Sourcefire Defense Center device.

Parameter	Description
Server Port	The port number QRadar uses to receive Sourcefire Defense Center Estreamer events.
Keystore Filename	The directory path and file name for the keystore private key and associated certificate.
Truststore Filename	The directory path and file name for the truststore files. The truststore file that contains the certificates that are trusted by the client.
Request Extra Data	Select this option to request extra data from Sourcefire Defense Center Estreamer, for example, extra data includes the original IP address of an event.
Use Extended Requests	Select this option to use an alternative method for retrieving events from an eStreamer source. Extended Requests are supported on Sourcefire DefenseCenter Estreamer version 5.0 or later.

Chapter 59. Trend Micro Deep Discovery Analyzer

The IBM Security QRadar DSM for Trend Micro Deep Discovery Analyzer can collect event logs from your Trend Micro Deep Discovery Analyzer console.

The following table identifies the specifications for the Trend Micro Deep Discovery Analyzer DSM:

Table 87. Trend Micro Deep Discovery Analyzer DSM specifications

Specification	**Value**
Manufacturer	Trend Micro
DSM name	Deep Discovery Analyzer
RPM file name	DSM-TrendMicroDeepDiscoveryAnalyzer-*build_number*.noarch.rpm
Supported versions	1.0
Event format	LEEF
QRadar recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Trend Micro website (www.trendmicro.com/DeepDiscovery⌂)

To send Trend Micro Deep Discovery events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the following RPMs.
   - DSMCommon
   - Trend Micro Deep Discovery DSM
2. Configure your Trend Micro Deep Discovery device to communicate with QRadar.
3. If QRadar does not automatically detect Trend Micro Deep Discovery as a log source, create a Trend Micro Deep Discovery log source on the QRadar Console. Configure all required parameters and use the following table to determine specific values that are required for Trend Micro Deep Discovery Inspector event collection:

Table 88. Trend Micro Deep Discovery Analyzer log source parameters

Parameter	**Value**
Log Source type	Trend Micro Deep Discovery Analyzer
Protocol Configuration	Syslog

Related tasks:

"Adding a single DSM" on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

"Configuring your Trend Micro Deep Discovery Analyzer instance for communication with QRadar"
To collect Trend Micro Deep Discovery Analyzer events, configure your third-party instance to enable logging.

"Adding a log source" on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your Trend Micro Deep Discovery Analyzer instance for communication with QRadar

To collect Trend Micro Deep Discovery Analyzer events, configure your third-party instance to enable logging.

Procedure

1. Log in to the Deep Discovery Analyzer web console.
2. Click **Administrator** > **Log Settings**.
3. Select **Forward logs to a syslog server**.
4. Select **LEEF** as the log format.
5. In the **Syslog server** field, type the IP address of your QRadar Console or Event Collector.
6. In the **Port** field, type `514`.

Chapter 60. WatchGuard Fireware OS

The IBM Security QRadar DSM for WatchGuard Fireware OS can collect event logs from your WatchGuard Fireware OS.

The following table identifies the specifications for the WatchGuard Fireware OS DSM:

Table 89. WatchGuard Fireware DSM specifications

Specification	Value
Manufacturer	WatchGuard
DSM name	WatchGuard Fireware OS
RPM file name	DSM-WatchGuardFirewareOS-*QRadar-version-Build_number*.noarch.rpm
Supported versions	Fireware XTM OS v11.9 and later
Event format	syslog
QRadar recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
More information	WatchGuard Website (http://www.watchguard.com/)

To integrate the WatchGuard Fireware OS with QRadar, use the following steps:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console.
   - DSMCommon RPM
   - WatchGuard Fireware OS RPM
2. For each instance of WatchGuard Fireware OS, configure your WatchGuard Fireware OS appliance to enable communication with QRadar. You can use one the following procedures:
   - “Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar” on page 198
   - “Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar” on page 198
3. If QRadar does not automatically discover the WatchGuard Fireware OS log source, create a log source for each instance of WatchGuard Fireware OS on your network.

Related tasks:

“Adding a single DSM” on page 2
If your system is disconnected from the Internet, you might need to install a DSM RPM manually.

“Adding a log source” on page 3
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar

To collect WatchGuard Fireware OS events, you can use the Policy Manager to configure your third-party appliance to send events to QRadar.

Before you begin

You must have Device Administrator access credentials.

Procedure

1. Open the WatchGuard System Manager.
2. Connect to your Firebox or XTM device.
3. Start the Policy Manager for your device.
4. To open the Logging Setup window, select **Setup > Logging**.
5. Select the **Send log messages to this syslog server** check box.
6. In the **IP address** text box, type the IP address for your QRadar Console or Event Collector.
7. In the **Port** text box, type `514`.
8. From the **Log Format** list, select **IBM LEEF**.
9. Optional: Specify the details to include in the log messages.
   a. Click **Configure**.
   b. To include the serial number of the XTM device in the log message details, select the **The serial number of the device** check box.
   c. To include the syslog header in the log message details, select the **The syslog header** check box.
   d. For each type of log message, select one of the following syslog facilities:
      - For high-priority syslog messages, such as alarms, select **Local0**.
      - To assign priorities to other types of log messages, select an option from **Local1** through **Local7**. Lower numbers have greater priority.
      - To not send details for a log message type, select **NONE**.
   e. Click **OK**.
10. Click **OK**.
11. Save the configuration file to your device.

Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar

To collect WatchGuard Fireware OS events, you can use the Fireware XTM web user interface to configure your third-party appliance to send events to QRadar.

Before you begin

You must have Device Administrator access credentials.

Procedure

1. Log in to the Fireware XTM web user interface for your Fireware or XTM device.
2. Select **System > Logging**.

3. In the Syslog Server pane, select the **Send log messages to the syslog server at this IP address** check box.
4. In the **IP Address** text box, type the IP address for the QRadar Console or Event Collector.
5. In the **Port** text box, type 514.
6. From the **Log Format** list, select **IBM LEEF**.
7. Optional: Specify the details to include in the log messages.
   a. To include the serial number of the XTM device in the log message details, select the **The serial number of the device** check box.
   b. To include the syslog header in the log message details, select the **The syslog header** check box.
   c. For each type of log message, select one of the following syslog facilities:
      - For high-priority syslog messages, such as alarms, select **Local0**.
      - To assign priorities to other types of log messages, select an option from **Local1** through **Local7**. Lower numbers have greater priority.
      - To not send details for a log message type, select **NONE**.
8. Click **Save**.

Configuring a WatchGuard Fireware OS log source in QRadar

Use this procedure if your QRadar Console did not automatically discover the WatchGuard Fireware OS log source.

Procedure

1. Log in to QRadar
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. In the **Log Source Identifier** field, type the IP address or host name of the WatchGuard Fireware OS device.
7. From the **Log Source Type** list, select **WatchGuard Fireware OS**.
8. From the **Protocol Configuration** list, select **Syslog**.
9. Configure the remaining parameters.
10. Click **Save**.

Chapter 61. Universal CEF

The IBM Security QRadar DSM for Universal CEF accepts events from any device that produces events in the Common Event Format (CEF).

The following table identifies the specifications for the Universal CEF DSM:

Table 90. Universal CEF DSM specifications

Specification	Value
DSM name	Universal CEF
RPM file name	`DSM-UniversalCEF-`*`Qradar_version-build_number`*`.noarch.rpm`
Protocol	syslog Log File
Recorded event types	CEF-formatted events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No

To send events from a device that generates CEF-formatted events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - Universal CEF RPM
2. Add a Universal CEF log source on the QRadar Console. Use the following values that are specific to Universal CEF:

Parameter	Description
Log Source Type	Universal DSM
Protocol Configuration	Syslog or Log File

3. Configure your third-party device to send events to QRadar. For more information about how to configure your third-party device, see your vendor documentation.
4. Configure event mapping for Universal CEF events.

Configuring event mapping for Universal CEF events

Universal CEF events do not contain a predefined QRadar Identifier (QID) map to categorize security events. You must search for unknown events from the Universal CEF log source and map them to high and low-level categories.

Before you begin

Ensure that you installed the Universal CEF DSM and added log source for it in QRadar.

About this task

By default, the Universal CEF DSM categorizes all events as unknown. All Universal CEF events display a value of **unknown** in the **Event Name** and **Low Level Category** columns on the **Log Activity** tab. You must modify the QID map to individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track events from your network devices.

For more information about event mapping, see the *IBM Security QRadar SIEM Users Guide*.

Procedure

1. Log in to QRadar.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. From the first list, select **Log Source**.
5. From the **Log Source Group** list, select **Other**.
6. From the **Log Source** list, select your Universal CEF log source.
7. Click **Add Filter**.
8. From the **View** list, select **Last Hour**.
9. Optional: Click **Save Criteria** to save your existing search filter.
10. On the **Event Name** column, double-click an unknown event for your Universal CEF DSM.
11. Click **Map Event**.
12. From the Browse for QID pane, select any of the following search options to narrow the event categories for a QRadar Identifier (QID):
    - From the **High-Level Category** list, select a high-level event category. For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *IBM Security QRadar SIEM Administration Guide*.
    - From the **Low-Level Category** list, select a low-level event category.
    - From the **Log Source Type** list, select a log source type.

      Tip: Searching for QIDs by log source is useful when the events from your Universal CEF DSM are similar to another existing network device. For example, if your Universal CEF provides firewall events, you might select Cisco ASA, as another firewall product that likely captures similar events.
    - To search for a QID by name, type a name in the **QID/Name** field.
13. Click **Search**.
14. Select the QID that you want to associate to your unknown Universal CEF DSM event and click **OK**.

Chapter 62. QRadar supported DSMs

IBM Security QRadar can collect events from your security products by using a plugin file that is called a Device Support Module (DSM).

If you can't find the documentation for your DSM in the IBM Knowledge Center, view the PDF library on the customer support web site (http://www-01.ibm.com/support/docview.wss?uid=swg21614644). All DSM documentation for each QRadar release is available from here in PDF format.

The following table lists supported DSMs for third-party and IBM security solutions. The documentation for the DSMs that are marked with an asterisk (*) in the Device name and version column is not yet available in the IBM Knowledge Center. Click the link in the column to download the *IBM Security QRadar DSM Configuration Guide* (PDF download).

Table 91. QRadar Supported DSMs

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
3Com	8800 Series Switch v3.01.30	Syslog	Status and network condition events	Yes	No	No
AccessData	AccessData InSight	Log File	Log file	No	No	No
AhnLab	AhnLab Policy Center	AhnLabPolicy CenterJdbc	Spyware detection Virus detection Audit	No	Yes	No
Amazon	Amazon AWS CloudTrail v1.0	Log File	All events	No	Yes	No
Ambiron	TrustWave ipAngel v4.0	Syslog	Snort-based events	No	No	No
Apache	HTTP Server v1.3 and later*	Syslog	HTTP status	Yes	No	No
APC	UPS	Syslog	Smart-UPS series events	No	No	No
Apple	Mac OS X (10)*	Syslog	Firewall, web server (access/ error), privilege, and information events	No	Yes	No
Application Security, Inc.	DbProtect v6.2, v6.3, v6.3sp1, v6.3.1, and v6.4*	Syslog	All events	Yes	No	No
Arbor Networks	Pravail APS v3.1 and later	Syslog	All events	Yes	No	No
Arpeggio Software	SIFT-IT v3.1 and later*	Syslog	All events configured in the SIFT-IT rule set	Yes	No	No
Array Networks	SSL VPN ArraySP v7.3*	Syslog	All events	No	Yes	Yes
Aruba Networks	Mobility Controllers v2.5 and later*	Syslog	All events	Yes	No	No
Avaya Inc.	Avaya VPN Gateway v9.0.7.2*	Syslog	All events	Yes	Yes	No
BalaBit IT Security	Microsoft Windows Security Event Log v4.x*	Syslog	Microsoft Event Log Events	Yes	Yes	No
BalaBit IT Security	Microsoft ISA v4.x*	Syslog	Microsoft Event Log Events	Yes	Yes	No
Barracuda Networks	Spam & Virus Firewall v5.x and later*	Syslog	All events	Yes	No	No
Barracuda Networks	Web Application Firewall v7.0.x	Syslog	System, web firewall, access, and audit events	Yes	No	No
Barracuda Networks	Web Filter 6.0.x and later*	Syslog	Web traffic and web interface events	Yes	No	No
Bit9	Security Platform v6.0.2 and later	Syslog	All events	Yes	Yes	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
BlueCat Networks	Adonis v6.7.1-P2 and later*	Syslog	DNS and DHCP events	Yes	No	No
Blue Coat	SG v4.x and later	Syslog Log File Protocol	All events	No	No	Yes
Bridgewater Systems	AAA v8.2c1*	Syslog	All events	Yes	Yes	No
Brocade	Fabric OS V7.x*	Syslog	System and audit events	Yes	No	No
CA	Access Control Facility v12 to v15*	Log File Protocol	All events	No	No	Yes
CA	SiteMinder*	Syslog	All events	No	No	No
CA	Top Secret v12 to v15*	Log File Protocol	All events	No	No	Yes
Check Point	FireWall-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX, and R75*	Syslog or OPSEC LEA	All events	Yes	Yes	Yes
Check Point	VPN-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77 NGX	Syslog or OPSEC LEA	All events	Yes	Yes	No
Check Point	Provider-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX*	Syslog or OPSEC LEA	All events	Yes	Yes	No
Cilasoft	Cilasoft QJRN/400 V5.14.K and later*	Syslog	IBM audit events	Yes	Yes	No
Cisco	4400 Series Wireless LAN Controller v7.2	Syslog or SNMPv2	All events	No	No	No
Cisco	CallManager v8.x*	Syslog	Application events	Yes	No	No
Cisco	ACS v4.1 and later if directly from ACS v3.x and later if using ALE	Syslog	Failed Access Attempts	Yes	Yes	No
Cisco	Aironet v4.x and later*	Syslog	Cisco Emblem Format	Yes	No	No
Cisco	ACE Firewall v12.2*	Syslog	All events	Yes	Yes	No
Cisco	ASA v7.x and later*	Syslog	All events	Yes	Yes	No
Cisco	ASA v7.x and later*	NSEL Protocol	All events	No	No	No
Cisco	CSA v4.x, v5.x and v6.x*	Syslog SNMPv1 SNMPv2	All events	Yes	Yes	No
Cisco	CatOS for catalyst systems v7.3 and later*	Syslog	All events	Yes	Yes	No
Cisco	IPS v7.1.10 and later, v7.2.x, v7.3.x	SDEE	All events	No	No	No
Cisco	IronPort v5.5, v6.5, v7.1, and v7.5*	Syslog, Log File Protocol	All events	No	No	No
Cisco	Firewall Service Module (FWSM) v2.1 and later*	Syslog	All events	Yes	Yes	Yes
Cisco	Catalyst Switch IOS, 12.2, 12.5, and later*	Syslog	All events	Yes	Yes	No
Cisco	NAC Appliance v4.x and later*	Syslog	Audit, error, failure, quarantine, and infected events	No	No	No
Cisco	Nexus v6.x*	Syslog	Nexus-OS events	Yes	No	No
Cisco	PIX Firewall v5.x, v6.3, and later*	Syslog	Cisco PIX events	Yes	Yes	Yes
Cisco	IOS 12.2, 12.5, and later*	Syslog	All events	Yes	Yes	No
Cisco	VPN 3000 Concentrator vVPN 3005, 4.1.7.H*	Syslog	All events	Yes	Yes	Yes
Cisco	Wireless Services Modules (WiSM) v 5.1 and later*	Syslog	All events	Yes	No	No
Cisco	Identity Services Engine v1.1*	UDP Multiline Syslog Protocol	Device events	No	Yes	No
Citrix	NetScaler v9.3 to v10.0*	Syslog	All events	Yes	Yes	No
Citrix	Access Gateway v4.5*	Syslog	Access, audit, and diagnostic events	Yes	No	No
CloudPassage	CloudPassage Halo	Syslog, Log file	All events	Yes	No	No
CorreLog	CorreLog Agent for IBM z/OS	Syslog LEEF	All events	Yes	No	No
CRYPTOCard	CRYPTO- Shield v6.3*	Syslog	All events	No	No	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Cyber-Ark	Vault v6.x*	Syslog	All events	Yes	Yes	No
CyberGuard	Firewall/VPN KS1000 v5.1*	Syslog	CyberGuard events	Yes	No	No
Damballa	Failsafe v5.0.2 and later*	Syslog	All events	Yes	No	No
Digital China Networks	DCS and DCRS Series switches v1.8.7 and later*	Syslog	DCS and DCRS IPv4 events	No	No	No
DG Technology	DG Technology MEAS	LEEF Syslog	Mainframe events	Yes	No	No
Enterasys	800-Series Switch*	Syslog	All events	Yes	No	No
Enterasys	Dragon v5.0, 6.x, v7.1, v7.2, v7.3, and v7.4*	Syslog SNMPv1 SNMPv3	All relevant Enterasys Dragon events	Yes	No	No
Enterasys	Matrix Router v3.5*	Syslog SNMPv1 SNMPv2 SNMPv3	SNMP and syslog login, logout, and login failed events	Yes	No	No
Enterasys	NetSight Automatic Security Manager v3.1.2*	Syslog	All events	Yes	No	No
Enterasys	Matrix N/K/S Series Switch v6.x, v7.x*	Syslog	All relevant Matrix K-Series, N-Series and S-Series device events	Yes	No	No
Enterasys	Stackable and Standalone Switches*	Syslog	All events	Yes	Yes	No
Enterasys	XSR Security Router v7.6.14.0002*	Syslog	All events	Yes	No	No
Enterasys	HiGuard Wireless IPS V2R2.0.30*	Syslog	All events	Yes	No	No
Enterasys	HiPath Wireless Controller V2R2.0.30*	Syslog	All events	Yes	No	No
Enterasys	NAC v3.2 and v3.3*	Syslog	All events	Yes	No	No
Extreme Networks	Extreme Ware v7.7 and XOS v12.4.1.x*	Syslog	All events	No	Yes	No
F5 Networks	BIG-IP AFM v11.3*	Syslog	Network, network DoS, protocol security, DNS, and DNS DoS events	Yes	No	No
F5 Networks	BIG-IP LTM v4.5, v9.x to v11.x*	Syslog	All events	No	Yes	No
F5 Networks	BIG-IP ASM v10.2*	Syslog	All events	No	Yes	No
F5 Networks	BIG-IP APM v10.x, and v11.x*	Syslog	All events	Yes	No	No
F5 Networks	FirePass v7.0*	Syslog	All events	Yes	Yes	No
Fair Warning	Fair Warning v2.9.2*	Log File Protocol	All events	No	No	No
Fidelis Security Systems	Fidelis XPS 7.3.x*	Syslog	Alert events	Yes	No	No
FireEye	FireEye CMS, MPS, EX, AX, NX, FX, and HX	Syslog	All relevant events Common Event Format (CEF) formatted messages Log Extended Format (LEEF)	No	Yes	No
FreeRADIUS	FreeRADIUS V2.x	Syslog	All events	Yes	Yes	No
ForeScout	CounterACT v7.x and later*	Syslog	Denial of Service, system, exploit, authentication, and suspicious events	No	No	No
Fortinet	FortiGate FortiOS v2.5 and later*	Syslog	All events	Yes	Yes	Yes
Foundry	FastIron v3.x.x and v4.x.x*	Syslog	All events	Yes	Yes	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
genua	genugate 8.2 and later	Syslog	General error messages High availability General relay messages Relay-specific messages genua programs/daemons EPSI Accounting Daemon - gg/src/acctd Configfw FWConfig ROFWConfig User-Interface Webserver	Yes	Yes	No
Great Bay	Beacon*	Syslog	All events	Yes	Yes	No
HBGary	Active Defense v1.2 and later*	Syslog	All events	Yes	No	No
HP	Tandem*	Log File Protocol	Safe Guard Audit file events	No	No	No
HP	ProCurve K.14.52*	Syslog	All events	Yes	No	No
HP	UX v11.x and later*	Syslog	All events	No	Yes	No
Honeycomb Technologies	Lexicon File Integrity Monitor mesh service v3.1 and later*	Syslog	integrity events	Yes	No	No
Huawei	S Series Switch S5700, S7700, and S9700 using V200R001C00	Syslog	IPv4 events from S5700, S7700, and S9700 Switches	No	No	No
Huawei	AR Series Router (AR150, AR200, AR1200, AR2200, and AR3200 routers using V200R002C00)	Syslog	IPv4 events	No	No	No
IBM	AIX® v6.1 and v7.1	Syslog, Log File Protocol	Configured audit events	Yes	No	No
IBM	AIX 5.x, 6.x, and v7.x	Syslog	Authentication and operating system events	Yes	Yes	No
IBM	AS/400iSeries DSM V5R4 and later	Log File Protocol	All events	No	Yes	No
IBM	AS/400 iSeries - Robert Townsend Security Solutions V5R1 and later	Syslog	CEF formatted messages	Yes	Yes	No
IBM	AS/400 iSeries - Powertech Interact V5R1 and later	Syslog	CEF formatted messages	Yes	Yes	No
IBM	Federated Directory Server V7.2.0.2 and later*	LEEF	FDS Audit	Yes	No	No
IBM	InfoSphere® 8.2p45	Syslog	Policy builder events	No	No	No
IBM	ISS Proventia M10 v2.1_2004.1122_15.13.53*	SNMP	All events	No	No	No
IBM	Lotus® Domino® v8.5*	SNMP	All events	No	No	No
IBM	Proventia Management SiteProtector™ v2.0 and v2.9*	JDBC	IPS and audit events	No	No	No
IBM	RACF® v1.9 to v1.13*	Log File Protocol	All events	No	No	Yes
IBM	CICS® v3.1 to v4.2*	Log File Protocol	All events	No	No	Yes
IBM	DB2® v8.1 to v10.1*	Log File Protocol	All events	No	No	Yes
IBM	z/OS® v1.9 to v1.13	Log File Protocol	All events	No	No	Yes
IBM	Informix® v11*	Log File Protocol	All events	No	No	No
IBM	IMS™*	Log File Protocol	All events	No	No	No
IBM	Security Network Protection (XGS) v5.0 with fixpack 7*	Syslog	System, access, and security events	Yes	No	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
IBM	Security Network IPS v4.6 and later	Syslog	Security, health, and system events	Yes	No	No
IBM	Security Identity Manager 6.0.x and later*	JDBC	Audit and recertification events	No	Yes	No
IBM	IBM Security Trusteer Apex™ Advanced Malware Protection	Syslog/LEEF Log File Protocol	Malware Detection Exploit Detection Data Exfiltration Detection Lockdown for Java™ Event File Inspection Event Apex Stopped Event Apex Uninstalled Event Policy Changed Event ASLR Violation Event ASLR Enforcement Event Password Protection Event	Yes	Yes	No
IBM	IBM SmartCloud Orchestrator v2.3 FP1 and later	IBM SmartCloud Orchestrator REST API	Audit Records	No	Yes	No
IBM	Tivoli® Access Manager IBM Web Security Gateway v7.x*	Syslog	audit, access, and HTTP events	Yes	Yes	No
IBM	Tivoli Endpoint Manager v8.2.x and later	IBM Tivoli Endpoint Manager SOAP Protocol	Server events	No	Yes	No
IBM	WebSphere® Application Server 5.0.x to 6.1	Log File Protocol	All events	No	Yes	No
IBM	WebSphere DataPower® FirmwareV6 and V7	Syslog	All events	Yes	No	No
IBM	zSecure™ Alert v1.13.x and later*	UNIX syslog	Alert events	Yes	Yes	No
IBM	Security Access Manager v8.1 and v8.2*	Syslog	Audit, system, and authentication events	Yes	No	No
IBM	Security Directory v6.3.1 and later*	Syslog LEEF	All events	Yes	Yes	No
Imperva	SecureSphere v6.2 and v7.x or 9.5 and 10.0 (LEEF)*	Syslog	All events	Yes	No	No
Infoblox	NIOS v6.x*	Syslog	All events	No	Yes	No
Internet Systems Consortium (ISC)	BIND v9.9*	Syslog	All events	Yes	No	No
iT-CUBE	agileSI v1.x*	SMB Tail	AgileSI SAP events	No	Yes	No
Itron	Openway Smart Meter*	Syslog	All events	Yes	No	No
Juniper Networks	AVT*	JDBC	All events	No	No	Yes
Juniper Networks	DDoS Secure*	Syslog	All events	Yes	No	No
Juniper Networks	DX*	Syslog	Status and network condition events	Yes	No	Yes
Juniper Networks*	Infranet Controller v2.1, v3.1 & v4.0*	Syslog	All events	No	Yes	Yes
Juniper Networks	Firewall and VPN v5.5r3 and later*	Syslog	NetScreen Firewall events	Yes	Yes	Yes
Juniper Networks	Junos WebApp Secure v4.2.x	Syslog	Incident and access events	Yes	No	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Juniper Networks	IDP v4.0, v4.1 & v5.0	Syslog	NetScreen IDP events	Yes	No	Yes
Juniper Networks	Network and Security Manager (NSM) and Juniper SSG v2007.1r2 to 2007.2r2, 2008.r1, 2009r1.1, 2010.x*	Syslog	NetScreen NSM events	Yes	No	Yes
Juniper Networks	Junos OS v7.x to v10.x Ex Series* Ethernet Switch DSM only supports v9.0 to v10.x*	Syslog or PCAP Syslog***	All events	Yes**	Yes	Yes
Juniper Networks	Secure Access RA* Juniper SA version 6.1R2 and Juniper IC version 2.1*	Syslog	All events	Yes	Yes	Yes
Juniper Networks	Juniper Security Binary Log Collector SRX or J Series appliances at v12.1 or above	Binary	Audit, system, firewall, and IPS events	No	No	Yes
Juniper Networks	Steel-Belted Radius v5.x and later*	Syslog	All events	Yes	Yes	Yes
Juniper Networks	vGW Virtual Gateway v4.5*	Syslog	Firewall, admin, policy and IDS Log events	Yes	No	No
Juniper Networks	Wireless LAN Controller* Wireless LAN devices with Mobility System Software (MSS) V7.6 and later*	Syslog	All events	Yes	No	No
Kaspersky	Security Center v9.2 and later	JDBC, LEEF	Antivirus, server, and audit events	No	Yes	No
Kisco	Kisco Information Systems SafeNet/i V10.11	Log File	All events	No	No	No
Lastline	Lastline Enterprise 6.0	LEEF	Anti-malware	Yes	No	No
Lieberman	Random Password Manager v4.8x*	Syslog	All events	Yes	No	No
Linux	Open Source Linux OS v2.4 and later*	Syslog	Operating system events	Yes	Yes	No
Linux	DHCP Server v2.4 and later*	Syslog	All events from a DHCP server	Yes	Yes	No
Linux	IPtables kernel v2.4 and later*	Syslog	Accept, Drop, or Reject events	Yes	No	No
McAfee	Intrushield v2.x - v5.x*	Syslog	Alert notification events	Yes	No	No
McAfee	Intrushield v6.x - v7.x*	Syslog	Alert and fault notification events	Yes	No	No
McAfee	ePolicy Orchestrator v3.5 to v4.6	JDBC, SNMPv2, SNMPv3	AntiVirus events	No	No	No
McAfee	Application / Change Control v4.5.x*	JDBC	Change management events	No	Yes	No
McAfee	Web v6.0.0 and later*	Syslog, Log File Protocol	All events	Yes	No	No
MetaInfo	MetaIP v5.7.00-6059 and later*	Syslog	All events	Yes	Yes	No
Microsoft	IIS v6.0 and 7.0*	Syslog	HTTP status code events	Yes	No	No
Microsoft	Internet and Acceleration (ISA) Server or Threat Management Gateway 2006*	Syslog	ISA or TMG events	Yes	No	No
Microsoft	Exchange Server 2003, 2007, and 2010	Windows Exchange Protocol	Exchange mail and security events	No	No	No
Microsoft	Endpoint Protection 2012*	JDBC	Malware detection events	No	No	No
Microsoft	Hyper V v2008 and v2012*	WinCollect	All events	No	No	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Microsoft	IAS Server v2000, 2003, and 2008	Syslog	All events	Yes	No	No
Microsoft	Microsoft Windows Event Security Log v2000, 2003, 2008, XP, Vista, and Windows 7 (32 or 64-bit systems supported)	Syslog non-Syslog MicrosoftWindows Event Log Protocol Source Common Event Format (CEF) format, Log Event Extended Format (LEEF)	All events	Yes	Yes	Yes
Microsoft	SQL Server 2008, 2012, and 2014	JDBC	SQL Audit events	No	No	No
Microsoft	SharePoint 2010*	JDBC	SharePoint audit, site, and file events	No	No	No
Microsoft	DHCP Server 2000/2003*	Syslog	All events	Yes	Yes	No
Microsoft	Operations Manager 2005*	JDBC	All events	No	No	No
Microsoft	System Center Operations Manager 2007*	JDBC	All events	No	No	No
Motorola	Symbol AP firmware v1.1 to 2.1*	Syslog	All events	No	No	No
NetApp	Data ONTAP*	Syslog	CIFS events	Yes	Yes	No
Netskope	Netskope Active	Netskope Active REST API	Alert, All events	No	Yes	No
Niksun	NetVCR 2005 v3.x*	Syslog	Niksun events	No	No	No
Nokia	Firewall NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and later*	Syslog or OPSEC LEA	All events	Yes	Yes	No
Nokia	VPN-1 NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and later	Syslog or OPSEC LEA	All events	Yes	Yes	No
Nominum	Vantio v5.3*	Syslog	All events	Yes	No	No
Nortel	Contivity *	Syslog	All events	Yes	No	No
Nortel	Application Switch v3.2 and later*	Syslog	Status and network condition events	No	Yes	No
Nortel	ARN v15.5	Syslog	All events	Yes	No	No
Nortel*	Ethernet Routing Switch 2500 v4.1*	Syslog	All events	No	Yes	No
Nortel*	Ethernet Routing Switch 4500 v5.1*	Syslog	All events	No	Yes	No
Nortel*	Ethernet Routing Switch 5500 v5.1*	Syslog	All events	No	Yes	No
Nortel	Ethernet Routing Switch 8300 v4.1*	Syslog	All events	No	Yes	No
Nortel	Ethernet Routing Switch 8600 v5.0*	Syslog	All events	No	Yes	No
Nortel	VPN Gateway v6.0, 7.0.1 and later, v8.x*	Syslog	All events	Yes	Yes	No
Nortel	Secure Router v9.3, v10.1*	Syslog	All events	Yes	Yes	No
Nortel	Secure Network Access Switch v1.6 and v2.0*	Syslog	All events	Yes	Yes	No
Nortel	Switched Firewall 5100 v2.4*	Syslog or OPSEC	All events	Yes	Yes	No
Nortel	Switched Firewall 6000 v4.2*	Syslog or OPSEC	All events	Yes	Yes	No
Nortel	Threat Protection System v4.6 and v4.7*	Syslog	All events	No	No	No
Novell	eDirectory v2.7*	Syslog	All events	Yes	No	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
ObserveIT	ObserveIT 5.7.x and later*	JDBC	Alerts User Activity System Events Session Activity DBA Activity	No	Yes	No
OpenBSD Project	OpenBSD v4.2 and later*	Syslog	All events	No	Yes	No
Open LDAP Foundation	Open LDAP 2.4.x*	UDP Multiline Syslog	All events	No	No	No
Open Source	SNORT v2.x*	Syslog	All events	Yes	No	No
OpenStack	OpenStack V2014.1	HTTP Reciever	Audit events	No	No	No
Oracle	Audit Records v9i, v10g, and v11g*	Syslog JDBC	All relevant Oracle events	Yes	Yes	No
Oracle	Audit Vault v10.2.3.2 and later*	JDBC	Oracle events	No	No	No
Oracle	OS Audit v9i, v10g, and v11g*	Syslog	Oracle events	Yes	Yes	No
Oracle	BEA WebLogic v10.3.x*	Log File Protocol	Oracle events	No	No	No
Oracle	Database Listener v9i, v10g, and v11g*	Syslog	Oracle events	Yes	No	No
Oracle	Fine Grained Auditing v9i and v10g*	JDBC	Select, insert, delete, or update events for tables configured with a policy	No	No	No
OSSEC	OSSEC v2.6 and later*	Syslog	All relevant	Yes	No	No
Palo Alto Networks	PanOS v3.0 and later	Syslog	All events	Yes	Yes	No
Pirean	Access: One v2.2 with DB2 v9.7*	JDBC	Access management and authentication events	No	No	No
PostFix	Mail Transfer Agent v2.6.6 and later*	UDP Multiline Protocol or Syslog	Mail events	No	No	No
ProFTPd	ProFTPd v1.2.x, v1.3.x*	Syslog	All events	Yes	Yes	No
Proofpoint	Proofpoint Enterprise Protection and Enterprise Privacy versions 7.0.2, 7.1, or 7.2*	Syslog	System, email audit, email encryption, and email security threat classification events	No	No	No
Radware	DefensePro v4.23 and 5.01*	Syslog	All events	Yes	No	No
Raz-Lee iSecurity	AS/400 iSeries Firewall 15.7 and Audit 11.7*	Syslog	Security and audit events	Yes	Yes	No
Redback Networks	ASE v6.1.5*	Syslog	All events	Yes	No	No
Riverbed	SteelCentral NetProfiler	JDBC	Alert events	No	No	No
Riverbed	SteelCentral NetProfiler Audit	Log file protocol	Audit events	No	Yes	No
RSA	Authentication Manager v6.x, v7.x and v8.x	Syslog or Log File Protocol	All events	No	No	No
SafeNet	DataSecure v6.3.0 and later	Syslog	All events	Yes	No	No
Salesforce	Security Auditing	Log File	Setup Audit Records	No	No	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Salesforce	Security Monitoring	Salesforce REST API Protocol	Login History Account History Case History Entitlement History Service Contract History Contract Line Item History Contract History Contact History Lead History Opportunity History Solution History	No	Yes	No
Samhain Labs	HIDS v2.4*	Syslog JDBC	All events	Yes	No	No
Secure Computing	Sidewinder G2 v61*	Syslog	All events	Yes	No	No
Sentrigo	Hedgehog v2.5.3*	Syslog	All events	Yes	No	No
SolarWinds	Orion v2011.2*	Syslog	All events	Yes	No	No
SonicWALL	UTM/Firewall/VPN Appliance v3.x and later*	Syslog	All events	Yes	No	No
Sophos	Astaro v8.x*	Syslog	All events	Yes	No	No
Sophos	Enterprise Console v4.5.1 and v5.1*	Sophos Enterprise Console protocol JDBC	All events	No	No	No
Sophos	PureMessage v3.1.0.0 and later for Microsoft Exchange v5.6.0 for Linux*	JDBC	Quarantined email events	No	No	No
Sophos	Web Security Appliance v3.x*	Syslog	Transaction log events	Yes	No	No
Sourcefire	Intrusion Sensor IS 500, v2.x, 3.x, 4.x	Syslog	All events	Yes	No	No
Sourcefire	Defense Center v4.8.0.2 to v5.2.0.4.	Sourcefire Defense Center	All events	No	No	No
Splunk	Microsoft Windows Security Event Log*	Windows-based event provided by Splunk Forwarders	All events	No	Yes	No
Squid	Web Proxy v2.5 and later*	Syslog	All cache and access log events	Yes	No	No
Startent Networks	Startent Networks*	Syslog	All events	Yes	No	No
STEALTHbits Technologies	StealthINTERCEPT	Syslog LEEF	Active Directory Audit Events	Yes	No	No
STEALTHbits Technologies	STEALTHbits StealthINTERCEPT Alerts	Syslog LEEF	Active Directory Alerts Events	Yes	No	No
STEALTHbits Technologies	STEALTHbits StealthINTERCEPT Analytics	Syslog LEEF	Active Directory Analytics Events	Yes	No	No
Stonesoft	Management Center v5.4*	Syslog	Management Center, IPS, Firewall, and VPN Events	Yes	No	No
Sun	Solaris v5.8, v5.9, Sun OS v5.8, v5.9*	Syslog	All events	Yes	Yes	No
Sun	Solaris DHCP v2.8*	Syslog	All events	Yes	Yes	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Sun	Solaris Sendmail v2.x	Syslog Log File Protocol Proofpoint 7.5 and 8.0 Sendmail log	All events	Yes	No	No
Sun	Solaris Basic Security Mode (BSM) v5.10 and later*	Log File Protocol	All events	No	Yes	No
Sun	ONE LDAP v11.1	Log File Protocol	All relevant access and LDAP events	No	No	No
Sybase	ASE v15.0 and later*	JDBC	All events	No	No	No
Symantec	Endpoint Protection v11 and v12*	Syslog	All Audit and Security Logs	Yes	No	Yes
Symantec	SGS Appliance v3.x and later*	Syslog	All events	Yes	No	Yes
Symantec	SSC v10.1*	JDBC	All events	Yes	No	No
Symantec	Data Loss Prevention (DLP) v8.x and later*	Syslog	All events	No	No	No
Symantec	PGP Universal Server 3.0.x*	Syslog	All events	Yes	No	No
Symark	PowerBroker 4.0*	Syslog	All events	Yes	No	No
ThreatGRID	Malware Threat Intelligence Platform v2.0*	Log file protocol Syslog	Malware events	No	No	No
TippingPoint	Intrusion Prevention System (IPS) v1.4.2 to v3.2.x*	Syslog	All events	No	No	No
TippingPoint	X505/X506 v2.5 and later*	Syslog	All events	Yes	Yes	No
Top Layer	IPS 5500 v4.1 and later*	Syslog	All events	Yes	No	No
Trend Micro	Control Manager v5.0 or v5.5 with hotfix 1697 or hotfix 1713 after SP1 Patch 1*	SNMPv1 SNMPv2 SNMPv3	All events	Yes	No	No
Trend Micro	Deep Discovery v3.x	Syslog	All events	Yes	No	No
Trend Micro	InterScan VirusWall v6.0 and later*	Syslog	All events	Yes	No	No
Trend Micro	Office Scan v8.x and v10.x*	SNMPv2	All events	No	No	No
Tripwire	Enterprise Manager v5.2 and later*	Syslog	Resource additions, removal, and modification events	Yes	No	No
Tropos Networks	Tropos Control v7.7*	Syslog	Fault management, login/logout, provision, and device image upload events	No	No	No
Trusteer®	Apex Local Event Aggregator v1304.x and later*	Syslog	Malware, exploit, and data exfiltration detection events	Yes	No	No
Universal	Syslog and SNMP	Syslog SNMP SDEE	All events	No	Yes	No
Universal	Syslog	Syslog Log File Protocol	All events	No	Yes	No
Universal	Authentication Server	Syslog	All events	No	Yes	No
Universal	Firewall	Syslog	All events	No	No	No
Verdasys	Digital Guardian 6.0.x*	Syslog	All events	Yes	No	No
Vericept	Content 360 up to v8.0*	Syslog	All events	Yes	No	No
VMware	VMware ESX or ESXi 3.5.x, 4.x, and 5.x*	Syslog VMWare protocol	All events	Yes if syslog	No	No
VMware	vCenter v5.x*	VMWare protocol	All events	No	No	No

Table 91. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
VMware	vCloud v5.1*	vCloud protocol	All events	No	Yes	No
VMWare	vShield*	Syslog	All events	Yes	No	No
Vormetric, Inc.	Vormetric Data Security*	Syslog (LEEF)	Audit Alarm Warn Learn Mode System	Yes	No	No
Watchguard	WatchGuard Fireware OS	Syslog	All events	Yes	No	No
Websense	TRITON v7.7*	Syslog	All events	Yes	No	No
Websense	V Series Data Security Suite (DSS) v7.1.x and later*	Syslog	All events	Yes	No	No
Websense	V Series Content Gateway v7.1.x and later*	Log File Protocol	All events	No	No	No
Zscaler	Zscaler NSS v4.1*	Syslog	Web log events	Yes	No	No

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).

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a 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.

Printed in USA