Note
Before using this information and the product that it supports, read the information in “Notices” on page 1193.

Product information
This document applies to IBM® QRadar® Security Intelligence Platform V7.2.1 and subsequent releases unless superseded by an updated version of this document.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Contents

About this DSM Configuration Guide................................................................. xxvii

Part 1. QRadar DSM installation and log source management........................... 1

Chapter 1. Event collection from third-party devices......................................... 3
  Adding a DSM............................................................................................... 4
  Adding a log source.................................................................................... 4
  Adding bulk log sources............................................................................ 6
  Adding a log source parsing order............................................................. 6

Chapter 2. Threat use cases by log source type............................................... 9

Chapter 3. Troubleshooting DSMs................................................................. 21

Part 2. Log sources.......................................................................................... 23

Chapter 4. Introduction to log source management........................................ 25

Chapter 5. Adding a log source...................................................................... 27

Chapter 6. Undocumented Protocols.............................................................. 29
  Configuring an undocumented protocol................................................... 29

Chapter 7. Protocol configuration options...................................................... 31
  Akamai Kona REST API protocol configuration options............................. 31
  Amazon AWS S3 REST API protocol configuration options....................... 32
  Amazon Web Services protocol configuration options.............................. 37
  Apache Kafka protocol configuration options.......................................... 40
    Configuring Apache Kafka to enable Client Authentication........................ 43
    Configuring Apache Kafka to enable SASL Authentication....................... 46
    Troubleshooting Apache Kafka .............................................................. 48
  Blue Coat Web Security Service REST API protocol configuration options..... 49
  Centrify Redrock REST API protocol configuration options....................... 49
  Cisco Firepower eStreamer protocol configuration options....................... 51
  Cisco NSEL protocol configuration options.............................................. 52
  EMC VMware protocol configuration options........................................... 53
  Forwarded protocol configuration options............................................... 53
  HTTP Receiver protocol configuration options.......................................... 54
  IBM BigFix SOAP protocol configuration options........................................ 54
  JDBC protocol configuration options......................................................... 55
  JDBC - SiteProtector protocol configuration options.................................... 59
  Juniper Networks NSM protocol configuration options............................. 61
  Juniper Security Binary Log Collector protocol configuration options........ 61
  Log File protocol configuration options.................................................... 62
  Microsoft Azure Event Hubs protocol configuration options..................... 63
  Microsoft DHCP protocol configuration options........................................ 65
  Microsoft Exchange protocol configuration options.................................... 67
  Microsoft IIS protocol configuration options............................................. 69
  Microsoft Security Event Log protocol configuration options................... 71
    Microsoft Security Event Log over MSRPC Protocol................................ 71
Chapter 24. Arbor Networks.................................................................................................................. 203
  Arbor Networks Peakflow SP............................................................................................................... 203
  Supported event types for Arbor Networks Peakflow SP................................................................. 204
  Configuring a remote syslog in Arbor Networks Peakflow SP........................................................ 204
  Configuring global notifications settings for alerts in Arbor Networks Peakflow SP.................... 204
  Configuring alert notification rules in Arbor Networks Peakflow SP............................................. 205
  Configuring an Arbor Networks Peakflow SP log source.............................................................. 206
  Arbor Networks Pravail....................................................................................................................... 207
  Configuring your Arbor Networks Pravail system to send events to IBM QRadar....................... 208

Chapter 25. Arpeggio SIFT-IT.................................................................................................................. 209
  Configuring a SIFT-IT agent.............................................................................................................. 209
  Configuring a Arpeggio SIFT-IT log source.................................................................................... 210
  Additional information.................................................................................................................... 211

Chapter 26. Array Networks SSL VPN.................................................................................................. 213
  Configuring a log source................................................................................................................ 213

Chapter 27. Aruba Networks.................................................................................................................. 215
  Aruba ClearPass Policy Manager..................................................................................................... 215
  Configuring Aruba ClearPass Policy Manager to communicate with QRadar................................ 216
  Aruba Introspect.............................................................................................................................. 216
  Configuring Aruba Introspect to communicate with QRadar........................................................ 218
  Aruba Mobility Controllers............................................................................................................. 219
  Configuring your Aruba Mobility Controller.................................................................................. 219
  Configuring a log source................................................................................................................ 220

Chapter 28. Avaya VPN Gateway........................................................................................................ 221
  Avaya VPN Gateway DSM integration process............................................................................. 221
  Configuring your Avaya VPN Gateway system for communication with IBM QRadar................ 222
  Configuring an Avaya VPN Gateway log source in IBM QRadar................................................ 222

Chapter 29. BalaBit IT Security.............................................................................................................. 223
  BalaBit IT Security for Microsoft Windows Events........................................................................ 223
  Configuring the Syslog-ng Agent event source............................................................................. 223
  Configuring a syslog destination.................................................................................................... 224
  Restarting the Syslog-ng Agent service............................................................................................ 225
  Configuring a log source................................................................................................................ 225
  BalaBit IT Security for Microsoft ISA or TMG Events.................................................................... 226
  Configure the BalaBit Syslog-ng Agent............................................................................................ 226
  Configuring the BalaBit Syslog-ng Agent file source.................................................................. 226
  Configuring a BalaBit Syslog-ng Agent syslog destination........................................................... 227
  Filtering the log file for comment lines........................................................................................... 227
  Configuring a BalaBit Syslog-ng PE Relay.................................................................................... 228
  Configuring a log source................................................................................................................ 229

Chapter 30. Barracuda............................................................................................................................. 231
  Barracuda Spam & Virus Firewall................................................................................................. 231
  Configuring syslog event forwarding............................................................................................ 231
  Configuring a log source................................................................................................................ 231
  Barracuda Web Application Firewall.............................................................................................. 232
  Configuring Barracuda Web Application Firewall to send syslog events to QRadar.................... 233
  Configuring Barracuda Web Application Firewall to send syslog events to QRadar for devices that do not support LEEF................................................................. 233
  Barracuda Web Filter..................................................................................................................... 234
  Configuring syslog event forwarding............................................................................................ 235
  Configuring a log source................................................................................................................ 235
Chapter 31. BeyondTrust PowerBroker ................................................................. 237
    Configuring BeyondTrust PowerBroker to communicate with QRadar .......... 238
    BeyondTrust PowerBroker DSM specifications ........................................... 239
    Sample event messages ............................................................................ 240

Chapter 32. BlueCat Networks Adonis .............................................................. 241
    Supported event types ............................................................................ 241
    Event type format ................................................................................... 241
    Configuring BlueCat Adonis .................................................................. 242
    Configuring a log source in IBM QRadar ................................................ 242

Chapter 33. Blue Coat ...................................................................................... 243
    Blue Coat SG ......................................................................................... 243
        Creating a custom event format ......................................................... 244
        Creating a log facility ..................................................................... 245
        Enabling access logging ................................................................ 245
    Configuring Blue Coat SG for FTP uploads ............................................ 246
    Configuring a Blue Coat SG Log Source ................................................. 246
    Configuring Blue Coat SG for syslog ..................................................... 246
    Creating extra custom format key-value pairs ........................................ 250
    Blue Coat Web Security Service .............................................................. 250
    Configuring Blue Coat Web Security Service to communicate with QRadar 252

Chapter 34. Box .............................................................................................. 253
    Configuring Box to communicate with QRadar ........................................ 255

Chapter 35. Bridgewater .................................................................................. 257
    Configuring Syslog for your Bridgewater Systems Device ....................... 257
    Configuring a log source ...................................................................... 257

Chapter 36. Brocade Fabric OS ....................................................................... 259
    Configuring syslog for Brocade Fabric OS appliances ............................ 259

Chapter 37. CA Technologies ........................................................................ 261
    CA ACF2 .............................................................................................. 261
        Create a log source for near real-time event feed ............................ 262
        Creating a log source for Log File protocol .................................... 262
        Integrate CA ACF2 with IBM QRadar by using audit scripts .......... 266
        Configuring CA ACF2 that uses audit scripts to integrate with IBM QRadar 266
    CA SiteMinder ..................................................................................... 269
        Configuring a log source ................................................................. 269
        Configuring Syslog-ng for CA SiteMinder ...................................... 271
    CA Top Secret ...................................................................................... 272
        Creating a log source for Log File protocol .................................... 272
        Create a log source for near real-time event feed ............................ 273
        Integrate CA Top Secret with IBM QRadar by using audit scripts ...... 277
        Configuring CA Top Secret that uses audit scripts to integrate with IBM QRadar 277

Chapter 38. Carbon Black .............................................................................. 281
    Carbon Black ....................................................................................... 281
        Configuring Carbon Black to communicate with QRadar ................. 282
    Carbon Black Protection ....................................................................... 283
        Configuring Carbon Black Protection to communicate with QRadar 284
    Carbon Black Bit9 Parity ....................................................................... 285
        Configuring a log source for Carbon Black Bit9 Parity ...................... 285
    Bit9 Security Platform .......................................................................... 286
        Configuring Carbon Black Bit9 Security Platform to communicate with QRadar 287
Configuring syslog forwarding in BIG-IP LTM ................................................................. 458
Configuring Remote Syslog for F5 BIG-IP LTM V11.x to V14.x .................................. 458
Configuring Remote Syslog for F5 BIG-IP LTM V10.x ..................................................... 459
Configuring Remote Syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8................................. 459
F5 Networks FirePass........................................................................................................ 460
Configuring syslog forwarding for F5 FirePass.............................................................. 460
Configuring a log source ............................................................................................... 460

Chapter 61. Fair Warning................................................................................................ 463
Configuring a log source ............................................................................................... 463

Chapter 62. Fasoo Enterprise DRM.................................................................................. 465
Configuring Fasoo Enterprise DRM to communicate with QRadar.............................. 469

Chapter 63. Fidelis XPS................................................................................................... 471
Configuring Fidelis XPS................................................................................................ 471
Configuring a log source ............................................................................................... 472

Chapter 64. FireEye........................................................................................................... 473
Configuring your FireEye system for communication with QRadar.............................. 475
Configuring your FireEye HX system for communication with QRadar....................... 475

Chapter 65. Forcepoint.................................................................................................... 477
FORCEPOINT Stonesoft Management Center................................................................. 477
Configuring FORCEPOINT Stonesoft Management Center to communicate with QRadar 478
Configuring a syslog traffic rule for FORCEPOINT Stonesoft Management Center........ 479
Forcepoint Sidewinder.................................................................................................... 480
Forcepoint Sidewinder DSM specifications................................................................. 481
Configure Forcepoint Sidewinder to communicate with QRadar.................................. 481
Sample event messages............................................................................................... 481
Forcepoint TRITON........................................................................................................ 482
Configuring syslog for Forcepoint TRITON................................................................. 483
Configuring a log source for Forcepoint TRITON....................................................... 483
Forcepoint V-Series Data Security Suite....................................................................... 484
Configuring syslog for Forcepoint V-Series Data Security Suite................................ 484
Configuring a log source for Forcepoint V-Series Data Security Suite......................... 485
Forcepoint V-Series Content Gateway.......................................................................... 485
Configure syslog for Forcepoint V-Series Content Gateway......................................... 485
Configuring the Management Console for Forcepoint V-Series Content Gateway....... 486
Enabling Event Logging for Forcepoint V-Series Content Gateway................................ 486
Configuring a log source for Forcepoint V-Series Content Gateway............................ 487
Log file protocol for Forcepoint V-Series Content Gateway......................................... 487

Chapter 66. ForeScout CounterACT............................................................................... 489
Configuring a log source ............................................................................................... 489
Configuring the ForeScout CounterACT Plug-in......................................................... 490
Configuring ForeScout CounterACT Policies............................................................... 490

Chapter 67. Fortinet FortiGate Security Gateway............................................................ 493
Configuring a syslog destination on your Fortinet FortiGate Security Gateway device...... 494
Configuring a syslog destination on your Fortinet FortiAnalyzer device.......................... 494

Chapter 68. Foundry FastIron......................................................................................... 497
Configuring syslog for Foundry FastIron..................................................................... 497
Configuring a log source ............................................................................................... 497

Chapter 69. FreeRADIUS................................................................................................. 499
Configuring your FreeRADIUS device to communicate with QRadar.......................... 499
<table>
<thead>
<tr>
<th>Product</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM BigFix</td>
<td>541</td>
</tr>
<tr>
<td>IBM BigFix Detect</td>
<td>543</td>
</tr>
<tr>
<td>Configuring IBM BigFix Detect to communicate with QRadar</td>
<td>545</td>
</tr>
<tr>
<td>IBM Bluemix Platform</td>
<td>546</td>
</tr>
<tr>
<td>Configuring IBM Bluemix Platform to communicate with QRadar</td>
<td>546</td>
</tr>
<tr>
<td>IBM CICS</td>
<td>548</td>
</tr>
<tr>
<td>Create a log source for near real-time event feed</td>
<td>549</td>
</tr>
<tr>
<td>Creating a log source for Log File protocol</td>
<td>550</td>
</tr>
<tr>
<td>IBM DataPower</td>
<td>553</td>
</tr>
<tr>
<td>Configuring IBM DataPower to communicate with QRadar</td>
<td>554</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>555</td>
</tr>
<tr>
<td>Create a log source for near real-time event feed</td>
<td>556</td>
</tr>
<tr>
<td>Creating a log source for Log File protocol</td>
<td>556</td>
</tr>
<tr>
<td>IBM Guardium</td>
<td>558</td>
</tr>
<tr>
<td>Creating a syslog destination for events</td>
<td>560</td>
</tr>
<tr>
<td>Configuring policies to generate syslog events</td>
<td>567</td>
</tr>
<tr>
<td>Installing an IBM Guardium Policy</td>
<td>568</td>
</tr>
<tr>
<td>Configuring a log source</td>
<td>568</td>
</tr>
<tr>
<td>Creating an event map for IBM Guardium events</td>
<td>568</td>
</tr>
<tr>
<td>IBM IMS</td>
<td>569</td>
</tr>
<tr>
<td>Configuring IBM IMS</td>
<td>570</td>
</tr>
<tr>
<td>Configuring a log source</td>
<td>570</td>
</tr>
<tr>
<td>IBM Informix Audit</td>
<td>573</td>
</tr>
<tr>
<td>IBM Lotus Domino</td>
<td>575</td>
</tr>
<tr>
<td>Setting Up SNMP Services</td>
<td>576</td>
</tr>
<tr>
<td>Setting up SNMP in AIX</td>
<td>576</td>
</tr>
<tr>
<td>Starting the Domino Server Add-in Tasks</td>
<td>577</td>
</tr>
<tr>
<td>Configuring SNMP Services</td>
<td>577</td>
</tr>
<tr>
<td>Configuring your IBM Lotus Domino device to communicate with QRadar</td>
<td>578</td>
</tr>
<tr>
<td>IBM Privileged Session Recorder</td>
<td>579</td>
</tr>
<tr>
<td>Configuring IBM Privileged Session Recorder to communicate with QRadar</td>
<td>580</td>
</tr>
<tr>
<td>Configuring a log source for IBM Privileged Session Recorder</td>
<td>580</td>
</tr>
<tr>
<td>IBM Proventia</td>
<td>581</td>
</tr>
<tr>
<td>IBM Proventia Management SiteProtector</td>
<td>581</td>
</tr>
<tr>
<td>IBM ISS Proventia</td>
<td>584</td>
</tr>
<tr>
<td>IBM QRadar Packet Capture</td>
<td>585</td>
</tr>
<tr>
<td>Configuring IBM QRadar Packet Capture to communicate with QRadar</td>
<td>586</td>
</tr>
<tr>
<td>Configuring IBM QRadar Network Packet Capture to communicate with QRadar</td>
<td>587</td>
</tr>
<tr>
<td>IBM RACF</td>
<td>587</td>
</tr>
<tr>
<td>Creating a log source for Log File protocol</td>
<td>588</td>
</tr>
<tr>
<td>Create a log source for near real-time event feed</td>
<td>592</td>
</tr>
<tr>
<td>Integrate IBM RACF with IBM QRadar by using audit scripts</td>
<td>592</td>
</tr>
<tr>
<td>Configuring IBM RACF that uses audit scripts to integrate with IBM QRadar</td>
<td>593</td>
</tr>
<tr>
<td>IBM SAN Volume Controller</td>
<td>595</td>
</tr>
<tr>
<td>Configuring IBM SAN Volume Controller to communicate with QRadar</td>
<td>596</td>
</tr>
<tr>
<td>IBM Security Access Manager for Enterprise Single Sign-On</td>
<td>597</td>
</tr>
<tr>
<td>Configuring a log server type</td>
<td>597</td>
</tr>
<tr>
<td>Configuring syslog forwarding</td>
<td>597</td>
</tr>
<tr>
<td>Configuring a log source in IBM QRadar</td>
<td>598</td>
</tr>
<tr>
<td>IBM Security Access Manager for Mobile</td>
<td>599</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>91</td>
<td>Lieberman Random Password Manager</td>
</tr>
<tr>
<td>92</td>
<td>LightCyber Magna</td>
</tr>
<tr>
<td>93</td>
<td>Linux</td>
</tr>
<tr>
<td>94</td>
<td>LOGbinder</td>
</tr>
<tr>
<td>95</td>
<td>McAfee</td>
</tr>
<tr>
<td>96</td>
<td>MetaInfo MetaIP</td>
</tr>
</tbody>
</table>

**Chapter 93. Linux**

- Linux DHCP
  - Configuring a log source
- Linux IPtables
  - Configuring IPtables
  - Configuring a log source
- Linux OS
  - Configuring syslog on Linux OS
  - Configuring syslog-ng on Linux OS
  - Configuring Linux OS to send audit logs

**Chapter 94. LOGbinder**

- LOGbinder EX event collection from Microsoft Exchange Server
  - Configuring your LOGbinder EX system to send Microsoft Exchange event logs to QRadar
- LOGbinder SP event collection from Microsoft SharePoint
  - Configuring your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar
- LOGbinder SQL event collection from Microsoft SQL Server
  - Configuring your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar

**Chapter 95. McAfee**

- McAfee Application / Change Control
- McAfee ePolicy Orchestrator
  - Adding a registered server to McAfee ePolicy Orchestrator
  - Configuring SNMP notifications on McAfee ePolicy Orchestrator
  - Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator
  - Installing the Java Cryptography Extension on QRadar
- Sample event message
- McAfee Network Security Platform (Formerly known as McAfee Intrushield)
  - Configuring alert events for McAfee Intrushield V2.x - V5.x
  - Configuring alert events for McAfee Network Security Platform V6.x and V7.x
  - Configuring fault notification events for McAfee Network Security Platform V6.x and V7.x
- McAfee Web Gateway
  - McAfee Web Gateway DSM integration process
  - Configuring McAfee Web Gateway to communicate with QRadar (syslog)
  - Importing the Syslog Log Handler
  - Configuring McAfee Web Gateway to communicate with IBM QRadar (log file protocol)
  - Pulling data by using the log file protocol
  - Creation of an event map for McAfee Web Gateway events
  - Discovering unknown events
  - Modifying the event map

**Chapter 96. MetaInfo MetaIP**
Chapter 100. NCC Group DDoS Secure................................................................. 829
   Configuring NCC Group DDoS Secure to communicate with QRadar.............. 830

Chapter 101. NetApp Data ONTAP........................................................................ 831

Chapter 102. Netskope Active............................................................................ 833
   Configuring QRadar to collect events from your Netskope Active system......... 834

Chapter 103. NGINX HTTP Server.................................................................... 835
   NGINX HTTP Server DSM specifications....................................................... 835
   Configuring NGINX HTTP Server to communicate with QRadar............... 836
   Sample event messages.............................................................................. 836

Chapter 104. Niksun......................................................................................... 839
   Configuring a log source............................................................................. 839

Chapter 105. Nokia Firewall............................................................................. 841
   Integration with a Nokia Firewall by using syslog.................................... 841
   Configuring IPtables.................................................................................. 841
   Configuring syslog..................................................................................... 842
   Configuring the logged events custom script........................................ 842
   Configuring a log source........................................................................... 842
   Integration with a Nokia Firewall by using OPSEC................................ 843
   Configuring a Nokia Firewall for OPSEC.............................................. 843
   Configuring an OPSEC log source.......................................................... 844

Chapter 106. Nominum Vantio......................................................................... 847

Chapter 107. Nortel Networks......................................................................... 849
   Nortel Multiprotocol Router....................................................................... 849
   Nortel Application Switch.......................................................................... 851
   Nortel Contivity......................................................................................... 852
   Nortel Ethernet Routing Switch 2500/4500/5500.................................... 853
   Nortel Ethernet Routing Switch 8300/8600.............................................. 854
   Nortel Secure Router.................................................................................. 855
   Nortel Secure Network Access Switch...................................................... 856
   Nortel Switched Firewall 5100..................................................................... 857
      Integrating Nortel Switched Firewall by using syslog......................... 857
      Integrate Nortel Switched Firewall by using OPSEC.......................... 858
      Configuring a log source...................................................................... 858
   Nortel Switched Firewall 6000..................................................................... 858
      Configuring syslog for Nortel Switched Firewalls............................. 858
      Configuring OPSEC for Nortel Switched Firewalls........................... 859
      Reconfiguring the Check Point SmartCenter Server.......................... 860
   Nortel Threat Protection System (TPS)...................................................... 860
   Nortel VPN Gateway................................................................................. 861

Chapter 108. Novell eDirectory....................................................................... 863
   Configure XDASv2 to forward events...................................................... 863
   Load the XDASv2 Module......................................................................... 864
   Loading the XDASv2 on a Linux Operating System............................... 864
   Loading the XDASv2 on a Windows Operating System.......................... 865
   Configure event auditing using Novell iManager.................................... 865
   Configure a log source............................................................................. 866

Chapter 109. Observe IT JDBC.......................................................................... 867
Chapter 119. Pirean Access: One................................................................. 935
Configuring a log source in QRadar to collect events from Pirean Access: One........ 935

Chapter 120. PostFix Mail Transfer Agent.................................................. 939
Configuring syslog for PostFix Mail Transfer Agent................................. 939
Configuring a PostFix MTA log source ..................................................... 939
Configuring IPtables for multiline UDP syslog events.................................. 941

Chapter 121. ProFTPD............................................................................... 943
Configuring ProFTPD................................................................................ 943
Configuring a log source ........................................................................... 943

Chapter 122. Proofpoint Enterprise Protection and Enterprise Privacy.............. 945
Configuring Proofpoint Enterprise Protection and Enterprise Privacy DSM to communicate with IBM QRadar......................................................... 946
Configuring a Proofpoint Enterprise Protection and Enterprise Privacy log source ................................................................. 946

Chapter 123. Pulse Secure Pulse Connect Secure........................................ 951
Configuring a Pulse Secure Pulse Connect Secure device to send WebTrends Enhanced Log File (WELF) events to IBM QRadar................................. 952
Configuring a Pulse Secure Pulse Connect Secure device to send syslog events to QRadar................................................................. 953
Sample event message.............................................................................. 954

Chapter 124. Radware.............................................................................. 955
Radware AppWall..................................................................................... 955
Configuring Radware AppWall to communicate with QRadar...................... 956
Increasing the maximum TCP Syslog payload length for Radware AppWall....... 956
Radware DefensePro............................................................................... 957
Configuring a log source ........................................................................... 957

Chapter 125. Raz-Lee iSecurity................................................................. 959
Configuring Raz-Lee iSecurity to communicate with QRadar...................... 959
Configuring a log source for Raz-Lee iSecurity........................................... 961

Chapter 126. Redback ASE..................................................................... 963
Configuring Redback ASE..................................................................... 963
Configuring a log source ........................................................................... 963

Chapter 127. Resolution1 CyberSecurity................................................... 965
Configuring your Resolution1 CyberSecurity device to communicate with QRadar................................................................. 966
Resolution1 CyberSecurity log source on your QRadar Console................. 966

Chapter 128. Riverbed............................................................................ 967
Riverbed SteelCentral NetProfiler (Cascade Profiler) Audit.......................... 967
Creating a Riverbed SteelCentral NetProfiler report template and generating an audit file................................................................. 968
Riverbed SteelCentral NetProfiler (Cascade Profiler) Alert.......................... 969
Configuring your Riverbed SteelCentral NetProfiler system to enable communication with QRadar................................................................. 971

Chapter 129. RSA Authentication Manager............................................. 973
Configuration of syslog for RSA Authentication Manager 6.x, 7.x and 8.x........ 973
Chapter 163. WatchGuard Fireware OS................................................................................................................. 1169
  Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication
  with QRadar................................................................................................................................ 1170
  Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with
  QRadar................................................................................................................................................... 1170
  Configuring a WatchGuard Fireware OS log source in QRadar.........................................................1171

Chapter 164. Websense............................................................................................................................................. 1173

Chapter 165. Zscaler Nanolog Streaming Service................................................................................................ 1175
  Configuring a syslog feed in Zscaler NSS........................................................................................ 1175
  Configuring a Zscaler NSS log source .............................................................................................. 1176

Chapter 166. QRadar supported DSMs................................................................................................................ 1179

Notices................................................................................................................................................................. 1193
  Trademarks.................................................................................................................................................. 1194
  Terms and conditions for product documentation.................................................................................. 1194
  IBM Online Privacy Statement.................................................................................................................... 1195
  Privacy policy considerations...................................................................................................................... 1195

Glossary............................................................................................................................................................... 1197
  A.......................................................................................................................................................... 1197
  B.......................................................................................................................................................... 1197
  C.......................................................................................................................................................... 1198
  D.......................................................................................................................................................... 1198
  E.......................................................................................................................................................... 1199
  F.......................................................................................................................................................... 1199
  G.......................................................................................................................................................... 1199
  H.......................................................................................................................................................... 1200
  I.......................................................................................................................................................... 1200
  K.......................................................................................................................................................... 1201
  L.......................................................................................................................................................... 1201
  M.......................................................................................................................................................... 1201
  N.......................................................................................................................................................... 1202
  O.......................................................................................................................................................... 1202
  P.......................................................................................................................................................... 1202
  Q.......................................................................................................................................................... 1203
  R.......................................................................................................................................................... 1203
  S.......................................................................................................................................................... 1204
  T.......................................................................................................................................................... 1204
  V.......................................................................................................................................................... 1205
  W.......................................................................................................................................................... 1205

Index................................................................................................................................................................. 1207
The DSM Configuration guide provides instructions about how to collect data from your third-party devices, also known as log sources.

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

**Note:** This guide describes the Device Support Modules (DSMs) that are produced by IBM. Third-party DSMs are available on the IBM App Exchange, but are not documented here.

**Intended audience**

System administrators must have QRadar access, knowledge of the corporate 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/knowledgcenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see QRadar Support – Assistance 101 (https://ibm.biz/qradarsupport).

**Contacting customer support**

For information about contacting customer support, see QRadar Support – Assistance 101 (https://ibm.biz/qradarsupport).

**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 lawful 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.

**Please Note:**

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.
Part 1. QRadar DSM installation and log source management
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 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.

**DSMs**

A Device Support Module (DSM) is a code module that parses received events from multiple log sources and converts 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 automatic updates, see the IBM QRadar 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
Adding a 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.

Before you begin

Note: The `rpm -Uvh <rpm_filename>` command line to install was replaced with the `yum -y install <rpm_filename>` command.

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:
   ```
   yum -y install <rpm_filename>
   ```
6. Log in to the QRadar user interface.
7. On the Admin tab, click Deploy Changes.

Related concepts

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

Akamai Kona
The IBM QRadar DSM for Akamai Kona collects event logs from your Akamai Kona platforms.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td>When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.</td>
</tr>
<tr>
<td>Credibility</td>
<td>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.</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>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.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

Akamai Kona
The IBM QRadar DSM for Akamai Kona collects event logs from your Akamai Kona platforms.

Adding bulk log sources

You can add up to 500 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. On the Admin tab, click Log Sources.
2. From the Bulk Actions list, select Bulk Add.
3. In the Bulk Log Sources window, configure the parameters for the bulk log source.
4. Select the Enabled check box to enable the log source. By default, this check box is selected.
5. Select the Coalescing Events check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value that is configured in the Coalescing Events list in the System Settings window on the Admin tab. However, when you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar Administration Guide.
6. Select the Store Event Payload check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the Store Event Payload list in the System Settings window on the Admin tab. When you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar Administration Guide.
7. Upload the log sources by choosing one of the following methods:
   - File Upload - Upload a text file that has one host name or IP per line. The text file must contain one IP address or host name per line. Extra characters after an IP address or host names longer than 255 characters can result in a value being bypassed from the text file. The file upload lists a summary of all IP address or host names that were added as the bulk log source.
   - Manual - Enter the host name or IP of the host that you want to add.
8. Click Add > Save.
   - Note: By default, a check box is selected for each log source in the host list. Clear the check box if you want the log source to be ignored. Duplicate host names or IP addresses are ignored.
9. Click Continue to add the log sources.
10. 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. Threat use cases by log source type

External log sources feed raw events to the QRadar system that provide different perspectives about your network, such as audit, monitoring, and security. It's critical that you collect all types of log sources so that QRadar can provide the information that you need to protect your organization and environment from external and internal threats. For example, if your organization adopts cloud services and begins to onboard Amazon Web Services (AWS), or Azure cloud services, or Microsoft Office 365, add the log sources to QRadar so that you continue to have visibility into all malicious activity and compliance breaches.

Click a check mark in the following matrix to go to the log source that you're most interested in. For each log source, the relevant ATT&CK framework categories are listed. The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework was developed by Mitre Corp. The public knowledge base of threat tactics and techniques helps your security analysts to understand hacker threats and how to prevent adversarial attacks from happening to your organization’s networks. These tactics can become your weaknesses if you’re not collecting that type of log source.

<table>
<thead>
<tr>
<th>Log sources</th>
<th>Advanced Persistent Threat</th>
<th>Insider Threat</th>
<th>Securing the Cloud</th>
<th>Critical Data Protection</th>
<th>Incident Response</th>
<th>Compliance</th>
<th>Risk and Vulnerability Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall/Router</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IDS/IPS (Intrusion Detection System/Intrusion Protection System)</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web Proxy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>VPN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mail Logs</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DLP (Data Loss Prevention)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity/Authentication (LDAP/AD/Radius)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti Virus</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QRadar Network Insights/Netflow</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Logs</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDR</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2. Log sources in QRadar with use cases (continued)

<table>
<thead>
<tr>
<th>Log sources</th>
<th>Advanced Persistent Threat</th>
<th>Insider Threat</th>
<th>Securing the Cloud</th>
<th>Critical Data Protection</th>
<th>Incident Response</th>
<th>Compliance</th>
<th>Risk and Vulnerability Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Infrastructure/ Audit</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(AWS CloudTrail, Azure Event Hubs)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office 365</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Firewall/Router**

The following table provides examples of use cases that are affected by firewall/router log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Defense Evasion
- Discovery
- Command and Control
- Exfiltration

Table 3. Firewall/Router log source and use case examples

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Firewall data helps detect command control issues. Use it for external recon and prevent malicious IP communications from entering your environment.</td>
</tr>
<tr>
<td>Securing the Cloud</td>
<td>Identify risky internet service provider connections, such as connections to TOR.</td>
</tr>
<tr>
<td>Critical Data Protection</td>
<td>Discover and protect against abnormal database connection attempts.</td>
</tr>
<tr>
<td>Incident Response</td>
<td>See which hosts communicated with an infected host so that you can stop the spread of data infection.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Monitor for unauthorized or unexpected firewall configuration changes to allow access to critical business assets. For example, PCI requires all critical assets that contain “banking information” to communicate through an internal DMZ with no direct access to the outside world.</td>
</tr>
<tr>
<td>Risk and Vulnerability Management</td>
<td>Discover assets that are actively communicating on vulnerable ports.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: [ATT&CK Technique matrix](https://attack.mitre.org/wiki/Technique_Matrix)
Intrusion detection system (IDS)/Intrusion protection system (IPS)

The following table provides examples of use cases that are affected by IDS/IPS log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Defense Evasion
- Persistence Mechanism
- Discovery
- Command and Control

<table>
<thead>
<tr>
<th>Table 4. IDS/IPS log source and use case examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use case</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>Critical Data Protection</td>
</tr>
<tr>
<td>Incident Response</td>
</tr>
<tr>
<td>Risk and Vulnerability Management</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

Web proxy

The following table provides examples of use cases that are affected by web proxy log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Defense Evasion
- Persistence Mechanism
- Data Exfiltration
- Command and Control
- Privilege Escalation
- Credential Access

<table>
<thead>
<tr>
<th>Table 5. Web proxy log source and use case examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use case</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>Insider Threat</td>
</tr>
<tr>
<td>Securing the Cloud</td>
</tr>
</tbody>
</table>
Table 5. Web proxy log source and use case examples (continued)

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Data Protection</td>
<td>Monitor for unauthorized data exfiltration.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Monitor for critical asset communication with the outside world.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

VPN

The following table provides examples of use cases that are affected by VPN log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Credential Access
- Lateral Movement

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Monitor for logins from suspicious locations.</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Detect the use of VPN for users outside of normal usage patterns or from abnormal geographical areas.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

DNS

The following table provides examples of use cases that are affected by DNS log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Defense Evasion
- Persistence Mechanism
- Command and Control
- Exfiltration
- Credential Access (note: Technique T1171)

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Monitor for malicious DNS usages such as domain name generation, tunneling, and squatting.</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Detect tunneling of traffic through DNS records.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)
DHCP
The following table provides examples of use cases that are affected by DHCP log sources. Data from this type of log source is important for detecting adversarial the techniques in the Defense Evasion ATT&CK category.

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Detection of rogue access points or other unexpected device presence on corporate network.</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Detection of rogue access points or other unexpected device presence on corporate network.</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Identification of which host had a specific IP address at the time of an incident.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

Mail logs
The following table provides examples of use cases that are affected by mail log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Execution
- Initial Access
- Collection

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Monitor for phishing and spam.</td>
</tr>
<tr>
<td>Insider threat</td>
<td>Phishing</td>
</tr>
<tr>
<td>Critical Data Protection</td>
<td>Phishing, data exfiltration by email</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

DLP (data loss prevention)
The following table provides examples of use cases that are affected by DLP log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Data Exfiltration
- Collection
<table>
<thead>
<tr>
<th><strong>Use case</strong></th>
<th><strong>Examples</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Data can be exfiltrated through many methods. Identify and track suspicious files such as:</td>
</tr>
<tr>
<td></td>
<td>• DNS abnormalities</td>
</tr>
<tr>
<td></td>
<td>• Sensitive content</td>
</tr>
<tr>
<td></td>
<td>• Aberrant connections</td>
</tr>
<tr>
<td></td>
<td>• Aliases</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Data can be exfiltrated through many methods. Identify and track suspicious files such as:</td>
</tr>
<tr>
<td></td>
<td>• DNS abnormalities</td>
</tr>
<tr>
<td></td>
<td>• Sensitive content</td>
</tr>
<tr>
<td></td>
<td>• Aberrant connections</td>
</tr>
<tr>
<td></td>
<td>• Aliases</td>
</tr>
<tr>
<td>Critical Data Protection</td>
<td>Data can be exfiltrated through many methods. Identify and track suspicious files such as:</td>
</tr>
<tr>
<td></td>
<td>• DNS abnormalities</td>
</tr>
<tr>
<td></td>
<td>• Sensitive content</td>
</tr>
<tr>
<td></td>
<td>• Aberrant connections</td>
</tr>
<tr>
<td></td>
<td>• Aliases</td>
</tr>
<tr>
<td>Compliance</td>
<td>Data can be exfiltrated through many methods. Identify and track suspicious files such as:</td>
</tr>
<tr>
<td></td>
<td>• DNS abnormalities</td>
</tr>
<tr>
<td></td>
<td>• Sensitive content</td>
</tr>
<tr>
<td></td>
<td>• Aberrant connections</td>
</tr>
<tr>
<td></td>
<td>• Aliases</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: [ATT&CK Technique matrix](https://attack.mitre.org/wiki/Technique_Matrix)

**Endpoint**

The following table provides examples of use cases that are affected by Endpoint log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Privilege Escalation
- Initial Access
- Execution
- Persistence
- Credential Access
- Defense Evasion
- Discovery
• Lateral Movement
• Collection
• Exfiltration
• Command and Control

**Table 11. Endpoint log source and use case examples**

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Monitor for malicious hashes, suspicious PowerShell activity, process abuse, or other suspicious endpoint activities.</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Detection of persistent malware by using host resources (for example, crypto mining)</td>
</tr>
<tr>
<td>Critical Data Protection</td>
<td>Data can be exfiltrated through many methods. Identify and track suspicious files such as:</td>
</tr>
<tr>
<td></td>
<td>• DNS abnormalities</td>
</tr>
<tr>
<td></td>
<td>• Sensitive content</td>
</tr>
<tr>
<td></td>
<td>• Aberrant connections</td>
</tr>
<tr>
<td></td>
<td>• Aliases</td>
</tr>
<tr>
<td>Compliance</td>
<td>Monitor for adherence to corporate company policy (for example, unapproved software use).</td>
</tr>
<tr>
<td>Risk and Vulnerability Management</td>
<td>Assess and manage risk through vulnerability.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

Identity/Authentication (LDAP/AD/Radius)

The following table provides examples of use cases that are affected by LDAP/AD/Radius log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

• Privilege Escalation
• Credential Access
• Initial Access

**Note:** You can also track privilege abuse (for example, surf with a super account, privileges that are given to users).

**Table 12. LDAP/AD/Radius log source and use case examples**

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Monitor for activities such as brute force login by malware, lateral movement through the network, or suspicious logins.</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Account takeover by malware</td>
</tr>
<tr>
<td>Securing the Cloud</td>
<td>Provide user-to-IP association to help identify cloud users from data that has only IP source address.</td>
</tr>
</tbody>
</table>
Table 12. LDAP/AD/Radius log source and use case examples (continued)

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Response</td>
<td>Visibility into where a user logged in during the IR process.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

Anti-virus

The following table provides examples of use cases that are affected by anti-virus log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Persistence
- Initial Access
- Defense Evasion

Table 13. Anti-virus log source and use case examples

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Monitor for activities such as:</td>
</tr>
<tr>
<td></td>
<td>• Endpoint infection by anti-virus</td>
</tr>
<tr>
<td></td>
<td>• Virus that is not cleaned</td>
</tr>
<tr>
<td></td>
<td>• Reinforcement of other suspicious endpoint behavior</td>
</tr>
<tr>
<td>Critical Data Protection</td>
<td>Detection of virus outbreak to prevent movement to servers that contain critical business data.</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Visibility into where a specific virus signature was seen.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Ensuring up-to-date AV definitions on critical hosts/servers.</td>
</tr>
<tr>
<td>Risk and Vulnerability Management</td>
<td>Malicious WWW domain connections indication of a vulnerable host that is compromised.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

QRadar Network Insights/Netflow

The following table provides examples of use cases that are affected by QRadar Network Insights/Netflow log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Lateral Movement
- Discovery
- Persistence Mechanism
- Defense Evasion
- Data Exfiltration
- Credential Access
- Command and Control

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Monitor for activities such as:</td>
</tr>
<tr>
<td></td>
<td>• Recon</td>
</tr>
<tr>
<td></td>
<td>• Malicious download</td>
</tr>
<tr>
<td></td>
<td>• Lateral movement</td>
</tr>
<tr>
<td></td>
<td>• Phishing</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Phishing detection</td>
</tr>
<tr>
<td>Securing the Cloud</td>
<td>Monitor for activities such as:</td>
</tr>
<tr>
<td></td>
<td>• Data exfiltration</td>
</tr>
<tr>
<td></td>
<td>• Expired WWW certificates</td>
</tr>
<tr>
<td></td>
<td>• Self-signed WWW certificates</td>
</tr>
<tr>
<td></td>
<td>• Phishing</td>
</tr>
<tr>
<td></td>
<td>• Risky WWW domain connections</td>
</tr>
<tr>
<td>Critical Data Protection</td>
<td>Data can be exfiltrated through many methods. Identify and track suspicious files such as:</td>
</tr>
<tr>
<td></td>
<td>• DNS abnormalities</td>
</tr>
<tr>
<td></td>
<td>• Sensitive content</td>
</tr>
<tr>
<td></td>
<td>• Aberrant connections</td>
</tr>
<tr>
<td></td>
<td>• Aliases</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Provides a huge pool of investigative data to determine the spread of an attack from domain communication, hashes that are downloaded, IP addresses that are communicated with, file names, data volumes transferred.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Monitor for critical asset communications (for example, crown jewel communicate to the open internet).</td>
</tr>
<tr>
<td>Risk and vulnerability management</td>
<td>Prioritize host vulnerability remediation based upon the level of risk that hosts are communicated with.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

Database logs

The following table provides examples of use cases that are affected by database log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:
- Credential Access
- Collection
Table 15. Database log source and use case examples

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider Threat</td>
<td>Detect unauthorized database access and data theft.</td>
</tr>
<tr>
<td>Critical Data Protection</td>
<td>Databases often include sensitive corporate information and require monitoring for most compliance standards. Monitor for unauthorized user permission changes.</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Evidence of what data was accessed, and by whom, during a breach.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Databases often include sensitive corporate information and require monitoring for most compliance standards.</td>
</tr>
<tr>
<td>Risk and Vulnerability Management</td>
<td>Prioritize vulnerabilities on hosts with active databases that potentially contain critical data. Detect default accounts and passwords that are enabled.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

EDR (endpoint detection and response)

The following table provides examples of use cases that are affected by EDR log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Credential Access
- Privilege Escalation
- Discovery

Table 16. EDR log source and use case examples

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Monitor for activities such as:</td>
</tr>
<tr>
<td></td>
<td>• Compromised endpoints</td>
</tr>
<tr>
<td></td>
<td>• Suspicious endpoint behavior</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Rapidly determine existence of IOCs at endpoints, including hashes and file names.</td>
</tr>
<tr>
<td>Risk and Vulnerability Management</td>
<td>Correlate vulnerability information with endpoint data.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)
Cloud Infrastructure/Audit (AWS Cloudtrail, Azure Event Hubs)

The following table provides examples of use cases that are affected by Cloud Infrastructure/Audit log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Credential Access
- Privilege Escalation

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threat</td>
<td>Multi-vector attacks that impact multiple cloud environments, crypto jacking (Hijacking cloud properties/computing resources for crypto currency mining).</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Detection of compromised cloud accounts, escalated role/user privilege, altering network security group access policies.</td>
</tr>
<tr>
<td>Securing the Cloud</td>
<td>Monitor for activities such as:</td>
</tr>
<tr>
<td></td>
<td>- Misconfiguration of S3 buckets and user policies</td>
</tr>
<tr>
<td></td>
<td>- Visibility into cloud environments</td>
</tr>
<tr>
<td></td>
<td>- Enforcing best cloud security practices</td>
</tr>
<tr>
<td></td>
<td>- Continuous monitoring of network interface traffic</td>
</tr>
<tr>
<td>Critical Data Protection</td>
<td>Lock down and isolation of sensitive data repositories.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Retention of cloud audit trail logs and ensuring log integrity</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

Microsoft Office 365

The following table provides examples of use cases that are affected by Microsoft Office 365 log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Initial Access
- Execution
- Persistence

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securing the Cloud</td>
<td>Monitor for activities such as:</td>
</tr>
<tr>
<td></td>
<td>- Brute force logins</td>
</tr>
<tr>
<td></td>
<td>- Suspicious logins from multiple locations</td>
</tr>
<tr>
<td></td>
<td>- Blacklisted countries and locations</td>
</tr>
<tr>
<td></td>
<td>- Excessive file access attempts</td>
</tr>
</tbody>
</table>
Table 18. Office 365 log source and use case examples (continued)

<table>
<thead>
<tr>
<th>Use case</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Response</td>
<td>Evidence of what data was accessed during a breach.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Continuous monitoring of file activity and user access.</td>
</tr>
</tbody>
</table>

Find out more about each technique and tactic: [ATT&CK Technique matrix](https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

**Related information**

Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)

See how QRadar Advisor with Watson 2.0.1 analyzes several MITRE ATT&CK techniques

A Basic Model to Measure SIEM Maturity
Chapter 3. Troubleshooting DSMs

If you come across a problem with your DSM, you can troubleshoot the following issues.

What happens when events, which are parsed, are collected with unofficial DSMs?

Not having an official DSM doesn't mean that the events aren't collected. It indicates that the event that is received by IBM QRadar might be identified as "Unknown" on the Log Activity tab of QRadar. "Unknown" means that IBM QRadar collected the event, but was unable to parse the event format to categorize the event. However, some unique events in unofficial DSMs cannot be parsed or identified if they don't follow an event format that is expected. When an event cannot be understood by the system, they are categorized as "Unknown".

What is the difference between an unknown event and a stored event?

Events comprise three different categories:

Parsed events
QRadar collects, parses, and categorizes the event to the proper log source.

Unknown events
The event is collected and parsed, but cannot be mapped or categorized to a specific log source. The Event Name and the Low-Level Category are set as Unknown. Log sources that aren't automatically discovered are typically identified as Unknown Event Log until a log source is manually created in the system. When an event cannot be associated to a log source, the event is assigned to a generic log source. You can identify these events by searching for events that are associated with the SIM Generic log source or by using the Event is Unparsed filter.

Stored events
The event cannot be understood or parsed by QRadar. When QRadar cannot parse an event, it writes the event to disk and categorize the event as Stored.

How can you find these events in the Log Activity tab?

To find events specific to your device, you can search in QRadar for the source IP address of your device. You can also select a unique value from the event payload and search for Payload Contains. One of these searches might locate your event, and it is likely either categorized as Unknown or Stored.

The easiest way to locate unknown or stored events is to add a search filter for Event in Unparsed. This search filter locates all events that either cannot be parsed (stored) or events that might not be associated with a log source or auto discovered (Unknown Log Event).

For more information about officially supported DSMs, see the r_supported_dsm_list.dita section.

What do you do if the product version or device you have is not listed in the DSM Configuration Guide?

Sometimes a version of a vendor product or a device is not listed as supported. If the product or device is not listed, follow these guidelines:

Version not listed
If the DSM is for a product that is officially supported by QRadar, but the version listed in the IBM QRadar DSM Configuration Guide appears to be out-of-date, try the DSM to see whether it works. The product versions that are listed in the guide are those specifically tested by IBM, but newer untested versions may also work. In most cases no changes are necessary, or at most a minor update to the IBM QRadar Identifier (QID) Map may be all that is required. Software updates by vendors might on rare occasions add or change event formats that break the DSM, requiring an RFE for the development of a new integration. This would be the only scenario where an RFE is required. In either event, open a
support ticket for a review of the log source to troubleshoot and rule out any potential issues not related to the software version.

**Device not listed**
When a device is not officially supported, you have the following options:

- Open a request for enhancement (RFE) to have your device become officially supported.
  1. Go to the QRadar SIEM RFE page (https://ibm.biz/BdRPx5).
  2. Log in to the support portal page.
  3. Click the **Submit** tab and type the necessary information.

  **Note:** If you have event logs from a device, attach the event information and include the product version of the device that generated the event log.

- Write a log source extension to parse events for your device. For more information, see Chapter 11, “Log source extensions,” on page 107 and the DSM Editor.
Part 2. Log sources
Chapter 4. Introduction to log source management

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

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

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

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

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

1. Download and install a device support module (DSM) that supports the log source. A DSM is software application that contains the event patterns that are required to identify and parse events from the original format of the event log to the format that QRadar can use.
2. If automatic discovery is supported for the DSM, wait for QRadar to automatically add the log source to your list of configured log sources.
3. If automatic discovery is not supported for the DSM, manually create the log source configuration.

Related tasks

“Adding a log source” on page 4
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 bulk log sources” on page 6
You can add up to 500 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.

“Adding a log source parsing order” on page 6
You can assign a priority order for when the events are parsed by the target event collector.

“Adding a DSM” on page 4
Chapter 5. 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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td>When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.</td>
</tr>
<tr>
<td>Credibility</td>
<td>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.</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>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.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>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.</td>
</tr>
</tbody>
</table>
**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**
- **3Com Switch 8800**
  The IBM QRadar DSM for 3Com Switch 8800 receives events by using syslog.
- **Akamai Kona**
  The IBM QRadar DSM for Akamai Kona collects event logs from your Akamai Kona platforms.
Chapter 6. Undocumented Protocols

When configuring a log source, the set of available protocol type options is limited based on the selected log source type. Not all log source types support all protocol types. The DSM Configuration Guide describes how to configure log sources of a particular type, with each of the protocol types that IBM fully supports for that log source type. Any protocol type that has configuration documentation for a particular log source type is considered a "documented" protocol for that log source type. By default, only these documented protocols are displayed in the Protocol Configuration list in the Log Sources window.

As an open platform, QRadar collects and processes event data through other integration methods (protocol types). Some protocol types can be configured for a particular log source type but are marked as "undocumented". However, the DSM Configuration Guide doesn't contain instructions on how to set up event collection for undocumented protocols. IBM does not offer support with the configuration of log sources that use undocumented protocols because they are not internally tested and documented. Users are responsible for determining how to get the event data into QRadar.

For example, the JDBC protocol is the documented configuration for obtaining events from a system that stores its event data in a database. However, it is possible to collect the same event data through a third-party product and then forward it to QRadar through Syslog. Configure the log source to use the undocumented protocol type "Syslog". QRadar accepts the events and routes them to the appropriate log source.

**Note:** You must configure the third-party product to retrieve the event data from the database and to send this data to QRadar through Syslog because this is not the documented collection method.

**Note:** Collecting and processing event data through undocumented protocols might result in data that is formatted differently from what a documented DSM log source type expects. As a result, parsing might not work for the DSM if it's receiving events from an undocumented protocol. For example, a JDBC protocol creates event payloads that consist of a series of space-separated key and value pairs. In the target database table, the key is a column name and the value is the column for the table row that the event represents. The DSM for a supported log source type that uses the JDBC protocol expects this event format. If the event data forwarded from a third-party product through the syslog protocol is in a different format, the DSM is unable to parse it. It might be necessary to use the DSM Editor to adjust the parsing of a DSM so that it can handle these events.

**Related tasks**

"Configuring an undocumented protocol" on page 29

As an open platform, QRadar collects and processes event data through multiple integration methods (protocol types). Some protocol types can be configured for a particular log source type but are marked as "undocumented". The DSM Configuration Guide doesn't contain instructions on how to set up event collection for undocumented protocols. IBM does not offer support with the configuration of log sources that use undocumented protocols because they are not internally tested and documented.

### Configuring an undocumented protocol

As an open platform, QRadar collects and processes event data through multiple integration methods (protocol types). Some protocol types can be configured for a particular log source type but are marked as "undocumented". The DSM Configuration Guide doesn't contain instructions on how to set up event collection for undocumented protocols. IBM does not offer support with the configuration of log sources that use undocumented protocols because they are not internally tested and documented.

**Procedure**

1. Use SSH to log in to your QRadar Console appliance as a root user.
2. Edit the following file: `/store/configservices/staging/globalconfig/nva.conf`
3. Set the EXPOSE_UNDOCUMENTED_PROTOCOLS property value to true.
4. Save the file.
5. To close the SSH session type `exit`.
6. Log in to the QRadar Console.
7. Click the Admin tab.
8. Click Deploy Changes.
   Undocumented protocol options appear in the Protocol Configuration list in the log source Add/Edit window.

Related concepts

“Undocumented Protocols” on page 29
When configuring a log source, the set of available protocol type options is limited based on the selected log source type. Not all log source types support all protocol types. The DSM Configuration Guide describes how to configure log sources of a particular type, with each of the protocol types that IBM fully supports for that log source type. Any protocol type that has configuration documentation for a particular log source type is considered a "documented" protocol for that log source type. By default, only these documented protocols are displayed in the Protocol Configuration list in the Log Sources window.
Protocols in IBM QRadar provide the capability of collecting a set of data files by using various connection options. These connections pull the data back or passively receive data into the event pipeline in QRadar. Then, the corresponding Device Support Module (DSM) parses and normalizes the data.

The following standard connection options pull data into the event pipeline:
- JDBC
- FTP
- SFTP
- SCP

The following standard connection options receive data into the event pipeline:
- Syslog
- HTTP Receiver
- SNMP

QRadar also supports proprietary vendor-specific protocol API calls, such as Amazon Web Services.

**Related tasks**

“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

## Akamai Kona REST API protocol configuration options

To receive events from your Akamai Kona Platform, configure a log source to use the Akamai Kona REST API protocol.

The Akamai Kona REST API protocol is an outbound/active protocol that queries the Akamai Kona Platform and sends events to the QRadar Console.

The following table describes the parameters that require specific values for Akamai KONA DSM event collection.

<table>
<thead>
<tr>
<th>Table 20. Akamai KONA DSM log source parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
<tr>
<td>Host</td>
</tr>
<tr>
<td>Client Token</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>Client Secret</td>
</tr>
<tr>
<td>Access Token</td>
</tr>
<tr>
<td>Security Configuration ID</td>
</tr>
<tr>
<td>Use Proxy</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate</td>
</tr>
<tr>
<td>Recurrence</td>
</tr>
<tr>
<td>EPS Throttle</td>
</tr>
</tbody>
</table>

**Amazon AWS S3 REST API protocol configuration options**

The Amazon AWS S3 REST API protocol for IBM Security QRadar is an outbound/active protocol that collects AWS CloudTrail logs from Amazon S3 buckets.

**Note:** It’s important to ensure that no data is missing when you collect logs from Amazon S3 to use with a custom DSM or other unsupported integrations. Because of the way the S3 APIs return the data, all files must be in an alphabetically increasing order when the full path is listed. Make sure that the full path name includes a full date and time in ISO9660 format (leading zeros in all fields and a YYYY-MM-DD date format).

Consider the following file path:
The full name of the file in the marker is MyLogs/2018-8-9/2018-08-09T23-59-25.955097.log.gz and the folder name is written as 2018-8-9 instead of 2018-08-09. This date format causes an issue when data for the 10 September 2018 is presented. When sorted, the date displays as 2018-8-10 and the files are not sorted chronologically:

2018-10-1
2018-11-1
2018-12-31
2018-8-10
2018-8-9
2018-9-1

After data for 9 August 2018 comes in to QRadar, you won't see data again until 1 September 2018 because leading zeros were not used in the date format. After September, you won't see data again until 2019. Leading zeros are used in the date (ISO 9660) so this issue does not occur.

By using leading zeros, files and folders are sorted chronologically:

2018-08-09
2018-08-10
2018-09-01
2018-10-01
2018-11-01
2018-12-01
2018-12-31

**Restriction:**

A log source can retrieve data from only one region, so use a different log source for each region. Include the region folder name in the file path for the Directory Prefix value when using the Directory Prefix event collection method to configure the log source.

The following table describes the common parameter values to collect audit events by using the Directory Prefix collection method or the SQS event collection method. These collection methods use the Amazon AWS S3 REST API protocol.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Amazon AWS S3 REST API</td>
</tr>
</tbody>
</table>
Table 21. Amazon AWS S3 REST API protocol common log source parameters when using the Directory Prefix method or the SQS method (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td></td>
<td>The Log Source Identifier can be any valid value and does not need to reference a specific server.</td>
</tr>
<tr>
<td></td>
<td>The Log Source Identifier can be the same value as the Log Source Name. If you have more than one Amazon AWS CloudTrail log source that is configured, you might want to identify the first log source as awscloudtrail1, the second log source as awscloudtrail2, and the third log source as awscloudtrail3.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Access Key ID / Secret Key</td>
</tr>
<tr>
<td></td>
<td>Standard authentication that can be used from anywhere.</td>
</tr>
<tr>
<td></td>
<td>For more information about configuring security credentials, see Configuring security credentials for your AWS user account.</td>
</tr>
<tr>
<td></td>
<td>Assume IAM Role</td>
</tr>
<tr>
<td></td>
<td>Authenticate with keys and then temporarily assume a role for access. This option is available only when you use the SQS Event Notifications collection method.</td>
</tr>
<tr>
<td></td>
<td>For more information about creating IAM users and assigning roles, see Creating an Identity and Access Management (IAM) user in the AWS Management Console when using the Amazon AWS S3 REST API</td>
</tr>
<tr>
<td></td>
<td>EC2 Instance IAM Role</td>
</tr>
<tr>
<td></td>
<td>If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata that is assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.</td>
</tr>
<tr>
<td>Event Format</td>
<td>Select AWS Cloud Trail JSON. The log source retrieves JSON formatted events.</td>
</tr>
<tr>
<td>Region Name</td>
<td>The region that the SQS Queue or the AWS S3 bucket is in.</td>
</tr>
<tr>
<td></td>
<td>Example: us-east-1, eu-west-1, ap-northeast-3</td>
</tr>
<tr>
<td>Use as a Gateway Log Source</td>
<td>Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.</td>
</tr>
<tr>
<td>Show Advanced Options</td>
<td>Select this option if you want to customize the event data.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File Pattern</td>
<td>This option is available when you set <strong>Show Advanced Options</strong> to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, <code>.\.*\.json\..gz</code></td>
</tr>
<tr>
<td>Local Directory</td>
<td>This option is available when you set <strong>Show Advanced Options</strong> to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API protocol attempts to retrieve events.</td>
</tr>
<tr>
<td>S3 Endpoint URL</td>
<td>This option is available when you set <strong>Show Advanced Options</strong> to Yes. The endpoint URL that is used to query the AWS S3 REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is <a href="http://s3.amazonaws.com">http://s3.amazonaws.com</a></td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses the Amazon Web Service by using a proxy, enable <strong>Use Proxy</strong>. If the proxy requires authentication, configure the <strong>Proxy Server</strong>, <strong>Proxy Port</strong>, <strong>Proxy Username</strong>, and <strong>Proxy Password</strong> fields. If the proxy does not require authentication, configure the <strong>Proxy Server</strong> and <strong>Proxy Port</strong> fields.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>How often a poll is made to scan for new data. If you are using the SQS event collection method, <strong>SQS Event Notifications</strong> can have a minimum value of 10 (seconds). Because SQS Queue polling can occur more often, a lower value can be used. If you are using the Directory Prefix event collection method, <strong>Use a Specific Prefix</strong> has a minimum value of 60 (seconds) or 1M. Because every listBucket request to an AWS S3 bucket incurs a cost to the account that owns the bucket, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds.</td>
</tr>
</tbody>
</table>
Table 21. Amazon AWS S3 REST API protocol common log source parameters when using the Directory Prefix method or the SQS method (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second that are sent to the flow pipeline. The default is 5000. Ensure that the EPS Throttle value is higher than the incoming rate or data processing might fall behind.</td>
</tr>
</tbody>
</table>

The following table describes the specific parameter values to collect audit events by using the Directory Prefix event collection method:

Table 22. Amazon AWS S3 REST API protocol log source-specific parameters when using the Directory Prefix method

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 Collection Method</td>
<td>Select <strong>Use a Specific Prefix</strong>.</td>
</tr>
<tr>
<td>Bucket Name</td>
<td>The name of the AWS S3 bucket where the log files are stored.</td>
</tr>
</tbody>
</table>
| Directory Prefix       | The root directory location on the AWS S3 bucket from where the CloudTrail logs are retrieved; for example, AWSLogs/<AccountNumber>/CloudTrail/<RegionName>/ To pull files from the root directory of a bucket, you must use a forward slash (/) in the **Directory Prefix** file path.  
**Note:**  
- Changing the **Directory Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull.  
- The **Directory Prefix** file path cannot begin with a forward slash (/) unless only the forward slash is used to collect data from the root of the bucket.  
- If the **Directory Prefix** file path is used to specify folders, you must not begin the file path with a forward slash (for example, use folder1/folder2 instead). |
| Signature Version      | Select **AWSSIGNATUREV2** or **AWSSIGNATURE4**. **AWSSIGNATUREV2** does not support all Amazon AWS regions. **AWSSIGNATURE4** supports all regions. If you are using a region that is supported only by **AWSSIGNATUREV4**, you must choose **AWSSIGNATURE4** from the list. |
Table 22. Amazon AWS S3 REST API protocol log source-specific parameters when using the Directory Prefix method (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Automatically Acquire Server Certificate(s)    | Select Yes for QRadar to automatically download the server certificate and begin trusting the target server. You can use this option to initialize a newly created log source, obtain new certificates, or replace expired certificates. Select No to download the certificate manually. Complete the following steps:  
1. Access your Amazon AWS CloudTrail S3 bucket.  
2. Export the certificate as a DER-encoded binary certificate to your desktop system. The file extension must be .DER.  
3. Copy the certificate to the /opt/QRadar/conf/trusted_certificates directory on the QRadar host where you plan to configure the log source. |

The following table describes the parameters that require specific values to collect audit events by using the SQS event collection method:

Table 23. Amazon AWS S3 REST API protocol log source-specific parameters when using the SQS method

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 Collection Method</td>
<td>Select SQS Event Notifications.</td>
</tr>
<tr>
<td>SQS Queue URL</td>
<td>The full URL that begins with https://, for the SQS Queue that is set up to receive notifications for ObjectCreated events from S3.</td>
</tr>
</tbody>
</table>

Related information
- t_logsource_add.dita
- t_amazon_aws_ct_credentials.dita#t_amazon_aws_ct_credentials
- t_DSM_guide_AWS_create_user_policy_REST_API.dita

Amazon Web Services protocol configuration options

The Amazon Web Services protocol for IBM Security QRadar collects AWS CloudTrail logs from Amazon CloudWatch logs. The following table describes the protocol-specific parameters for the Amazon Web Services protocol:

Table 24. Amazon Web Services log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Select Amazon Web Services from the Protocol Configuration list.</td>
</tr>
</tbody>
</table>
Table 24. Amazon Web Services log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Authentication Method** | **Access Key ID / Secret Key**  
Standard authentication that can be used from anywhere.  
**EC2 Instance IAM Role**  
If your QRadar managed host is running in an AWS EC2 instance, choosing this option uses the IAM role from the metadata that is assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container. |
| Access Key         | The Access Key ID that was generated when you configured the security credentials for your AWS user account. If you selected Access Key ID / Secret Key, the Access Key parameter displays. |
| Secret Key         | The Secret Key that was generated when you configured the security credentials for your AWS user account. If you selected Access Key ID / Secret Key, the Secret Key parameter displays. |
| Regions            | Select the check box for each region that is associated with the Amazon Web Service that you want to collect logs from.                                                                                        |
| Other Regions      | Type the names of any additional regions that are associated with the Amazon Web Service that you want to collect logs from. To collect from multiple regions use a comma-separated list, as shown in the following example: region1,region2 |
| AWS Service        | The name of the Amazon Web Service. From the AWS Service list, select CloudWatch Logs.                                                                                                                       |
| Log Group          | The name of the log group in Amazon CloudWatch where you want to collect logs from. **Note:** A single log source collects CloudWatch logs from 1 log group at a time. If you want to collect logs from multiple log groups, create a separate log source for each log group. |
| Log Stream (Optional) | The name of the log stream within a log group. If you want to collect logs from all log streams within a log group, leave this field blank.                                                                 |
| Filter Pattern (Optional) | Type a pattern for filtering the collected events. This pattern is not a regex filter. Only the events that contain the exact value that you specified are collected from CloudWatch Logs. If you type ACCEPT as the Filter Pattern value, only the events that contain the word ACCEPT are collected, as shown in the following example. |

{LogStreamName: LogStreamTest, Timestamp: 0, Message: ACCEPT OK, IngestionTime: 0, EventId: 0}
### Table 24. Amazon Web Services log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Extract Original Event**         | To forward only the original event that was added to the CloudWatch logs to QRadar, select this option. CloudWatch logs wrap the events that they receive with extra metadata. The original event is the value for the message key that is extracted from the CloudWatch log. The following CloudWatch logs event example shows the original event that is extracted from the CloudWatch log in bold text:  

```json
{LogStreamName: 123456786_CloudTrail_us-east-2, Timestamp: 1505744407363, Message: {"eventVersion": "1.05", "userIdentity": {"type": "IAMUser", "principalId": "AAAABBBCCCDDBBCCCM", "arn": "arn:aws:iam::1234567890:user/QRadar-ITeam", "accountId": "1234567890", "accessKeyId": "AAAABBBCCCDDBBCCCM", "userName": "User-Name", "sessionContext": {"attributes": {"mfaAuthenticated": "false", "creationDate": "2017-09-18T13:22:10Z"}}, "invokedBy": "signin.amazonaws.com", "eventTime": "2017-09-18T14:10:15Z", "eventSource": "cloudtrail.amazonaws.com", "eventName": "DescribeTrails", "awsRegion": "us-east-1", "sourceIPAdddress": "127.0.0.1", "userAgent": "signin.amazonaws.com", "requestParameters": {"includeShadowTrails": false, "trailNameList": []}, "responseElements": null, "requestID": "11ba0-7a9a-11a1-1b9a-444444441", "eventId": "2b914e08-1111-491d-bb0b-addd3f45b362", "eventType": "AwsApiCall", "recipientAccountId": "1234567890", "IngestionTime": 1505744407506, "EventId": 3357922236111111122224791267222222253333}
``` |
| **Use As A Gateway Log Source**    | If you do not want to define a custom log source identifier for events, ensure that this check box is clear. |
| **Log Source Identifier Pattern** | If you selected **Use As A Gateway Log Source**, use this option to define a custom Log Source Identifier for events that are being processed. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key.  

Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier displays. The following examples show multiple key-value pair functions.  

#### Patterns  

```
VPC=\sREJECT\sFAILURE
$1=\s(REJECT)\sOK
VPC-$1-$2=\s(ACCEPT)\s(OK)
```

#### Events  

```
{LogStreamName: LogStreamTest, Timestamp: 0, Message: ACCEPT OK, IngestionTime: 0, EventId: 0}
```

**Resulting custom log source identifier**  

```
VPC-ACCEPT-OK
```
Table 24. Amazon Web Services log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses the Amazon Web Service by using a proxy, select this option. If the proxy requires authentication, configure the Proxy Server, Proxy Port, Proxy Username, and Proxy Password fields. If the proxy does not require authentication, configure the Proxy Server and Proxy Port fields.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>Select Yes for QRadar to automatically download the server certificate and begin trusting the target server. You can use this option to initialize a newly created log source and obtain certificates, or to replace expired certificates.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The upper limit for the maximum number of events per second (EPS). The default is 5000. If the Use As A Gateway Log Source option is selected, this value is optional. If the EPS Throttle parameter value is left blank, no EPS limit is imposed by QRadar.</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Apache Kafka protocol configuration options
QRadar uses the Apache Kafka protocol to read streams of event data from topics in a Kafka cluster that uses the Consumer API. The Apache Kafka protocol can be used as a gateway log source by using the Universal DSM.

The Apache Kafka protocol is an outbound/active protocol.

The following table describes the protocol-specific parameters for the Apache Kafka protocol:

Table 25. Apache Kafka protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bootstrap Server List</td>
<td>The &lt;hostname/ip&gt;:&lt;port&gt; of the bootstrap server (or servers). Multiple servers can be specified in as a comma-separated list, such as in this example: hostname1:9092,1.1.1.1:9092.</td>
</tr>
<tr>
<td>Consumer Group</td>
<td>A unique string that identifies the consumer group this log source belongs to. A Consumer Group is a label that consumers give themselves so that each record that is published to a Kafka topic is delivered to one consumer instance within each subscribing consumer group. These labels allow Kafka to load balance the records over all consumer instances in a group.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Topic Subscription Method</strong></td>
<td>Select the method to use for subscribing to Kafka topics. Use the <strong>List Topics</strong> option to specify a list of topics. Use the <strong>Regex Pattern Matching</strong> option to specify a regular expression to match against available topics.</td>
</tr>
<tr>
<td><strong>Topic List</strong></td>
<td>Specify a comma-separated list of topic names to subscribe to. For example, Topic1,Topic2,Topic3 This option is only displayed when <strong>List Topics</strong> is selected for the <strong>Topic Subscription Method</strong> option.</td>
</tr>
<tr>
<td><strong>Topic Filter Pattern</strong></td>
<td>Specify a regular expression to match the topics to subscribe to. This option is only displayed when <strong>Regex Pattern Matching</strong> is selected for the <strong>Topic Subscription Method</strong> option.</td>
</tr>
<tr>
<td><strong>Use SASL Authentication</strong></td>
<td>Select this option to display SASL authentication configuration options. When you use SASL authentication without client authentication, you must place a copy of the server certificate in the /opt/qradar/conf/trusted_certificates/ directory.</td>
</tr>
<tr>
<td><strong>SASL Username</strong></td>
<td>The user name for SASL authentication.</td>
</tr>
<tr>
<td><strong>SASL Password</strong></td>
<td>The password for SASL authentication.</td>
</tr>
<tr>
<td><strong>Confirm SASL Password</strong></td>
<td>The password for SASL authentication.</td>
</tr>
<tr>
<td><strong>Use Client Authentication</strong></td>
<td>Select this option to display the client authentication configuration options.</td>
</tr>
<tr>
<td><strong>Key Store/Trust Store Type</strong></td>
<td>Select the archive file format for your Key Store and Trust Store Type: • JKS • PKCS12</td>
</tr>
<tr>
<td><strong>Trust Store Filename</strong></td>
<td>The name of the truststore file. The truststore must be placed in /opt/qradar/conf/trusted_certificates/kafka/.</td>
</tr>
<tr>
<td><strong>Trust Store Password</strong></td>
<td>The password for the truststore file.</td>
</tr>
<tr>
<td><strong>Confirm Trust Store Password</strong></td>
<td>Confirmation of the truststore <strong>Password</strong> field.</td>
</tr>
<tr>
<td><strong>Key Store Filename</strong></td>
<td>The name of the keystore file. The keystore must be placed in /opt/qradar/conf/trusted_certificates/kafka/.</td>
</tr>
<tr>
<td><strong>Key Store Password</strong></td>
<td>The password for the keystore file.</td>
</tr>
<tr>
<td><strong>Confirm Key Store Password</strong></td>
<td>Confirmation of the keystore <strong>Password</strong> field.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Private Key Password</strong></td>
<td>The password of the private key in the keystore file.</td>
</tr>
<tr>
<td><strong>Confirm Private Key Password</strong></td>
<td>Confirmation of the Private Key Password field.</td>
</tr>
<tr>
<td><strong>Use As A Gateway Log Source</strong></td>
<td>Select this option for the collected events to go through the QRadar Traffic Analysis engine and to automatically detect the appropriate log sources.</td>
</tr>
</tbody>
</table>
| **Log Source Identifier Pattern** | If you selected Use As A Gateway Log Source, use this option to define a custom Log Source Identifier for events that are being processed. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier displays. The following examples show multiple key-value pair functions. **Patterns**  
VPC=\sREJECT\sFAILUERE  
$1=\s(REJECT)\sOK  
VPC-$1-$2=\s(ACCEPT)\s(OK)  
**Events**  
{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}  
**Resulting custom log source identifier**  
VPC-ACCEPT-OK |
| **Character Sequence Replacement** | Select this option to replace specific literal character sequences in the event payload to actual characters. You can choose 1 or more of the following options:  
• Newline(CR LF) Character (\r\n)  
• Line Feed Character (\n)  
• Carriage Return Character (\r)  
• Tab Character (\t)  
• Space Character (\s) |
### Configuring Apache Kafka to enable Client Authentication

This task discusses how to enable Client Authentication with Apache Kafka.

#### Before you begin

1. Ensure that the ports that are used by the Kafka server are not blocked by a firewall.
2. To enable client authentication between the Kafka consumers (QRadar) and a Kafka brokers, a key and certificate for each broker and client in the cluster must be generated. The certificates also need to be signed by a certificate authority (CA).

#### About this task

In the following steps, you generate a CA, sign the client and broker certificates with it, and add it to the client and broker truststores. You also generate the keys and certificates by using the Java keytool and OpenSSL. Alternatively, an external CA can be used along with multiple CAs, one for signing broker certificates and another for client certificates.

#### Procedure

1. Generate the truststore, keystore, private key, and CA certificate.

   **Note:** Replace PASSWORD, VALIDITY, SERVER_ALIAS and CLIENT_ALIAS in the following commands with appropriate values.

   a) Generate Server keystore.

      **Note:**

      The common name (CN) of the broker certificates must match the fully qualified domain name (FQDN) of the server/host. The Kafka Consumer client that is used by QRadar compares the CN with the DNS domain name to ensure that it is connecting to the correct broker instead of a malicious one. Make sure to enter the FQDN for the CN/First and Last name value when you generate the Server keystore.

      ```
      keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -validity VALIDITY -genkey
      ```

   b) Generate CA Certificate.

      **Note:**

      This CA certificate can be used to sign all broker and client certificates.

      ```
      openssl req -new -x509 -keyout ca-key -out ca-cert -days VALIDITY
      ```

2. Generate Broker keystore.

3. Generate Client keystore.
c) Create Server truststore and import CA Certificate.

```shell
keytool -keystore kafka.server.truststore.jks -alias CARoot -import -file ca-cert
```

d) Create Client truststore and import CA Certificate.

```shell
keytool -keystore kafka.client.truststore.jks -alias CARoot -import -file ca-cert
```

e) Generate a Server Certificate and sign it using the CA.

```shell
keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -certreq -file cert-file
openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -days VALIDITY -CAcreateserial
```

```
Example
keytool -keystore kafka.server.keystore.jks -alias server.hostname -certreq -file cert-file
openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -days 365 -CAcreateserial
```

f) Import CA Certificate into the Server keystore.

```shell
keytool -keystore kafka.server.keystore.jks -alias CARoot -import -file ca-cert
```

g) Import Signed Server Certificate to the Server keystore.

```shell
keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -import -file cert-signed
```

```
Example
keytool -keystore kafka.server.keystore.jks -alias server.hostname -import -file cert-signed
```

h) Export the Server Certificate into the binary DER file.

**Note:** The `keytool -exportcert` command uses the DER format by default. Place the certificate in the `trusted_certificates/` directory of any EP that communicates with Kafka. You need the server certificate for every bootstrap server that you use in the configuration. Otherwise, QRadar rejects the TLS handshake with the server.

```shell
keytool -exportcert -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -file SERVER_ALIAS.der
```

```
Example
keytool -exportcert -keystore kafka.server.keystore.jks -alias server.hostname -file server.hostname.der
```

i) Generate a Client keystore.

```shell
keytool -keystore kafka.client.keystore.jks -alias CLIENT_ALIAS -validity VALIDITY -genkey
```
Example

keytool -keystore kafka.client.keystore.jks -alias client.hostname -validity 365 -genkey

j) Generate a Client Certificate and sign it using the CA.

keytool -keystore kafka.client.keystore.jks -alias CLIENT_ALIAS -certreq -file client-cert-file

openssl x509 -req -CA ca-cert -CAkey ca-key -in client-cert-file -out client-cert-signed -days VALIDITY -CAcreateserial

Example

keytool -keystore kafka.client.keystore.jks -alias client.hostname -certreq -file client-cert-file

openssl x509 -req -CA ca-cert -CAkey ca-key -in client-cert-file -out client-cert-signed -days 365 -CAcreateserial

k) Import CA Certificate into the Client keystore.

keytool -keystore kafka.client.keystore.jks -alias CARoot -import -file ca-cert

l) Import Signed Client Certificate to the Client keystore.

keytool -keystore kafka.client.keystore.jks -alias CLIENT_ALIAS -import -file client-cert-signed

Example

keytool -keystore kafka.client.keystore.jks -alias client.hostname -import -file client-cert-signed

m) Copy Client keystore and truststore and to QRadar.

1) Copy the kafka.client.keystore.jks and kafka.client.truststore.jks to /opt/qradar/conf/trusted_certificates/kafak/ on each of the Event processors that the log source is configured for.

2) Copy the server certificates <filename>.der that were generated for each broker to /opt/qradar/conf/trusted_certificates/.

2. Configure Kafka brokers for Client Authentication.

a) Find the **Socket Server Settings** section.

b) Complete 1 of the following options:

- If you are not using SASL Authentication, change `listeners=PLAINTEXT://:<port>` to `listeners=SSL://:<PORT>` and add `security.inter.broker.protocol=SSL`.
- If you are using SASL Authentication, change `listeners=PLAINTEXT://:<port>` to `listeners=SASL_SSL://:<PORT>` and add `security.inter.broker.protocol=SASL_SSL`.

c) Add the following properties to force encrypted communication between brokers and between the brokers and clients. Adjust the paths, file names, and passwords as you need them. These properties are the truststore and keystore of the **server**:

security.inter.broker.protocol=SSL

ssl.client.auth=required

ssl.keystore.location=/somefolder/kafka.server.keystore.jks

ssl.keystore.password=test1234
ssl.key.password=test1234
ssl.truststore.location=/somefolder/kafka.server.truststore.jks
ssl.truststore.password=test1234

Note:
Since the passwords are stored in plain text in the server.properties, it is advised that access to the file is restricted by way of file system permissions.

d) Restart the Kafka brokers that had their server.properties modified.

**Configuring Apache Kafka to enable SASL Authentication**

This task discusses how to enable SASL Authentication with Apache Kafka without SSL Client Authentication.

**Before you begin**

If you are using SASL Authentication with Client Authentication enabled, see “Configuring Apache Kafka to enable Client Authentication” on page 43.

1. Ensure that the ports that are used by the Kafka server are not blocked by a firewall.
2. To enable client authentication between the Kafka consumers (QRadar) and a Kafka brokers, a key and certificate for each broker and client in the cluster must be generated. The certificates also need to be signed by a certificate authority (CA).

**About this task**

In the following steps, you generate a CA, sign the client and broker certificates with it, and add it to the broker truststores. You also generate the keys and certificates by using the Java keytool and OpenSSL. Alternatively, an external CA can be used along with multiple CAs, one for signing broker certificates and another for client certificates.

**Procedure**

1. Generate the truststore, keystore, private key, and CA certificate.

   **Note:** Replace PASSWORD, VALIDITY, SERVER_ALIAS and CLIENT_ALIAS in the following commands with appropriate values.

   a) Generate Server keystore.

      **Note:**
      The common name (CN) of the broker certificates must match the fully qualified domain name (FQDN) of the server/host. The Kafka Consumer client that is used by QRadar compares the CN with the DNS domain name to ensure that it is connecting to the correct broker instead of a malicious one. Make sure to enter the FQDN for the CN/First and Last name value when you generate the Server keystore.

      ```
      keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -validity VALIDITY -genkey
      
      Example
      
      keytool -keystore kafka.server.keystore.jks -alias server.hostname -validity 365 -genkey
      ```

   b) Generate CA Certificate.

      **Note:**
      This CA certificate can be used to sign all broker and client certificates.
openssl req -new -x509 -keyout ca-key -out ca-cert -days VALIDITY

**Example**

openssl req -new -x509 -keyout ca-key -out ca-cert -days 365

c) Create Server truststore and import CA Certificate.

keytool -keystore kafka.server.truststore.jks -alias CARoot -import -file ca-cert

d) Generate a Server Certificate and sign it using the CA.

keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -certreq -file cert-file

openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -days VALIDITY -CAcreateserial

**Example**

keytool -keystore kafka.server.keystore.jks -alias server.hostname -certreq -file cert-file

openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -days 365 -CAcreateserial

e) Import CA Certificate into the Server keystore.

keytool -keystore kafka.server.keystore.jks -alias CARoot -import -file ca-cert

f) Import Signed Server Certificate to the Server keystore.

keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -import -file cert-signed

**Example**

keytool -keystore kafka.server.keystore.jks -alias server.hostname -import -file cert-signed

g) Export the Server Certificate into the binary DER file.

**Note:** The keytool -exportcert command uses the DER format by default. Place the certificate in the trusted_certificates/ directory of any EP that communicates with Kafka. You need the server certificate for every bootstrap server that you use in the configuration. Otherwise, QRadar rejects the TLS handshake with the server.

keytool -exportcert -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -file SERVER_ALIAS.der

**Example**

keytool -exportcert -keystore kafka.server.keystore.jks -alias server.hostname -file server.hostname.der

2. Configure Kafka brokers for Client Authentication.

a) Find the **Socket Server Settings** section and then change listeners=PLAINTEXT://:<port> to listeners=SSL://:<PORT>.

b) Add the following properties to force encrypted communication between brokers and between the brokers and clients. Adjust the paths, file names, and passwords as you need them. These properties are the truststore and keystore of the server:
security.inter.broker.protocol=SASL_SSL
ssl.client.auth=none
ssl.keystore.location=/somefolder/kafka.server.keystore.jks
ssl.keystore.password=test1234
ssl.key.password=test1234
ssl.truststore.location=/somefolder/kafka.server.truststore.jks
ssl.truststore.password=test1234

Note:
Since the passwords are stored in plain text in the server.properties, it is advised that access to the file is restricted by way of file system permissions.
c) Restart the Kafka brokers that had their server.properties modified.

Troubleshooting Apache Kafka

This reference provides troubleshooting options for configuring Apache Kafka to enable Client Authentication.

Apache Kafka

<table>
<thead>
<tr>
<th>Table 26. Troubleshooting for Apache Kafka Client Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issue</strong></td>
</tr>
<tr>
<td>The <strong>Use As A Gateway Log Source</strong> option is selected in the log source configuration, but log sources are not being automatically detected.</td>
</tr>
</tbody>
</table>
| No events are being received and the following error is displayed in the log source configuration form: “Encountered an error while attempting to fetch topic metadata... Please verify the configuration information.” | Verify that the bootstrap server and port details that are entered into the configuration are valid. If Client Authentication is enabled, verify the following things:  
  • The passwords that are entered are correct.  
  • The client truststore and keystore files are present in /opt/qradar/conf/trusted_certificates/kafka/ folder and the file names specified match.  
  • The server certificates (*.der) are present in /opt/qradar/conf/trusted_certificates/ folder. |
| No events are being received and the following error is displayed in the log source configuration form: “The user specified list of topics did not contain any topics that exists in the Kafka cluster. Please verify the topic list.” | When you use the **List Topics** options to subscribe to topics, QRadar attempts to verify the topics available in the Kafka cluster to the specified topics when the log source is initially started. If no topics match between what was entered in the configuration and what is available on the cluster, you are presented with this message. Verify the topic names that are entered in the configuration; also, consider the use of the **Regex Pattern Matching** option for subscribing to topics. |
### Blue Coat Web Security Service REST API protocol configuration options

To receive events from Blue Coat Web Security Service, configure a log source to use the Blue Coat Web Security Service REST API protocol.

The Blue Coat Web Security Service REST API protocol is an outbound/active protocol that queries the Blue Coat Web Security Service Sync API and retrieves recently hardened log data from the cloud.

The following table describes the protocol-specific parameters for the Blue Coat Web Security Service REST API protocol:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Username</td>
<td>The API user name that is used for authenticating with the Blue Coat Web Security Service. The API user name is configured through the Blue Coat Threat Pulse Portal.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is used for authenticating with the Blue Coat Web Security Service.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirmation of the Password field.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>When you configure a proxy, all traffic for the log source travels through the proxy for QRadar to access the Blue Coat Web Security Service. Configure the Proxy IP or Hostname, 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.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>If you select Yes from the list, QRadar downloads the certificate and begins trusting the target server.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>You can specify when the log collects data. The format is M/H/D for Months/Hours/Days. The default is 5 M.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The upper limit for the maximum number of events per second (EPS). The default is 5000.</td>
</tr>
</tbody>
</table>

### Centrify Redrock REST API protocol configuration options

The Centrify Redrock REST API protocol is an outbound/active protocol for IBM Security QRadar that collects events from Centrify Identity Platform.

The following parameters require specific values to collect events from Centrify Identity Platform:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Centrify Identity Platform</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Protocol Configuration</strong></td>
<td>Centrify Redrock REST API</td>
</tr>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type a unique name for the log source. The Log Source Identifier can be any valid value and does not need to reference a specific server. The Log Source Identifier can be the same value as the Log Source Name. If you have more than one Centrify Identity Platform log source that is configured, you might want to identify the first log source as centrify1, the second log source as centrify2, and the third log source as centrify3.</td>
</tr>
<tr>
<td><strong>Tenant ID</strong></td>
<td>The Centrify assigned unique customer or tenant ID.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>The user name that is associated with the Cloud service for Centrify Identity Platform.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password that is associated with the Centrify Identity Platform user name.</td>
</tr>
<tr>
<td><strong>Event Logging Filter</strong></td>
<td>Select the logging level of the events that you want to retrieve. Info, Warning and Error are selectable. At least one filter must be selected.</td>
</tr>
<tr>
<td><strong>Use Proxy</strong></td>
<td>When a proxy is configured, all traffic from the Centrify Redrock REST API travels through the proxy. 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.</td>
</tr>
<tr>
<td><strong>Automatically Acquire Server Certificate(s)</strong></td>
<td>Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>The maximum number of events per second. The default is 5000.</td>
</tr>
<tr>
<td><strong>Recurrence</strong></td>
<td>The time interval can be in hours (H), minutes (M) or days (D). The default is 5 minutes (5M).</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

### Cisco Firepower eStreamer protocol configuration options

To collect events in IBM QRadar from a Cisco Firepower eStreamer (Event Streamer) service, configure a log source to use the Cisco Firepower eStreamer protocol.

The Cisco Firepower eStreamer protocol is formerly known as Sourcefire Defense Center eStreamer protocol.

The Cisco firepower eStreamer protocol is an inbound/passive protocol.

Events are streamed to QRadar to be processed after the Cisco Firepower Management Center DSM is configured.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Cisco Firepower eStreamer</td>
</tr>
<tr>
<td>Server Port</td>
<td>The port number that the Cisco Firepower eStreamer services is configured to accept connection requests on. The default port that QRadar uses for Cisco Firepower eStreamer is 8302.</td>
</tr>
<tr>
<td>Keystore Filename</td>
<td>The directory path and file name for the keystore private key and associated certificate. By default, the import script creates the keystore file in the following directory: /opt/qradar/conf/ estreamer.keystore</td>
</tr>
<tr>
<td>Truststore Filename</td>
<td>The directory path and file name for the truststore files. The truststore file contains the certificates that are trusted by the client. By default, the import script creates the truststore file in the following directory: /opt/qradar/conf/ estreamer.truststore</td>
</tr>
<tr>
<td>Request Extra Data</td>
<td>Select this option to request intrusion event extra data from Cisco Firepower Management Center. For example, extra data includes the original IP address of an event.</td>
</tr>
</tbody>
</table>
Table 29. Cisco Firepower eStreamer protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Note: Domain Streaming Requests are supported only for eStreamer version 6.x. Leave the Domain field blank for eStreamer version 5.x. The domain where the events are streamed from. The value in the Domain field must be a fully qualified domain. This means that all ancestors of the desired domain must be listed starting with the top-level domain and ending with the leaf domain that you want to request events from. Example: Global is the top level domain, B is a second level domain that is a subdomain of Global, and C is a third-level domain and a leaf domain that is a subdomain of B. To request events from C, type the following value for the Domain parameter: Global \ B \ C</td>
</tr>
</tbody>
</table>

Cisco NSEL protocol configuration options

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

The Cisco NSEL protocol is an inbound/passive protocol. To integrate Cisco NSEL with QRadar, you must manually create a log source to receive NetFlow events. QRadar does not automatically discover or create log sources for syslog events from Cisco NSEL.

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

Table 30. Cisco NSEL protocol parameters

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

Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**EMC VMware protocol configuration options**

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

The EMC VMware protocol is an outbound/active protocol.

IBM QRadar supports the following event types for the EMC VMware protocol:

- Account Information
- Notice
- Warning
- Error
- System Informational
- System Configuration
- System Error
- User Login
- Misc Suspicious Event
- Access Denied
- Information
- Authentication
- Session Tracking

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td><strong>EMC VMware</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The value for this parameter must match the <strong>VMware IP</strong> parameter.</td>
</tr>
<tr>
<td>VMware IP</td>
<td>The IP address of the VMWare ESXi server. The VMware protocol appends the IP address of your VMware ESXi server with HTTPS before the protocol requests event data.</td>
</tr>
</tbody>
</table>

**Forwarded protocol configuration options**

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

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

To collect events from devices that forward HTTP or HTTPS requests, configure a log source to use the HTTP Receiver protocol.

The HTTP Receiver protocol is an inbound/passive protocol. The HTTP Receiver acts as an HTTP server on the configured listening port and converts the request body of any received POST requests into events. It supports both HTTPS and HTTP requests.

The following table describes the protocol-specific parameters for the HTTP Receiver protocol:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>From the list, select <strong>HTTP Receiver</strong>.</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address, host name, or any name to identify the device. Must be unique for the log source type.</td>
</tr>
<tr>
<td>Communication Type</td>
<td>Select <strong>HTTP</strong>, or <strong>HTTPS</strong>, or <strong>HTTPS and Client Authentication</strong>.</td>
</tr>
<tr>
<td>Client Certificate Path</td>
<td>If you select <strong>HTTPS and Client Authentication</strong> as the communication type, you must set the absolute path to the client certificate. You must copy the client certificate to the QRadar Console or the Event Collector for the log source.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The port that is used by QRadar to accept incoming HTTP Receiver events. The default port is 12469. <strong>Important</strong>: Do not use port 514. Port 514 is used by the standard Syslog listener.</td>
</tr>
<tr>
<td>Message Pattern</td>
<td>Denotes the start of each event.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second (EPS) that you do not want this protocol to exceed. The default is 5000.</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

IBM BigFix SOAP protocol configuration options

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

This protocol requires IBM BigFix versions 8.2.x to 9.5.2, and the Web Reports application for IBM BigFix. The IBM BigFix SOAP protocol is an outbound/active protocol that retrieves events in 30-second intervals over HTTP or HTTPS. As events are retrieved, the IBM BigFix DSM parses and categorizes the events.

The following table describes the protocol-specific parameters for the IBM BigFix SOAP protocol:
**Table 33. IBM BigFix SOAP protocol parameters**

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

---

**JDBC protocol configuration options**

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

The JDBC protocol is an outbound/active protocol. QRadar Does not include a MySQL driver for JDBC. If you are using a DSM or protocol that requires a MySQL JDBC driver, you must download and install the platform-independent MySQL Connector/J from http://dev.mysql.com/downloads/connector/j/.

1. Copy the Java™ archive (JAR) file to /opt/qradar/jars.
2. If you are using QRadar V7.3.1, you must also copy the JAR file to /opt/ibm/si/services/ecs-ec-ingress/eventgnosis/lib/q1labs/.
3. Restart Tomcat service by typing one of the following commands:
   - If you are using QRadar V7.2.8, type service tomcat restart.
   - If you are using QRadar V7.3.0 or V7.3.1, type systemctl restart tomcat.
4. Restart event collection services by typing one of the following commands:
   - If you are using QRadar V7.2.8, type service ecs-ec restart.
   - If you are using QRadar V7.3.0, type systemctl restart ecs-ec.
   - If you are using QRadar V7.3.1, type systemctl restart ecs-ec-ingress.

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

**Table 34. JDBC protocol parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>Select your Device Support Module (DSM) that uses the JDBC protocol from the Log Source Type list.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td><strong>Database Type</strong></td>
<td>Select the type of database that contains the events.</td>
</tr>
<tr>
<td><strong>Database Name</strong></td>
<td>The name of the database to which you want to connect.</td>
</tr>
<tr>
<td><strong>IP or Hostname</strong></td>
<td>The IP address or host name of the database server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Sybase - 1521 • Oracle - 1521 • Informix® - 9088 • DB2® - 50000 If a database instance is used with the MSDE database type, you must leave the Port field blank.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>A user account for QRadar in the database.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password that is required to connect to the database.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>The password that is required to connect to the database.</td>
</tr>
<tr>
<td><strong>Authentication Domain</strong></td>
<td>(MSDE only) If you did not select Use Microsoft JDBC, Authentication Domain is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td><strong>Database Instance</strong></td>
<td>(MSDE or Informix only) The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the Database Instance parameter must be blank in the log source configuration.</td>
</tr>
</tbody>
</table>
Table 34. JDBC protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Predefined Query (Optional)</strong></td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the <strong>none</strong> option.</td>
</tr>
<tr>
<td><strong>Table Name</strong></td>
<td>The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td><strong>Select List</strong></td>
<td>The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the <strong>Compare Field</strong>.</td>
</tr>
<tr>
<td><strong>Compare Field</strong></td>
<td>A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. Enables the protocol to identify events that were previously polled by the protocol to ensure that duplicate events are not created.</td>
</tr>
<tr>
<td><strong>Use Prepared Statements</strong></td>
<td>Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.</td>
</tr>
<tr>
<td><strong>Start Date and Time (Optional)</strong></td>
<td>Type the start date and time for database polling in the following format: 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.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value. The maximum polling interval is one week.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000.</td>
</tr>
<tr>
<td><strong>Security Mechanism (DB2 only)</strong></td>
<td>From the list, select the security mechanism that is supported by your DB2 server. If you don't want to select a security mechanism, select <strong>None</strong>. The default is <strong>None</strong>. For more information about security mechanisms that are supported by DB2 environments, see the IBM Support website (<a href="https://www.ibm.com/support/knowledgelcenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvjcsec.html">https://www.ibm.com/support/knowledgelcenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvjcsec.html</a>)</td>
</tr>
<tr>
<td><strong>Use Named Pipe Communication (MSDE only)</strong></td>
<td>If you did not select <strong>Use Microsoft JDBC, Use Named Pipe Communication</strong> is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Database Cluster Name (MSDE only)</strong></td>
<td>If you selected <strong>Use Named Pipe Communication</strong>, the <strong>Database Cluster Name</strong> parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.</td>
</tr>
<tr>
<td><strong>Use NTLMv2 (MSDE only)</strong></td>
<td>If you did not select <strong>Use Microsoft JDBC</strong>, <strong>Use NTLMv2</strong> is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td><strong>Use Microsoft JDBC (MSDE only)</strong></td>
<td>If you want to use the Microsoft JDBC driver, you must enable <strong>Use Microsoft JDBC</strong>.</td>
</tr>
<tr>
<td><strong>Use SSL (MSDE only)</strong></td>
<td>Select this option if your connection supports SSL. This option appears only for MSDE.</td>
</tr>
<tr>
<td><strong>Microsoft SQL Server Hostname (MSDE only)</strong></td>
<td>If you selected <strong>Use Microsoft JDBC</strong> and <strong>Use SSL</strong>, the <strong>Microsoft SQL Server Hostname</strong> parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
<tr>
<td><strong>Use Oracle Encryption</strong></td>
<td><strong>Oracle Encryption and Data Integrity settings</strong> is also known as <strong>Oracle Advanced Security</strong>. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.</td>
</tr>
<tr>
<td><strong>Database Locale (Informix only)</strong></td>
<td>For multilingual installations, use this field to specify the language to use.</td>
</tr>
<tr>
<td><strong>Code-Set (Informix only)</strong></td>
<td>The <strong>Code-Set</strong> parameter displays after you choose a language for multilingual installations. Use this field to specify the character set to use.</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>Select this check box to enable the log source. By default, the check box is selected.</td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
<td>From the list, select the <strong>Credibility</strong> of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
<td>Select the <strong>Target Event Collector</strong> to use as the target for the log source.</td>
</tr>
</tbody>
</table>
Table 34. JDBC protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coalescing Events</td>
<td>Select the <strong>Coalescing Events</strong> check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the <strong>Coalescing Events</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>Select the <strong>Store Event Payload</strong> check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the <strong>Store Event Payload</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

Related information
- Configuring JDBC Over SSL with a Self-signed Certificate
- Configuring JDBC Over SSL with an Externally-signed Certificate

**JDBC - SiteProtector protocol configuration options**

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

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

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

Table 35. JDBC - SiteProtector protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td><strong>JDBC - SiteProtector</strong></td>
</tr>
<tr>
<td>Database Type</td>
<td>From the list, select <strong>MSDE</strong> as the type of database to use for the event source.</td>
</tr>
<tr>
<td>Database Name</td>
<td>Type <strong>RealSecureDB</strong> as the name of the database to which the protocol can connect.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number that is used by the database server. The JDBC - SiteProtector configuration port must match the listener port of the database. The database must have incoming TCP connections enabled. If you define a <strong>Database Instance</strong> when with MSDE as the database type, you must leave the <strong>Port</strong> parameter blank in your log source configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>If you want to track access to a database by the JDBC protocol, you can create a specific user for your QRadar system.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication Domain</td>
<td>If you select MSDE and the database is configured for Windows, you must define a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>If you select MSDE and you have multiple SQL server instances on one server, define the instance to which you want to connect. If you use a non-standard port in your database configuration, or access is blocked to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>The predefined database query for your log source. Predefined database queries are only available for special log source connections.</td>
</tr>
<tr>
<td>Table Name</td>
<td>SensorData1</td>
</tr>
<tr>
<td>AVP View Name</td>
<td>SensorDataAVP</td>
</tr>
<tr>
<td>Response View Name</td>
<td>SensorDataResponse</td>
</tr>
<tr>
<td>Select List</td>
<td>Type * to include all fields from the table or view.</td>
</tr>
<tr>
<td>Compare Field</td>
<td>SensorDataRowID</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Prepared statements allow the JDBC protocol source to set up the SQL statement, and then execute the SQL statement numerous times with different parameters. For security and performance reasons, use prepared statements. You can clear this check box to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
<tr>
<td>Include Audit Events</td>
<td>Specifies to collect audit events from IBM Proventia Management SiteProtector®.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>Optional. A start date and time for when the protocol can start to poll the database.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>The amount of time between queries to the event table. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. Numeric values without an H or M designator poll in seconds.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed.</td>
</tr>
<tr>
<td>Database Locale</td>
<td>For multilingual installations, use the Database Locale field to specify the language to use.</td>
</tr>
<tr>
<td>Database Codeset</td>
<td>For multilingual installations, use the Codeset field to specify the character set to use.</td>
</tr>
<tr>
<td>Use Named Pipe Communication</td>
<td>If you are using Windows authentication, enable this parameter to allow authentication to the AD server. If you are using SQL authentication, disable Named Pipe Communication.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>The cluster name to ensure that named pipe communications function properly.</td>
</tr>
</tbody>
</table>
Table 35. JDBC - SiteProtector protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use NTLMv2</td>
<td>Forces MSDE connections to use the NTLMv2 protocol with SQL servers that require NTLMv2 authentication. The <strong>Use NTLMv2</strong> check box does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Enables SSL encryption for the JDBC protocol.</td>
</tr>
<tr>
<td>Log Source Language</td>
<td>Select the language of the events that are generated by the log source. The log source language helps the system parse events from external appliances or operating systems that can create events in multiple languages.</td>
</tr>
</tbody>
</table>

**Juniper Networks NSM protocol configuration options**

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

The Juniper Networks NSM protocol is an inbound/passive protocol.

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

| Table 36. Juniper Networks NSM protocol parameters |
|---------------------------------|--------------------------------------------------|
| Parameter                      | Description                                     |
| Log Source Type                | **Juniper Networks Network and Security Manager** |
| Protocol Configuration         | **Juniper NSM**                                 |

**Juniper Security Binary Log Collector protocol configuration options**

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


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

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

<table>
<thead>
<tr>
<th>Table 37. Juniper Security Binary Log Collector protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
</tbody>
</table>
Table 37. Juniper Security Binary Log Collector protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| XML Template File Location       | The path to the XML file used to decode the binary stream from your Juniper SRX or Juniper J Series appliance. By default, the device support module (DSM) includes an XML file for decoding the binary stream.  
|                                  | The XML file is in the following directory: /opt/qradar/conf/security_log.xml.                                                                                                                                 |

Log File protocol configuration options

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

The Log File protocol is an outbound/active protocol that is intended for systems that write daily event logs. It is not appropriate to use the Log File protocol for devices that append information to their event files.

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

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

Table 38. Log File protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Log File</td>
</tr>
<tr>
<td>Remote Port</td>
<td>If the remote host uses a non-standard port number, you must adjust the port value to retrieve events.</td>
</tr>
</tbody>
</table>
| SSH Key File     | If the system is configured to use key authentication, type the SSH key. When an SSH key file is used, the Remote Password field is ignored. The SSH key must be located in the /opt/qradar/conf/keys directory.  
|                  | **Note:** The SSH Key File field no longer accepts a file path. It can't contain "/" or ".". You must type the file name for the SSH key. The keys for existing configurations are copied to the /opt/qradar/conf/keys directory. To ensure uniqueness, the keys will have "_<Timestamp>" appended to the file name. |
| Remote Directory | For FTP, if the log files are in the remote user’s home directory, you can leave the remote directory blank. A blank remote directory field supports systems where a change in the working directory (CWD) command is restricted. |
| Recursive        | Enable this check box to allow FTP or SFTP connections to recursively search sub folders of the remote directory for event data. Data that is collected from sub folders depends on matches to the regular expression in the FTP File Pattern. The Recursive option is not available for SCP connections. |
| FTP File Pattern | The regular expression (regex) that is needed to identify the files to download from the remote host.                                                                                                       |
Table 38. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP Transfer Mode</td>
<td>For ASCII transfers over FTP, you must select NONE in the Processor field and LINEBYLINE in the Event Generator field.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The time interval to determine how frequently the remote directory is scanned for new event log files. The time interval can include values in hours (H), minutes (M), or days (D). For example, a recurrence of 2H scans the remote directory every 2 hours.</td>
</tr>
<tr>
<td>Run On Save</td>
<td>Starts the log file import immediately after you save the log source configuration. When selected, this check box clears the list of previously downloaded and processed files. After the first file import, the Log File protocol follows the start time and recurrence schedule that is defined by the administrator.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The number of Events Per Second (EPS) that the protocol cannot exceed.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>Changes the local directory on the Target Event Collector to store event logs before they are processed.</td>
</tr>
<tr>
<td>Local Directory</td>
<td>The local directory on the Target Event Collector. The directory must exist before the Log File protocol attempts to retrieve events.</td>
</tr>
<tr>
<td>File Encoding</td>
<td>The character encoding that is used by the events in your log file.</td>
</tr>
<tr>
<td>Folder Separator</td>
<td>The character that is used to separate folders for your operating system. Most configurations can use the default value in Folder Separator field. This field is intended for operating systems that use a different character to define separate folders. For example, periods that separate folders on mainframe systems.</td>
</tr>
</tbody>
</table>

Configure QRadar to use FTPS for the Log File protocol

To configure FTPS for the Log File protocol, you must place server SSL certificates on all QRadar Event Collectors that connect to your FTP server. If your SSL certificate is not RSA 2048, create a new SSL certificate.

The following command provides an example of creating a certificate on a LINUX system by using OpenSSL:

```
openssl req -newkey rsa:2048 -nodes -keyout ftpserver.key -x509 -days 365 -out ftpserver.crt
```

Files on the FTP server that have a .crt file extension must be copied to the /opt/qradar/conf/trusted_certificates directory on each of your Event Collectors.

Microsoft Azure Event Hubs protocol configuration options

The Microsoft Azure Event Hubs protocol is an outbound/active protocol for IBM Security QRadar collects events from Microsoft Azure Event Hubs.

The following parameters require specific values to collect events from Microsoft Azure Event Hubs appliances:

Table 39. Microsoft Azure Event Hubs log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Microsoft Azure</td>
</tr>
</tbody>
</table>
Table 39. Microsoft Azure Event Hubs log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Microsoft Azure Event Hubs</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The Log Source Identifier can be any valid value, including the same value as the Log Source Name parameter, and doesn't need to reference a specific server. If you configured multiple Microsoft Azure Event Hub log sources, you might want to identify the first log source as EventHub-1, the second log source as EventHub-2, and the third log source as EventHub-3.</td>
</tr>
<tr>
<td>Use as a Gateway Log Source</td>
<td>Enable this check box to send all events through the QRadar Traffic Analysis Engine and automatically detect one or more appropriate log sources.</td>
</tr>
<tr>
<td>Use Event Hub Connection String</td>
<td>Enable this check box to use an Event Hub Connection String. Clear this check box to manually enter the values for the Event Hub Namespace Name, Event Hub Name, SAS Key Name, and SAS Key parameters.</td>
</tr>
<tr>
<td>Event Hub Connection String</td>
<td>The Event Hub Connection String contains the Namespace Name, the path to the Event Hub within the namespace, and the Shared Access Signature (SAS) Authentication information.</td>
</tr>
<tr>
<td>Namespace Name</td>
<td>The Namespace Name value is the name of the top-level directory that contains the Event Hub entities in the Microsoft Azure Event Hubs user interface.</td>
</tr>
<tr>
<td>Event Hub Name</td>
<td>The Event Hub Name is the identifier for the Event Hub that you want to access. The Event Hub Name should match one of the Event Hub entities within the namespace.</td>
</tr>
<tr>
<td>SAS Key Name</td>
<td>The Shared Access Signature (SAS) Name identifies the event publisher.</td>
</tr>
<tr>
<td>SAS Key</td>
<td>The Shared Access Signature (SAS) Key authenticates the event publisher.</td>
</tr>
<tr>
<td>Consumer Group</td>
<td>A Consumer Group specifies the view that is used during the connection. Each Consumer Group maintains its own session tracking. Any connection that shares consumer groups and connection information shares session tracking information.</td>
</tr>
<tr>
<td>Use Storage Account Connection String</td>
<td>Enable this check box to use a Storage Account Connection String. Clear this check box to manually enter the Storage Account Name and Storage Account Key.</td>
</tr>
<tr>
<td>Storage Account Connection String</td>
<td>A Storage Account Connection String includes authentication for the Storage Account Name and Storage Account Key that is used to access the data in the Azure Storage Account.</td>
</tr>
</tbody>
</table>
Table 39. Microsoft Azure Event Hubs log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Account Name</td>
<td>The Storage Account Name is part of the authentication process that is required to access data in the Azure Storage Account.</td>
</tr>
<tr>
<td>Storage Account Key</td>
<td>The Storage Account Key is part of the authentication process that is required to access data in the Azure Storage Account.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second (EPS). The default is 5000.</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a log source” on page 4
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 DHCP protocol configuration options
To receive events from Microsoft DHCP servers, configure a log source to use the Microsoft DHCP protocol.

The Microsoft DHCP protocol is an outbound/active protocol.

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

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

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

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

Table 40. Microsoft DHCP protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Microsoft DHCP</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique hostname or other identifier unique to the log source.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IP address or host name of your Microsoft DHCP server.</td>
</tr>
<tr>
<td>Domain</td>
<td>Type the domain for your Microsoft DHCP server.</td>
</tr>
<tr>
<td></td>
<td>This parameter is optional if your server is not in a domain.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name that is required to access the DHCP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password that is required to access the DHCP server.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password that is required to access the server.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Folder Path</td>
<td>The directory path to the DHCP log files. The default is c$:/WINDOWS/system32/dhcp/</td>
</tr>
<tr>
<td>File Pattern</td>
<td>The regular expression (regex) that identifies event logs. The log files must contain a three-character abbreviation for a day of the week.</td>
</tr>
<tr>
<td></td>
<td>Use one of the following file patterns:</td>
</tr>
<tr>
<td></td>
<td>English:</td>
</tr>
<tr>
<td></td>
<td>• IPv4 file pattern: DhcpSrvLog-(?:Sun</td>
</tr>
<tr>
<td></td>
<td>• IPv6 file pattern: DhcpV6SrvLog-(?:Sun</td>
</tr>
<tr>
<td></td>
<td>• Mixed IPv4 and IPv6 file pattern: Dhcp.*SrvLog-(?:Sun</td>
</tr>
<tr>
<td></td>
<td>Polish:</td>
</tr>
<tr>
<td></td>
<td>• IPv4 file pattern: DhcpSrvLog-(?:Piq</td>
</tr>
<tr>
<td></td>
<td>• IPv6 file pattern: DhcpV6SrvLog-(?:Pt</td>
</tr>
<tr>
<td>Recursive</td>
<td>Select this option if you want the file pattern to search the sub folders.</td>
</tr>
<tr>
<td>SMB Version</td>
<td>The version of SMB to use:</td>
</tr>
<tr>
<td></td>
<td>AUTO Auto-detects to the highest version that the client and server agree to use.</td>
</tr>
<tr>
<td></td>
<td>SMB1 Forces the use of SMB1.</td>
</tr>
<tr>
<td></td>
<td>SMB2 Forces the use of SMB2.</td>
</tr>
<tr>
<td>Polling Interval (in seconds)</td>
<td>The number of seconds between queries to the log files to check for new data. The minimum polling interval is 10 seconds. The maximum polling interval is 3,600 seconds.</td>
</tr>
<tr>
<td>Throttle events/sec</td>
<td>The maximum number of events the DHCP protocol can forward per second. The minimum value is 100 EPS. The maximum value is 20,000 EPS.</td>
</tr>
<tr>
<td>File Encoding</td>
<td>The character encoding that is used by the events in your log file.</td>
</tr>
<tr>
<td>Enabled</td>
<td>When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.</td>
</tr>
<tr>
<td>Credibility</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 40. Microsoft DHCP protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Event Collector</td>
<td>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.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>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.</td>
</tr>
</tbody>
</table>

Microsoft Exchange protocol configuration options


The Microsoft Exchange protocol is an outbound/active protocol.

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

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

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

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

Table 41. Microsoft Exchange protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Microsoft Exchange</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address, host name, or name to identify your log source.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IP address or host name of your Microsoft Exchange server.</td>
</tr>
<tr>
<td>Domain</td>
<td>Type the domain for your Microsoft Exchange server. This parameter is optional if your server is not in a domain.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name that is required to access your server.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password that is required to access your server.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password that is required to access the server.</td>
</tr>
<tr>
<td>SMTP Log Folder Path</td>
<td>When the folder path is clear, SMTP event collection is disabled.</td>
</tr>
<tr>
<td>OWA Log Folder Path</td>
<td>When the folder path is clear, OWA event collection is disabled.</td>
</tr>
<tr>
<td>MSGTRK Log Folder Path</td>
<td>Message tracking is available on Microsoft Exchange servers that are</td>
</tr>
<tr>
<td></td>
<td>assigned the Hub Transport, Mailbox, or Edge Transport server role.</td>
</tr>
<tr>
<td>Use Custom File Patterns</td>
<td>Select this check box to configure custom file patterns. Leave the check</td>
</tr>
<tr>
<td></td>
<td>box clear to use the default file patterns.</td>
</tr>
<tr>
<td>MSGTRK File Pattern</td>
<td>The regular expression (regex) that is used to identify and download the</td>
</tr>
<tr>
<td></td>
<td>MSTRK logs. All files that match the file pattern are processed.</td>
</tr>
<tr>
<td></td>
<td>The default file pattern is MSGTRK\d+-\d+. (?:\log</td>
</tr>
<tr>
<td>MSGTRKMD File Pattern</td>
<td>The regular expression (regex) that is used to identify and download the</td>
</tr>
<tr>
<td></td>
<td>MSGTRKMD logs. All files that match the file pattern are processed.</td>
</tr>
<tr>
<td></td>
<td>The default file pattern is MSGTRKMD\d+-\d+. (?:\log</td>
</tr>
<tr>
<td>MSGTRKMS File Pattern</td>
<td>The regular expression (regex) that is used to identify and download the</td>
</tr>
<tr>
<td></td>
<td>MSGTRKMS logs. All files that match the file pattern are processed.</td>
</tr>
<tr>
<td></td>
<td>The default file pattern is MSGTRKMS\d+-\d+. (?:\log</td>
</tr>
<tr>
<td>MSGTRKMA File Pattern</td>
<td>The regular expression (regex) that is used to identify and download the</td>
</tr>
<tr>
<td></td>
<td>MSGTRKMA logs. All files that match the file pattern are processed.</td>
</tr>
<tr>
<td></td>
<td>The default file pattern is MSGTRKMA\d+-\d+. (?:\log</td>
</tr>
<tr>
<td>SMTP File Pattern</td>
<td>The regular expression (regex) that is used to identify and download the</td>
</tr>
<tr>
<td></td>
<td>SMTP logs. All files that match the file pattern are processed.</td>
</tr>
<tr>
<td></td>
<td>The default file pattern is *. (?:\log</td>
</tr>
<tr>
<td>OWA File Pattern</td>
<td>The regular expression (regex) that is used to identify and download the</td>
</tr>
<tr>
<td></td>
<td>OWA logs. All files that match the file pattern are processed.</td>
</tr>
<tr>
<td></td>
<td>The default file pattern is *. (?:\log</td>
</tr>
<tr>
<td>Force File Read</td>
<td>If the check box is cleared, the log file is read only when QRadar</td>
</tr>
<tr>
<td></td>
<td>detects a change in the modified time or file size.</td>
</tr>
<tr>
<td>Recursive</td>
<td>If you want the file pattern to search sub folders, use this option. By</td>
</tr>
<tr>
<td></td>
<td>default, the check box is selected.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SMB Version</td>
<td>The version of SMB to use:</td>
</tr>
<tr>
<td>AUTO</td>
<td>Auto-detects to the highest version that the client and server agree to use.</td>
</tr>
<tr>
<td>SMB1</td>
<td>Forces the use of SMB1.</td>
</tr>
<tr>
<td>SMB2</td>
<td>Forces the use of SMB2.</td>
</tr>
<tr>
<td>Polling Interval (In seconds)</td>
<td>Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds.</td>
</tr>
<tr>
<td>Throttle Events/Second</td>
<td>The maximum number of events the Exchange protocol can forward per second.</td>
</tr>
<tr>
<td>File Encoding</td>
<td>The character encoding that is used by the events in your log file.</td>
</tr>
</tbody>
</table>

**Microsoft IIS protocol configuration options**

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

The Microsoft IIS protocol is an outbound/active protocol.

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

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Microsoft IIS</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address, host name, or name to identify your log source.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IP address or host name of your Microsoft IIS server.</td>
</tr>
<tr>
<td>Domain</td>
<td>Type the domain for your Microsoft IIS server.</td>
</tr>
<tr>
<td></td>
<td>This parameter is optional if your server is not in a domain.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name that is required to access your server.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password that is required to access your server.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password that is required to access the server.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Log Folder Path</td>
<td>The directory path to access the log files. For example, administrators can use the c$/LogFiles/ directory for an administrative share, or the LogFiles/ directory for a public share folder path. However, the c:/LogFiles directory is not a supported log folder path. If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the privileges that are required to read the log files. Local system or domain administrator privileges are also sufficient to access a log files that are on an administrative share.</td>
</tr>
<tr>
<td>File Pattern</td>
<td>The regular expression (regex) that identifies the event logs.</td>
</tr>
<tr>
<td>Recursive</td>
<td>If you want the file pattern to search sub folders, use this option. By default, the check box is selected.</td>
</tr>
<tr>
<td>SMB Version</td>
<td>The version of SMB to use:</td>
</tr>
<tr>
<td>AUTO</td>
<td>Auto-detects to the highest version that the client and server agree to use.</td>
</tr>
<tr>
<td>SMB1</td>
<td>Forces the use of SMB1.</td>
</tr>
<tr>
<td>SMB2</td>
<td>Forces the use of SMB2.</td>
</tr>
<tr>
<td>Polling Interval (In seconds)</td>
<td>Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds.</td>
</tr>
<tr>
<td>Throttle Events/Second</td>
<td>The maximum number of events the IIS protocol can forward per second.</td>
</tr>
<tr>
<td>File Encoding</td>
<td>The character encoding that is used by the events in your log file.</td>
</tr>
</tbody>
</table>

**Note:** If you use Advanced IIS Logging, you need to create a new log definition. In the Log Definition window, ensure that the following fields are selected in the Selected Fields section:

- Date-UTC
- Time-UTC
- URI-Stem
- URI-Querystring
- ContentPath
- Status
- Server Name
- Referer
- Win325Status
- Bytes Sent
Microsoft Security Event Log protocol configuration options

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Windows Security Event Log</td>
</tr>
</tbody>
</table>

Microsoft Security Event Log over MSRPC Protocol

The Microsoft Security Event Log over MSRPC protocol (MSRPC) is an outbound/active protocol that collects Windows events without installing an agent on the Windows host.

The MSRPC protocol uses the Microsoft Distributed Computing Environment/Remote Procedure Call (DCE/RPC) specification to provide agentless, encrypted event collection. The MSRPC protocol provides higher event rates than the default Microsoft Windows Security Event Log protocol, which uses WMI/DCOM for event collection.

The following table lists the supported features of the MSRPC protocol.
<table>
<thead>
<tr>
<th>Features</th>
<th>Microsoft Security Event Log over MSRPC protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Connection test tool</td>
<td>The MSRPC test tool checks the connectivity between the QRadar appliance and a Windows host. The MSRPC test tool is part of the MSRPC protocol RPM and can be found in /opt/qradar/jars after you install the protocol. For more information, see MSRPC test tool (<a href="http://www.ibm.com/support/docview.wss?uid=swg21959348">http://www.ibm.com/support/docview.wss?uid=swg21959348</a>)</td>
</tr>
<tr>
<td>Protocol type</td>
<td>The operating system dependent type of the remote procedure protocol for collection of events. Select one of the following options from the Protocol Type list:</td>
</tr>
<tr>
<td></td>
<td><strong>MS-EVEN6</strong></td>
</tr>
<tr>
<td></td>
<td>The default protocol type for new log sources. The protocol type that is used by QRadar to communicate with Windows Vista and Windows Server 2008 and later.</td>
</tr>
<tr>
<td></td>
<td><strong>MS-EVEN (for Windows XP/2003)</strong></td>
</tr>
<tr>
<td></td>
<td>The protocol type that is used by QRadar to communicate with Windows XP and Windows Server 2003. Windows XP and Windows Server 2003 are not supported by Microsoft. The use of this option might not be successful.</td>
</tr>
<tr>
<td></td>
<td><strong>auto-detect (for legacy configurations)</strong></td>
</tr>
<tr>
<td></td>
<td>Previous log source configurations for the Microsoft Windows Security Event Log DSM use the auto-detect (for legacy configurations) protocol type. Upgrade to the MS_EVEN6 or the MS-EVEN (for Windows XP/2003) protocol type.</td>
</tr>
<tr>
<td>Maximum EPS rate</td>
<td>100 EPS / Windows host</td>
</tr>
<tr>
<td>Maximum overall EPS rate of MSRPC</td>
<td>8500 EPS / IBM QRadar 16xx or 18xx appliance</td>
</tr>
<tr>
<td>Maximum number of supported log sources</td>
<td>500 log sources / QRadar 16xx or 18xx appliance</td>
</tr>
<tr>
<td>Bulk log source support</td>
<td>Yes</td>
</tr>
<tr>
<td>Encryption</td>
<td>Yes</td>
</tr>
<tr>
<td>Features</td>
<td>Microsoft Security Event Log over MSRPC protocol</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Supported event types</td>
<td>Application</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>DNS Server</td>
</tr>
<tr>
<td></td>
<td>File Replication</td>
</tr>
<tr>
<td></td>
<td>Directory Service logs</td>
</tr>
<tr>
<td>Supported Windows Operating Systems</td>
<td>Windows Server 2019 (including Core)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016 (including Core)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 (including Core)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 (including Core)</td>
</tr>
<tr>
<td></td>
<td>Windows 10</td>
</tr>
<tr>
<td></td>
<td>Windows 8</td>
</tr>
<tr>
<td></td>
<td>Windows 7</td>
</tr>
<tr>
<td></td>
<td>MSRPC is not supported on versions of Microsoft Windows with end of life status such as Windows 2003 and Windows XP.</td>
</tr>
<tr>
<td>Required permissions</td>
<td>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 be used depending on how Microsoft Group Policy Objects are configured.</td>
</tr>
<tr>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\eventlog</td>
</tr>
<tr>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Nls \Language</td>
</tr>
<tr>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft Windows\CurrentVersion</td>
</tr>
<tr>
<td>Required RPM files</td>
<td>PROTOCOL-WindowsEventRPC-QRadar_release-Build_number.noarch.rpm</td>
</tr>
<tr>
<td></td>
<td>DSM-MicrosoftWindows-QRadar_release-Build_number.noarch.rpm</td>
</tr>
<tr>
<td></td>
<td>DSM-DSMCommon-QRadar_release-Build_number.noarch.rpm</td>
</tr>
</tbody>
</table>
Table 44. Supported features of the MSRPC protocol (continued)

<table>
<thead>
<tr>
<th>Features</th>
<th>Microsoft Security Event Log over MSRPC protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows service requirements</td>
<td><strong>For Windows Vista and later</strong></td>
</tr>
<tr>
<td></td>
<td>Remote Procedure Call (RPC)</td>
</tr>
<tr>
<td></td>
<td>RPC Endpoint Mapper</td>
</tr>
<tr>
<td></td>
<td><strong>For Windows 2003</strong></td>
</tr>
<tr>
<td></td>
<td>Remote Registry</td>
</tr>
<tr>
<td></td>
<td>Server</td>
</tr>
<tr>
<td>Windows port requirements</td>
<td><strong>For Windows Vista and later</strong></td>
</tr>
<tr>
<td></td>
<td>TCP port 135</td>
</tr>
<tr>
<td></td>
<td>TCP port 445</td>
</tr>
<tr>
<td></td>
<td>TCP port that is dynamically allocated for RPC,</td>
</tr>
<tr>
<td></td>
<td>from port 49152 up to 65535</td>
</tr>
<tr>
<td></td>
<td><strong>For Windows 2003</strong></td>
</tr>
<tr>
<td></td>
<td>TCP port 445</td>
</tr>
<tr>
<td></td>
<td>TCP port 139</td>
</tr>
<tr>
<td>Special features</td>
<td>Supports encrypted events by default.</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>A security content pack with Windows custom</td>
</tr>
<tr>
<td></td>
<td>event properties is available on IBM Fix Central.</td>
</tr>
<tr>
<td>Intended application</td>
<td>Agentless event collection for Windows operating</td>
</tr>
<tr>
<td></td>
<td>systems that can support 100 EPS per log source.</td>
</tr>
<tr>
<td>Tuning support</td>
<td>MSRPC is limited to 100 EPS / Windows host. For</td>
</tr>
<tr>
<td></td>
<td>higher event rate systems, see the <em>IBM QRadar</em></td>
</tr>
<tr>
<td></td>
<td><em>WinCollect User Guide</em>.</td>
</tr>
<tr>
<td>Event filtering support</td>
<td>MSRPC does not support event filtering. See the</td>
</tr>
<tr>
<td></td>
<td><em>IBM QRadar WinCollect User Guide</em> for this feature.*</td>
</tr>
<tr>
<td>More information</td>
<td>Microsoft support (<a href="http://support.microsoft.com/">http://support.microsoft.com/</a>)</td>
</tr>
</tbody>
</table>

In contrast to WMI/DCOM, the MSRPC protocol provides twice the EPS. The event rates are shown in the following table.

Table 45. Contrast between MSRPC and WMI/DCOM event rates

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol type</th>
<th>Maximum event rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Security Event Log</td>
<td>WMI/DCOM</td>
<td>50EPS / Windows host</td>
</tr>
<tr>
<td>Microsoft Security Event Log over MSRPC</td>
<td>MSRPC</td>
<td>100EPS / Windows host</td>
</tr>
</tbody>
</table>
MQ protocol configuration options

To receive messages from a message queue (MQ) service, configure a log source to use the MQ protocol. The protocol name appears in IBM QRadar as MQ JMS.

IBM MQ is supported.

The MQ protocol is an inbound/passive protocol that can monitor multiple message queues, up to a maximum of 50 per log source.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Name</td>
<td>MQ JMS</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name of the primary queue manager.</td>
</tr>
<tr>
<td>Port</td>
<td>The default port that is used for communicating with the primary queue manager is 1414.</td>
</tr>
<tr>
<td>Standby IP or Hostname</td>
<td>The IP address or host name of the standby queue manager.</td>
</tr>
<tr>
<td>Standby Port</td>
<td>The port that is used to communicate with the standby queue manager.</td>
</tr>
<tr>
<td>Queue Manager</td>
<td>The name of the queue manager.</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel through which the queue manager sends messages. The default channel is SYSTEM.DEF.SVRCONN.</td>
</tr>
<tr>
<td>Queue</td>
<td>The queue or list of queues to monitor. A list of queues is specified with a comma-separated list.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name that is used for authenticating with the MQ service.</td>
</tr>
<tr>
<td>Password</td>
<td>Optional: The password that is used to authenticate with the MQ service.</td>
</tr>
<tr>
<td>Incoming Message Encoding</td>
<td>The character encoding that is used by incoming messages.</td>
</tr>
<tr>
<td>Process Computational Fields</td>
<td>Select this option if the retrieved messages contain computational data. The binary data in the messages will be processed according to the field definition found in the specified CopyBook file.</td>
</tr>
<tr>
<td>CopyBook File Name</td>
<td>The name of the CopyBook file to use for processing data. The CopyBook file must be placed in /store/ec/mqjms/*</td>
</tr>
<tr>
<td>Event Formatter</td>
<td>Select the event formatting to be applied for any events that are generated from processing data containing computational fields. By default, No Formatting is used.</td>
</tr>
<tr>
<td>Include JMS Message Header</td>
<td>Select this option to include a header in each generated event containing JMS message fields such as the JMSMessageID and JMSTimestamp.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The upper limit for the maximum number of events per second (EPS).</td>
</tr>
</tbody>
</table>

Related concepts
“Creating a log source extensions document to get data into QRadar” on page 125
You create log source extensions (LSX) when log sources don’t have a supported DSM, or to repair an
event that has missing or incorrect information, or to parse an event when the associated DSM fails to
produce a result.

Related tasks
“Building a Universal DSM ” on page 107
The first step in building a Universal DSM is to create the log source in IBM QRadar. When you create the
log source, it prevents the logs from being automatically classified and you can export the logs for review.

Okta REST API protocol configuration options

To receive events from Okta, configure a log source to use the Okta REST API protocol.

The Okta REST API protocol is an outbound/active protocol that queries the Okta Events and Users API endpoints to retrieve information about actions that are completed by users in an organization.

The following table describes the protocol-specific parameters for the Okta REST API protocol:

<table>
<thead>
<tr>
<th>Table 47. Okta REST API protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>IP or Hostname</td>
</tr>
<tr>
<td>Authentication Token</td>
</tr>
<tr>
<td>Use Proxy</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
</tr>
<tr>
<td>Recurrence</td>
</tr>
<tr>
<td>EPS Throttle</td>
</tr>
</tbody>
</table>

OPSEC/LEA protocol configuration options

To receive events on port 18184, configure a log source to use the OPSEC/LEA protocol.

The OPSEC/LEA protocol is an outbound/active protocol.

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

<table>
<thead>
<tr>
<th>Table 48. OPSEC/LEA protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Server IP</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td><strong>Server Port</strong></td>
</tr>
<tr>
<td><strong>Use Server IP for Log Source</strong></td>
</tr>
<tr>
<td><strong>Statistics Report Interval</strong></td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
</tr>
<tr>
<td><strong>OPSEC Application Object SIC Attribute (SIC Name)</strong></td>
</tr>
<tr>
<td><strong>Log Source SIC Attribute (Entity SIC Name)</strong></td>
</tr>
<tr>
<td><strong>Specify Certificate</strong></td>
</tr>
<tr>
<td><strong>Certificate Filename</strong></td>
</tr>
<tr>
<td><strong>Certificate Authority IP</strong></td>
</tr>
<tr>
<td><strong>Pull Certificate Password</strong></td>
</tr>
<tr>
<td><strong>OPSEC Application</strong></td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Table 48. OPSEC/LEA protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store Event Payload</td>
<td>Select the Store Event Payload check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Store Event Payload list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

**Important:** If you receive the error message **Unable to pull SSL certificate** after an upgrade, follow these steps:

1. Clear the Specify Certificate check box.
2. Reenter the password for Pull Certificate Password.

---

**Oracle Database Listener protocol configuration options**

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

The Oracle Database Listener protocol is an outbound/active protocol.

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

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

Table 49. Oracle Database Listener protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td><strong>Oracle Database Listener</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address, host name, or name to identify your log source.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IP address or host name of your Oracle Database Listener server.</td>
</tr>
<tr>
<td>Domain</td>
<td>Type the domain for your Oracle Database Learner server. This parameter is optional if your server is not in a domain.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name that is required to access your server.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password that is required to access your server.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password that is required to access the server.</td>
</tr>
<tr>
<td>Log Folder Path</td>
<td>Type the directory path to access the Oracle Database Listener log files.</td>
</tr>
<tr>
<td>File Pattern</td>
<td>The regular expression (regex) that identifies the event logs.</td>
</tr>
</tbody>
</table>
### Table 49. Oracle Database Listener protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force File Read</td>
<td>Select this check box to force the protocol to read the log file when the timing of the polling interval specifies. When the check box is selected, the log file source is always examined when the polling interval specifies, regardless of the last modified time or file size attribute. When the check box is not selected, the log file source is examined at the polling interval if the last modified time or file size attributes changed.</td>
</tr>
<tr>
<td>Recursive</td>
<td>If you want the file pattern to search sub folders, use this option. By default, the check box is selected.</td>
</tr>
</tbody>
</table>
| SMB Version        | The version of SMB to use: AUTO  
|                    |  
|                    | Auto-detects to the highest version that the client and server agree to use.  
|                    | SMB1  
|                    | Forces the use of SMB1.  
|                    | SMB2  
|                    | Forces the use of SMB2.  |
| Polling Interval (in seconds) | Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds. |
| Throttle events/sec | The maximum number of events the Oracle Database Listener protocol forwards per second.                                                      |
| File Encoding      | The character encoding that is used by the events in your log file.                                                                           |

### PCAP Syslog Combination protocol configuration options

To collect events from Juniper SRX Series Services Gateway or Juniper Junos OS Platform that forward packet capture (PCAP) data, configure a log source to use the PCAP Syslog Combination protocol.

The PCAP Syslog Combination protocol is an inbound/passive protocol.

Before you configure a log source that uses the PCAP Syslog Combination protocol, determine the outgoing PCAP port that is configured on the Juniper SRX Series Services Gateway or Juniper Junos OS Platform. PCAP data cannot be forwarded to port 514.

**Note:**

QRadar supports receiving PCAP data only from Juniper SRX Series Services Gateway or Juniper Junos OS Platform for each event collector.

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

### Table 50. PCAP Syslog Combination protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name of the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Optional. Type a description for the log source.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>From the list, you can select either Juniper SRX Series Services Gateway or Juniper Junos OS Platform.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>From the list, select PCAP Syslog Combination.</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type an IP address, host name, or name to identify the Juniper SRX Series Services Gateway or Juniper Junos OS Platform appliance. The log source identifier must be unique for the log source type.</td>
</tr>
<tr>
<td>Incoming PCAP Port</td>
<td>If the outgoing PCAP port is edited on the Juniper SRX Series Services Gateway or Juniper Junos OS Platform appliance, you must edit the log source to update the incoming PCAP Port. To edit the Incoming PCAP Port number, complete the following steps:  1. Type the new port number for receiving PCAP data  2. Click Save. The port update is complete and event collection starts on the new port number.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the log source. When this check box is clear, the log source does not collect events and the log source is not counted in the license limit.</td>
</tr>
<tr>
<td>Credibility</td>
<td>Select the credibility of the log source. The range is 0 (lowest) - 10 (highest). The default credibility is 5. 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.</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>Select the target for the log source. When a log source actively collects events from a remote source, this field defines which appliance polls for the events. This option enables administrators to poll and process events on the target event collector, instead of the Console appliance. This can improve performance in distributed deployments.</td>
</tr>
</tbody>
</table>
### Table 50. PCAP Syslog Combination protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coalescing Events</td>
<td>Select this check box to enable the log source to coalesce (bundle) events. Coalescing events increase the event count when the same event occurs multiple times within a short time interval. Coalesced events provide administrators 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, the events are displayed individually and the information is not bundled. New and automatically discovered log sources inherit the value of this check box from the System Settings configuration on the Admin tab. Administrators can use this check box to override the default behavior of the system settings for an individual log source.</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>Select this check box to enable the log source to store the payload information from an event. New and automatically discovered log sources inherit the value of this check box from the System Settings configuration on the Admin tab. Administrators can use this check box to override the default behavior of the system settings for an individual log source.</td>
</tr>
<tr>
<td>Log Source Extension</td>
<td>Optional. Select the name of the extension to apply to the log source. This parameter is available after a log source extension is uploaded. Log source extensions are XML files that contain regular expressions, which can override or repair the event parsing patterns that are defined by a device support module (DSM).</td>
</tr>
<tr>
<td>Extension Use Condition</td>
<td>From the list box, select the use condition for the log source extension. The options include: • Parsing enhancement - Select this option when most fields parse correctly for your log source. • Parsing override - Select this option when the log source is unable to correctly parse events.</td>
</tr>
<tr>
<td>Groups</td>
<td>Select one or more groups for the log source.</td>
</tr>
</tbody>
</table>

### SDEE protocol configuration options

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

The SDEE protocol is an outbound/active protocol.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>SDEE</td>
</tr>
</tbody>
</table>
### Table 51. SDEE protocol parameters (continued)

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

### SMB Tail protocol configuration options

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

The SMB Tail protocol is an outbound/active protocol.

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

### Table 52. SMB Tail protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol Configuration</strong></td>
<td>SMB Tail</td>
</tr>
<tr>
<td><strong>Server Address</strong></td>
<td>The IP address or host name of your SMB Tail server.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Type the domain for your SMB Tail server. This parameter is optional if your server is not in a domain.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Type the user name that is required to access your server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Type the password that is required to access your server.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>Confirm the password that is required to access the server.</td>
</tr>
<tr>
<td><strong>Log Folder Path</strong></td>
<td>The directory path to access the log files. For example, administrators can use the $c$/LogFiles/ directory for an administrative share, or the LogFiles/ directory for a public share folder path. However, the c:/LogFiles directory is not a supported log folder path. If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the privileges that are required to read the log files. Local system or domain administrator privileges are also sufficient to access a log files that are on an administrative share.</td>
</tr>
<tr>
<td><strong>File Pattern</strong></td>
<td>The regular expression (regex) that identifies the event logs.</td>
</tr>
</tbody>
</table>
## Table 52. SMB Tail protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB Version</td>
<td>The version of SMB to use:</td>
</tr>
<tr>
<td>AUTO</td>
<td>Auto-detects to the highest version that the client and server agree to use.</td>
</tr>
<tr>
<td>SMB1</td>
<td>Forces the use of SMB1.</td>
</tr>
<tr>
<td>SMB2</td>
<td>Forces the use of SMB2.</td>
</tr>
<tr>
<td>Force File Read</td>
<td>If the check box is cleared, the log file is read only when QRadar detects a change in the modified time or file size.</td>
</tr>
<tr>
<td>Recursive</td>
<td>If you want the file pattern to search sub folders, use this option. By default, the check box is selected.</td>
</tr>
<tr>
<td>Polling Interval (In seconds)</td>
<td>Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds.</td>
</tr>
<tr>
<td>Throttle Events/Second</td>
<td>The maximum number of events the SMB Tail protocol forwards per second.</td>
</tr>
<tr>
<td>File Encoding</td>
<td>The character encoding that is used by the events in your log file.</td>
</tr>
</tbody>
</table>

## SNMPv2 protocol configuration options

You can configure a log source to use the SNMPv2 protocol to receive SNMPv2 events. The SNMPv2 protocol is an inbound/passive protocol. The following table describes the protocol-specific parameters for the SNMPv2 protocol:

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

## SNMPv3 protocol configuration options

You can configure a log source to use the SNMPv3 protocol to receive SNMPv3 events. The SNMPv3 protocol is an inbound/passive protocol. The following table describes the protocol-specific parameters for the SNMPv3 protocol:
Table 54. SNMPv3 protocol parameters

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

Seculert Protection REST API protocol configuration options

To receive events from Seculert, configure a log source to use the Seculert Protection REST API protocol. The Seculert Protection REST API protocol is an outbound/active protocol. Seculert Protection provides alerts on confirmed incidents of malware that are actively communicating or exfiltrating information.

Before you can configure a log source for Seculert, you must obtain your API key from the Seculert web portal.

1. Log in to the Seculert web portal.
2. On the dashboard, click the API tab.
3. Copy the value for Your API Key.

The following table describes the protocol-specific parameters for the Seculert Protection REST API protocol:

Table 55. Seculert Protection REST API protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td><strong>Seculert</strong></td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td><strong>Seculert Protection REST API</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from Seculert. Each additional log source that you create when you have multiple installations ideally includes a unique identifier, such as an IP address or host name.</td>
</tr>
<tr>
<td>API Key</td>
<td>The API key that is used for authenticating with the Seculert Protection REST API. The API key value is obtained from the Seculert web portal.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>When you configure a proxy, all traffic for the log source travels through the proxy for QRadar to access the Seculert Protection REST API. Configure the Proxy IP or Hostname, 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.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>If you select Yes form the list, QRadar downloads the certificate and begins trusting the target server.</td>
</tr>
</tbody>
</table>
Table 55. Seculert Protection REST API protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurrence</td>
<td>Specify when the log collects data. The format is M/H/D for Months/Hours/Days. The default is 1 M.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The upper limit for the maximum number of events per second (eps) for events that are received from the API.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the log source. By default, the check box is selected.</td>
</tr>
<tr>
<td>Credibility</td>
<td>Select the Credibility of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>Select the Target Event Collector to use as the target for the log source.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the Coalescing Events list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Store Event Payload list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

**Sophos Enterprise Console JDBC protocol configuration options**

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

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

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

Table 56. Sophos Enterprise Console JDBC protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Sophos Enterprise Console JDBC</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>MSDE</td>
</tr>
<tr>
<td>Database Name</td>
<td>The database name must match the database name that is specified in the Log Source Identifier field.</td>
</tr>
<tr>
<td>Port</td>
<td>The default port for MSDE in Sophos Enterprise Console is 1168. The JDBC configuration port must match the listener port of the Sophos database to communicate with QRadar. The Sophos database must have incoming TCP connections enabled. If a Database Instance is used with the MSDE database type, you must leave the Port parameter blank.</td>
</tr>
<tr>
<td>Authentication Domain</td>
<td>If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or administrators block access to port 1434 for SQL database resolution, the Database Instance parameter must be blank.</td>
</tr>
<tr>
<td>Table Name</td>
<td>vEventsCommonData</td>
</tr>
<tr>
<td>Select List</td>
<td>*</td>
</tr>
<tr>
<td>Compare Field</td>
<td>InsertedAt</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Prepared statements enable the protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most configurations can use prepared statements. Clear this check box to use an alternative method of querying that do not use pre-compiled statements.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>Optional. A start date and time for when the protocol can start to poll the database. If a start time is not defined, the protocol attempts to poll for events after the log source configuration is saved and deployed.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>The polling interval, which is the amount of time between queries to the database. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.</td>
</tr>
</tbody>
</table>
**Table 56. Sophos Enterprise Console JDBC protocol parameters (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPS Throttle</td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed.</td>
</tr>
<tr>
<td>Use Named Pipe Communication</td>
<td>If MSDE is configured as the database type, administrators can select this check box to use an alternative method to a TCP/IP port connection.</td>
</tr>
<tr>
<td></td>
<td>Named pipe connections for MSDE databases require the user name and password field to use a Windows authentication username and password and not the database user name and password. The log source configuration must use the default named pipe on the MSDE database.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>If you use your SQL server in a cluster environment, define the cluster name to ensure that named pipe communications function properly.</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>Forces MSDE connections to use the NTLMv2 protocol with SQL servers that require NTLMv2 authentication. The default value of the check box is selected.</td>
</tr>
<tr>
<td></td>
<td>The Use NTLMv2 check box does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
</tbody>
</table>

---

**Sourcefire Defense Center eStreamer protocol options**

Sourcefire Defense Center eStreamer protocol is now known as Cisco Firepower eStreamer protocol.

**Syslog Redirect protocol overview**

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

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

**Table 57. Syslog Redirect protocol parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Syslog Redirect</td>
</tr>
<tr>
<td>Log Source Identifier Regex</td>
<td>devname=(\w+)</td>
</tr>
<tr>
<td>Log Source Identifier Regex Format String</td>
<td>Type the syslog header host name in the Log Source Name field. You can use capture groups to substitute the syslog header host name. Specify the capture group substitution by using \x where x is a group number that contains a regular expression (regex). You can use multiple capture groups. For example, if the payload source name is hostname=(.*) and the regex in capture group 1 is ibm, type \1.hostname.com to customize the payload to the following host name: ibm.hostname.com</td>
</tr>
</tbody>
</table>
### Table 57. Syslog Redirect protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform DNS Lookup On Regex Match</td>
<td>Select the Perform DNS Lookup On Regex Match check box to enable DNS functionality, which is based on the Log Source Identifier parameter value. By default, the check box is not selected.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>517</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
</tr>
</tbody>
</table>

## TCP multiline syslog protocol configuration options

You can configure a log source that uses the TCP multiline syslog protocol. The TCP multiline syslog protocol is an inbound/passive protocol that uses regular expressions to identify the start and end pattern of multiline events.

The following example is a multiline event:

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

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

### Table 58. TCP multiline syslog protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>TCP Multiline Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type an IP address or host name to identify the log source. To use a name instead, select Use Custom Source Name and fill in the Source Name Regex and Source Name Formatting String parameters. Note: These parameters are only available if Show Advanced Options is set to Yes.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The default port is 12468.</td>
</tr>
<tr>
<td>Aggregation Method</td>
<td>The default is Start/End Matching. Use ID-Linked if you want to combine multiline events that are joined by a common identifier.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Event Start Pattern</strong></td>
<td>This parameter is available when you set the Aggregation Method parameter to <strong>Start/End Matching</strong>. The regular expression (regex) that is required to identify the start of a TCP multiline event payload. Syslog headers typically begin with a date or time stamp. The protocol can create a single-line event that is based on solely on an event start pattern, such as a time stamp. When only a start pattern is available, the protocol captures all the information between each start value to create a valid event.</td>
</tr>
<tr>
<td><strong>Event End Pattern</strong></td>
<td>This parameter is available when you set the Aggregation Method parameter to <strong>Start/End Matching</strong>. This regular expression (regex) that is required to identify the end of a TCP multiline event payload. If the syslog event ends with the same value, you can use a regular expression to determine the end of an event. The protocol can capture events that are based on solely on an event end pattern. When only an end pattern is available, the protocol captures all the information between each end value to create a valid event.</td>
</tr>
<tr>
<td><strong>Message ID Pattern</strong></td>
<td>This parameter is available when you set the <strong>Aggregation Method</strong> parameter to <strong>ID-Linked</strong>. This regular expression (regex) required to filter the event payload messages. The TCP multiline event messages must contain a common identifying value that repeats on each line of the event message.</td>
</tr>
<tr>
<td><strong>Event Formatter</strong></td>
<td>Use the <strong>Windows Multiline</strong> option for multiline events that are formatted specifically for Windows.</td>
</tr>
<tr>
<td><strong>Show Advanced Options</strong></td>
<td>The default is <strong>No</strong>. Select <strong>Yes</strong> if you want to customize the event data.</td>
</tr>
<tr>
<td><strong>Use Custom Source Name</strong></td>
<td>This parameter is available when you set <strong>Show Advanced Options</strong> to <strong>Yes</strong>. Select the check box if you want to customize the source name with regex.</td>
</tr>
<tr>
<td><strong>Source Name Regex</strong></td>
<td>This parameter is available when you check <strong>Use Custom Source Name</strong>. The regular expression (regex) that captures one or more values from event payloads that are handled by this protocol. These values are used along with the <strong>Source Name Formatting String</strong> parameter to set a source or origin value for each event. This source value is used to route the event to a log source with a matching Log Source Identifier value.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Source Name Formatting String** | This parameter is available when you check **Use Custom Source Name**. You can use a combination of one or more of the following inputs to form a source value for event payloads that are processed by this protocol:  
- One or more capture groups from the **Source Name Regex**. To refer to a capture group, use `\x` notation where `x` is the index of a capture group from the **Source Name Regex**.  
- The IP address where the event data originated from. To refer to the packet IP, use the token `$PIP$`.  
- Literal text characters. The entire **Source Name Formatting String** can be user-provided text. For example, if the **Source Name Regex** is `hostname=(.*?)` and you want to append `hostname.com` to the capture group 1 value, set the **Source Name Formatting String** to `\1.hostname.com`. If an event is processed that contains `hostname=ibm`, then the event payload's source value is set to `ibm.hostname.com`, and QRadar routes the event to a log source with that **Log Source Identifier**. |
| **Use as a Gateway Log Source** | This parameter is available when you set **Show Advanced Options** to **Yes**.  
When selected, events that flow through the log source can be routed to other log sources, based on the source name tagged on the events.  
When this option is not selected and **Use Custom Source Name** is not checked, incoming events are tagged with a source name that corresponds to the Log Source Identifier parameter. |
| **Flatten Multiline Events into Single Line** | This parameter is available when you set **Show Advanced Options** to **Yes**.  
Shows an event in one single line or multiple lines. |
| **Retain Entire Lines during Event Aggregation** | This parameter is available when you set **Show Advanced Options** to **Yes**.  
If you set the **Aggregation Method** parameter to **ID-Linked**, you can enable **Retain Entire Lines during Event Aggregation** to either discard or keep the part of the events that comes before **Message ID Pattern** when concatenating events with the same ID pattern together. |
| **Time Limit** | The number of seconds to wait for additional matching payloads before the event is pushed into the event pipeline. The default is 10 seconds. |
| **Enabled** | Select this check box to enable the log source. |
Table 58. TCP multiline syslog protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credibility</td>
<td>Select the credibility of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>Select the Event Collector in your deployment that should host the TCP Multiline Syslog listener.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the Coalescing Events list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Store Event Payload list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

TCP Multiline Syslog protocol configuration use cases

To set the TCP Multiline Syslog listener log source to collect all events that are sent from the same system, follow these steps:

1. Leave **Use As A Gateway Log Source** and **Use Custom Source Name** cleared.
2. Enter the IP address of the system that is sending events in the **Log Source Identifier** parameter.

![QRadar log source collects events sent from a single system to a TCP Multiline Syslog Listener](image)

Figure 1. A QRadar log source collects events sent from a single system to a TCP Multiline Syslog Listener

If multiple systems are sending events to the TCP Multiline Syslog listener, or if one intermediary system is forwarding events from multiple systems and you want the events to be routed to separate log sources based on their syslog header or IP address, check the **Use As A Gateway Log Source** check box.

**Note:** QRadar checks each event for an RFC3164 or RFC5424-compliant syslog header, and if present, uses the IP/hostname from that header as the source value for the event. The event is routed to a log source with that same IP or host name as its Log Source Identifier. If no such header is present, QRadar
uses the source IP value from the network packet that the event arrived on as the source value for the event.

**Figure 2.** Separate QRadar log sources collect events sent from multiple systems to a TCP Multiline Listener, by using the syslog header.

To route events to separate log sources based on a value other than the IP or host name in their syslog header, follow these steps:

1. Check the **Use Custom Source Name** check box.
2. Configure a **Source Name Regex** and **Source Name Formatting String** to customize how QRadar sets a source name value for routing the received events to log sources.

**Figure 3.** Separate QRadar log sources collect events sent from multiple systems and forwarded via an intermediate system to a TCP Multiline Listener, by using the syslog header.

**Figure 4.** Separate QRadar log sources collect events sent from multiple systems and forwarded through an intermediate system to a TCP Multiline Listener, by using the Source Name Regex and Source Name Formatting String.
TLS syslog protocol configuration options

Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

The TLS syslog protocol is an inbound/passive protocol. The log source creates a listen port for incoming TLS Syslog events and generates a certificate file for the network devices. Up to 50 network appliances can forward events to the listen port that is created for the log source. If you create more log sources with unique listen ports, you can configure up to 1000 network appliances.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>TLS Syslog</td>
</tr>
<tr>
<td>TLS Listen Port</td>
<td>The default TLS listen port is 6514.</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>The mode by which your TLS connection is authenticated. If you select the <strong>TLS and Client Authentication</strong> option, you must configure the certificate parameters.</td>
</tr>
<tr>
<td>Client Certificate Path</td>
<td>The absolute path to the client-certificate on disk. The certificate must be stored on the QRadar Console or Event Collector for this log source.</td>
</tr>
</tbody>
</table>
### Table 59. TLS syslog protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Type</td>
<td>The type of certificate to use for authentication for the server certificate and server key. Select one of the following Certificate Type parameter options:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certificate Type Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generated Certificate</td>
<td>If you want to use the default certificate and key that is generated by QRadar for the server certificate and server key, select this option.</td>
</tr>
<tr>
<td>Single Certificate and Private Key</td>
<td>If you want to use a single PEM certificate for the server certificate, select this option and then configure the following parameters:</td>
</tr>
<tr>
<td></td>
<td>• Provided Server Certificate Path - The absolute path to the server certificate.</td>
</tr>
<tr>
<td></td>
<td>• Provided Private Key Path - The absolute path to the private key.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The corresponding private key must be a DER-encoded PKCS8 key. The configuration fails with any other key format.</td>
</tr>
<tr>
<td>PKCS12 Certificate and Password</td>
<td>If you want to use a PKCS12 file that contains the server certificate and server key, select this option and then configure the following parameters:</td>
</tr>
<tr>
<td></td>
<td>• PKCS12 Certificate Path - Type the file path for the PKCS12 file that contains the server certificate and server key.</td>
</tr>
<tr>
<td></td>
<td>• PKCS12 Password - Type the password to access the PKCS12 file.</td>
</tr>
<tr>
<td></td>
<td>• Certificate Alias - If there is more than one entry in the PKCS12 file, an alias must be provided to specify which entry to use. If there is only one alias in the PKCS12 file, leave this field blank.</td>
</tr>
</tbody>
</table>
Table 59. TLS syslog protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Payload Length</td>
<td>The maximum payload length (characters) that is displayed for TLS Syslog message.</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>The Maximum Connections parameter controls how many simultaneous connections the TLS Syslog protocol can accept for each Event Collector. There is a limit of 1000 connections across all TLS syslog log source configurations for each Event Collector. The default for each device connection is 50. Note: Automatically discovered log sources that share a listener with another log source, such as if you use the same port on the same event collector, count only one time towards the limit.</td>
</tr>
</tbody>
</table>
| TLS Protocols      | The TLS Protocol to be used by the log source. Select one of the following options:  
• TLS 1.2 and above  
• TLS 1.1 and above  
• TLS 1.0 and above |

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

**TLS syslog use cases**

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

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

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

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

**Configuring multiple log sources over TLS syslog**
You can configure multiple devices in your network to send encrypted Syslog events to a single TLS Syslog listen port. The TLS Syslog listener acts as a gateway, decrypts the event data, and feeds it within QRadar to extra log sources configured with the Syslog protocol.

**Before you begin**

Ensure that the TLS Syslog log source is configured.

**Note:** You can use any placeholder for the Log Source Identifier and Log Source Type to identify the TLS Syslog log source. The TLS Syslog log source is configured to host the TLS Syslog listener and acts as a gateway.
About this task

Multiple devices within your network that support TLS-encrypted Syslog can send encrypted events via a TCP connection to the TLS Syslog listen port. These encrypted events are decrypted by the TLS Syslog (gateway) and are fired into the event pipeline. The decrypted events get routed to the appropriate receiver log sources or to the traffic analysis engine for autodiscovery.

Events are routed within QRadar to log sources with a Log Source Identifier value that matches the source value of an event. For Syslog events with an RFC3164- or RFC5424-compliant Syslog header, the source value is the IP address or the host name from the header. For events that do not have a compliant header, the source value is the IP address of the device that sent the Syslog event.

On QRadar, you can configure multiple log sources with the Syslog protocol to receive encrypted events that are sent to a single TLS Syslog listen port from multiple devices.

Note: Most TLS-enabled clients require the target server or listener's public certificate to authenticate the server's connection. By default, a TLS Syslog log source generates a certificate that is named syslog-tls.cert in /opt/qradar/conf/trusted_certificates/ on the target Event Collector that the log source is assigned to. This certificate file must be copied to all clients that are making a TLS connection.

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. Click Log Sources > Add.
4. From the Protocol Configuration list, select TLS Syslog.
5. Configure the log source device to use the TLS Syslog port to send events to QRadar.
6. Repeat steps 3-5 for each log source that receives events through the gateway TLS listener.

Note: You can also add multiple receiver log sources in bulk by clicking Bulk Actions > Bulk Add from the Log Sources window.

Related concepts

“TLS syslog protocol configuration options” on page 93
Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

UDP multiline syslog protocol configuration options

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

The UDP multiline syslog protocol is an inbound/passive protocol. The original multiline event must contain a value that repeats on each line in order for a regular expression to capture that value and identify the individual syslog messages that make up the multiline event. For example, this multiline event contains a repeated value, 2467222, in the conn field. This field value is captured so that all syslog messages that contain conn=2467222 are combined into a single event.

```
15:08:56 <IP_address> slapd[517]: conn=2467222 op=2 SEARCH RESULT tag=101
15:08:56 <IP_address> slapd[517]: conn=2467222 op=2 SRCH base="dc=xxx"
15:08:56 <IP_address> slapd[517]: conn=2467222 op=2 SRCH attr=gidNumber
15:08:56 <IP_address> slapd[517]: conn=2467222 op=1 SRCH base="dc=xxx"
```

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>UDP Multiline Syslog</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The default port number that is used by QRadar to accept incoming UDP Multiline Syslog events is 517. You can use a different port in the range 1 - 65535. To edit a saved configuration to use a new port number, complete the following steps: 1. In the Listen Port field, type the new port number for receiving UDP Multiline Syslog events. 2. Click Save. 3. Click Deploy Changes to make this change effective. The port update is complete and event collection starts on the new port number.</td>
</tr>
<tr>
<td>Message ID Pattern</td>
<td>The regular expression (regex) required to filter the event payload messages. The UDP multiline event messages must contain a common identifying value that repeats on each line of the event message.</td>
</tr>
<tr>
<td>Event Formatter</td>
<td>The event formatter that formats incoming payloads that are detected by the listener. Select No Formatting to leave the payload untouched. Select Cisco ACS Multiline to format the payload into a single-line event. In ACS syslog header, there are total_seg and seg_num fields. These two fields are used to rearrange ACS multiline events into a single-line event with correct order when you select the Cisco ACS Multiline option.</td>
</tr>
<tr>
<td>Show Advanced Options</td>
<td>The default is No. Select Yes if you want to configure advanced options.</td>
</tr>
<tr>
<td>Use Custom Source Name</td>
<td>Select the check box if you want to customize the source name with regex.</td>
</tr>
<tr>
<td>Source Name Regex</td>
<td>Use the Source Name Regex and Source Name Formatting String parameters if you want to customize how QRadar determines the source of the events that are processed by this UDP Multiline Syslog configuration. For Source Name Regex, enter a regex to capture one or more identifying values from event payloads that are handled by this protocol. These values are used with the Source Name Formatting String to set a source or origin value for each event. This source value is used to route the event to a log source with a matching Log Source Identifier value when the Use As A Gateway Log Source option is enabled.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Source Name Formatting String**                  | You can use a combination of one or more of the following inputs to form a source value for event payloads that are processed by this protocol:  
  • One or more capture groups from the **Source Name Regex**. To refer to a capture group, use \x notation where x is the index of a capture group from the **Source Name Regex**.  
  • The IP address from which the event data originated. To refer to the packet IP, use the token $PIP$.  
  • Literal text characters. The entire **Source Name Formatting String** can be user-provided text.  
  For example, CiscoACS\1\2$PIP$, where \1\2 means first and second capture groups from the **Source Name Regex** value, and $PIP$ is the packet IP. |
| **Use As A Gateway Log Source**                    | If this check box is clear, incoming events are sent to the log source with the **Log Source Identifier** matching the IP that they originated from.  
  When checked, this log source serves as a single entry point or gateway for multiline events from many sources to enter QRadar and be processed in the same way, without the need to configure a UDP Multiline Syslog log source for each source. Events with an RFC3164- or RFC5424-compliant syslog header are identified as originating from the IP or host name in their header, unless the **Source Name Formatting String** parameter is in use, in which case that format string is evaluated for each event. Any such events are routed through QRadar based on this captured value.  
  If one or more log sources exist with a corresponding **Log Source Identifier**, they are given the event based on configured Parsing Order. If they do not accept the event, or if no log sources exist with a matching **Log Source Identifier**, the events are analyzed for autodetection. |
| **Flatten Multiline Events Into Single Line**      | Shows an event in one single line or multiple lines. If this check box is selected, all newline and carriage return characters are removed from the event.                                                                                                                                                                                                                                                                                                                                 |
| **Retain Entire Lines During Event Aggregation**   | Choose this option to either discard or keep the part of the events that comes before **Message ID Pattern** when the protocol concatenates events with same ID pattern together.                                                                                                                                                                                                                                                                                      |
| **Time Limit**                                     | The number of seconds to wait for additional matching payloads before the event is pushed into the event pipeline. The default is 10 seconds.                                                                                                                                                                                                                                                                                              |
| **Enabled**                                        | Select this check box to enable the log source.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
Table 61. UDP multiline syslog protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credibility</strong></td>
<td>Select the credibility of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
<td>Select the Event Collector in your deployment that should host the UDP Multiline Syslog listener.</td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
<td>Select this check box to enable the log source to coalesce (bundle) events.</td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
<td>Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Coalescing Events list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

**Configuring UDP multiline syslog for Cisco ACS appliances**

The Cisco ACS DSM for IBM Security QRadar accepts syslog events from Cisco ACS appliances with log sources that are configured to use the UDP Multiline Syslog protocol.

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the Data Sources section, click the **Log Sources** icon, and then click **Add**.
4. In the **Log Source Name** field, type a name for your log source.
5. From the **Log Source Type** list, select **Cisco ACS**.
6. From the **Protocol Configuration** list, select **UDP Multiline Syslog**.
7. Configure the parameters:

   The following parameters require specific values to collect events from Cisco ACS appliances:

   Table 62. Cisco ACS log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type the IP address, host name, or name to identify your Cisco ACS appliance.</td>
</tr>
</tbody>
</table>
Table 62. Cisco ACS log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen Port</td>
<td>The default port number that is used by QRadar to accept incoming UDP Multiline Syslog events is 517. You can use a different port. The valid port range is 1 - 65535. To edit a saved configuration to use a new port number, complete the following steps. a. In the <strong>Listen Port</strong> field, type the new port number for receiving UDP Multiline Syslog events. b. Click <strong>Save</strong>. The port update is complete and event collection starts on the new port number.</td>
</tr>
<tr>
<td>Message ID Pattern</td>
<td>\s(\d{10})\s</td>
</tr>
<tr>
<td>Event Formatter</td>
<td>Select <strong>Cisco ACS Multiline</strong> from the list.</td>
</tr>
</tbody>
</table>

**Related concepts**

“UDP multiline syslog protocol configuration options” on page 96

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

**VMware vCloud Director protocol configuration options**

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

The VMware vCloud Director protocol is an outbound/active protocol.

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

Table 63. VMware vCloud Director protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td><strong>VMware vCloud Director</strong></td>
</tr>
<tr>
<td>vCloud URL</td>
<td>The URL that is configured on the VMware vCloud appliance to access the REST API. The URL must match the address that is configured as the VCD public REST API base URL on the vCloud Server, for example, <a href="https://192.0.2.1">https://192.0.2.1</a>.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name that is required to remotely access the vCloud Server, for example, console/user@organization. To configure a read-only account to use with the vCloud Director protocol, a user must have Console Access Only permission.</td>
</tr>
</tbody>
</table>
Chapter 8. Adding bulk log sources

You can add up to 500 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. On the Admin tab, click Log Sources.
2. From the Bulk Actions list, select Bulk Add.
3. In the Bulk Log Sources window, configure the parameters for the bulk log source.
4. Select the Enabled check box to enable the log source. By default, this check box is selected.
5. Select the Coalescing Events check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value that is configured in the Coalescing Events list in the System Settings window on the Admin tab. However, when you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar Administration Guide.
6. Select the Store Event Payload check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the Store Event Payload list in the System Settings window on the Admin tab. When you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar Administration Guide.
7. Upload the log sources by choosing one of the following methods:
   - File Upload - Upload a text file that has one host name or IP per line. The text file must contain one IP address or host name per line. Extra characters after an IP address or host names longer than 255 characters can result in a value being bypassed from the text file. The file upload lists a summary of all IP address or host names that were added as the bulk log source.
   - Manual - Enter the host name or IP of the host that you want to add.
8. Click Add > Save.
   Note: By default, a check box is selected for each log source in the host list. Clear the check box if you want the log source to be ignored. Duplicate host names or IP addresses are ignored.
9. Click Continue to add the log sources.
10. On the Admin tab, click Deploy Changes.
Chapter 9. Editing bulk log sources

You can edit log sources in bulk to update the configuration parameters for log sources that were added as part of a bulk log source. The **Log Source Type** and **Protocol Configuration** parameters cannot be edited in bulk.

**About this task**

The following table describes the default parameters for the log source configuration. These parameters might differ based on the **Log Source Type** selected:

**Procedure**

1. Click the **Admin** tab.
2. In the **Data Sources** section, click the **Log Sources** icon.
3. Select the log sources that you want to edit, and from the **Bulk Actions** list, select **Bulk Edit**.
4. Modify the relevant parameters.
5. The list of log sources is for display purposes only. The check boxes are only used during the workflow for adding log sources to QRadar.
6. Click **Save** to update your log source configuration.
7. Click **Continue** to add the log sources.
8. On the **Admin** tab, click **Deploy Changes** if you added an IP address or host name to your bulk log source.

**Results**

The bulk log source is updated.
Chapter 10. 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 11. Log source extensions

An extension document can extend or modify how the elements of a particular log source are parsed. You can use the extension document to correct a parsing issue or override the default parsing for an event from an existing DSM.

An extension document can also provide event support when a DSM does not exist to parse events for an appliance or security device in your network.

An extension document is an Extensible Markup Language (XML) formatted document that you can create or edit one by using any common text, code or markup editor. You can create multiple extension documents but a log source can have only one applied to it.

The XML format requires that all regular expression (regex) patterns be contained in character data (CDATA) sections to prevent the special characters that are required by regular expressions from interfering with the markup format. For example, the following code shows the regex for finding protocols:

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

(TCP | UDP | ICMP | GRE) is the regular expression pattern.

The log sources extension configuration consists of the following sections:

**Pattern**
Regular expressions patterns that you associate with a particular field name. Patterns are referenced multiple times within the log source extension file.

**Match groups**
An entity within a match group that is parsed, for example, EventName, and is paired with the appropriate pattern and group for parsing. Any number of match groups can appear in the extension document.

---

Building a Universal DSM

The first step in building a Universal DSM is to create the log source in IBM QRadar. When you create the log source, it prevents the logs from being automatically classified and you can export the logs for review.

**Procedure**

1. On the Admin tab, click the Log Sources icon.
2. Click Add.
3. Specify the name in the Log Source Name field.
4. From the Log Source Type list, select Universal DSM.
   
   You might not see the Log Source Extension unless you already applied a log source extension to the QRadar Console.
5. From the Protocol Configuration list, specify the protocol that you want to use.
   
   This method is used by QRadar to get the logs from the unsupported log source.
6. For the Log Source Identifier, enter either the IP address or host name of the unsupported log source.
7. Click Save to save the new log source and close the window.
8. From the Admin tab, click Deploy Changes.

**What to do next**

“Exporting the logs ” on page 108
Exporting the logs

Export the logs that are created after you build a Universal DSM.

About this task

Typically you want a significant number of logs for review. Depending on the EPS rate of the unsupported log source, it might take several hours to obtain a comprehensive log sample.

When QRadar can't detect the log source type, events are collected, but are not parsed. You can filter on these unparsed events and then review the last system notification that you received. After you reviewed the system notification, you can create a search that is based on that time frame.

Procedure

1. To look at only the events that are not parsed, filter the logs.
   a) Click the Log Activity tab.
   b) Click Add Filter.
   c) Select Event is Unparsed.
      Tip: Type inside the Parameter text box to see the Event is Unparsed item.
   d) Select a time frame.
   e) If you see Information events from system notifications, right-click to filter them out.
   f) Review the Source IP column to determine what device is sending the events.

You can view the raw event payloads. Typically, manufacturers put identifiable product names in the headers, so you can set your search to Display: Raw Events to show the payloads without having to manually open each event. Sorting by network can also help you find a specific device where the event originated from.

2. Create a search for exporting the logs.
   a) From the Log Activity tab, select Search > Edit Search.
   b) For the Time Range, specify as enough time, for example 6 hours, from when the log source was created.
   c) Under Search Parameters, from the Parameter list, select Log Source (Indexed), from the Operator list, select Equals, and from the Log Source Group list, select Other, specify the log source that was created when you built the Universal DSM.

   ![Search Parameters](image)

   Note: Depending on your settings, you might see Log Source in the Parameter list instead of Log Source (Indexed).
   d) Click Search to view the results.

3. Review the results in the console to check the payload.

4. Optionally, you can export the results by clicking select Actions > Export to XML > Full Export (All Columns).
   Don't select Export to CSV because the payload might be split across multiple columns, therefore making it difficult to find the payload. XML is the preferred format for event reviews.
a) You are prompted to download a compressed file. Open the compressed file and then open the resulting file.

b) Review the logs.

   Event payloads are between the following tags:
   
   ```
   <payloadAsUTF>
   ... 
   </payloadAsUTF>
   ```

   The following code shows an example payload:
   
   ```
   <payloadAsUTF>ecs-ep (pid 4162 4163 4164) is running... </payloadAsUTF>
   ```

   A critical step in creating a Universal DSM is reviewing the logs for usability. At a minimum, the logs must have a value that can be mapped to an event name. The event name must be a unique value that can distinguish the various log types.

   The following code shows an example of usable logs:
   
   ```
   May 20 17:16:14 <server>[22331]: bad password attempt for 'root' from <IP_address>:3364
   May 20 17:16:26 <server>[22331]: password auth succeeded for 'root' from <IP_address>:3364
   May 20 16:42:19 kernel: DROP IN=vlan2 OUT=
   MAC=<MAC_address> SRC=<IP_address> DST=<IP_address> PROTO=UDP SPT=67 DPT=68
   ```

   The following codes shows an example of slightly less usable logs:
   
   ```
   Oct 26 08:12:08 loopback 1256559128 autotrace[215824]: W: trace: no map for prod 49420003, idf 010029a2, lal 00af0008
   Oct 26 16:35:00 <server> last message repeated 7 times
   Nov 24 01:30:00 <server> /usr/local/monitor-rrd/<server>/.rrd (rc=-1, opening '/usr/local/monitor-rrd/<server>/.rrd':
   No such file or directory)
   ```

---

**Examples of log source extensions on QRadar forum**

You can create log source extensions (LSX) for log sources that don't have a supported DSM. To help you create your own log source extensions (also known as DSM extensions), you modify existing ones that were created.


The IBM QRadar forums is an online discussion site where users and subject matter experts collaborate and share information.

**Related concepts**

[Creating a log source extensions document to get data into QRadar](https://www.ibm.com/developerworks/community/forums/html/topic?id=d15cac8d-b0fa-4461-bb1e-dc1b291de440&ps=25)
You create log source extensions (LSX) when log sources don’t have a supported DSM, or to repair an event that has missing or incorrect information, or to parse an event when the associated DSM fails to produce a result.

**Patterns in log source extension documents**

Rather than associating a regular expression directly with a particular field name, patterns (patterns) are declared separately at the top of the extension document. These regex patterns can be then referenced multiple times within the log source extension file.

All characters between the start tag `<pattern>` and end tag `</pattern>` are considered part of the pattern. Do not use extra spaces or hard returns inside or around your pattern or `<CDATA>` expression. Extra characters or spaces can prevent the DSM extension from matching your intended pattern.

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (Required)</td>
<td>String</td>
<td>A regular string that is unique within the extension document.</td>
</tr>
<tr>
<td>case-insensitive (Optional)</td>
<td>Boolean</td>
<td>If true, the character case is ignored. For example, abc is the same as ABC. If not specified, this parameter defaults to false.</td>
</tr>
<tr>
<td>trim-whitespace (Optional)</td>
<td>Boolean</td>
<td>If true, whitespace and carriage returns are ignored. If the CDATA sections are split onto different lines, any extra spaces and carriage returns are not interpreted as part of the pattern. If not specified, this parameter defaults to false.</td>
</tr>
<tr>
<td>use-default-pattern (Optional)</td>
<td>Boolean</td>
<td>If true, the system uses Java Patterns for the Log Source Extension, instead of the more effective Adaptive Patterns. Set this option to true if Adaptive Patterns are providing inconsistent matching. If not specified, this parameter defaults to false.</td>
</tr>
</tbody>
</table>

**Match groups**

A *match group* (match-group) is a set of patterns that are used for parsing or modifying one or more types of events.

A *matcher* is an entity within a match group that is parsed, for example, EventName, and is paired with the appropriate pattern and group for parsing. Any number of match groups can appear in the extension document.
### Table 65. Description of match group parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>order (Required)</td>
<td>An integer greater than zero that defines the order in which the match groups are executed. It must be unique within the extension document.</td>
</tr>
<tr>
<td>description (Optional)</td>
<td>A description for the match group, which can be any string. This information can appear in the logs. If not specified, this parameter defaults to empty.</td>
</tr>
<tr>
<td>device-type-id-override (Optional)</td>
<td>Define a different device ID to override the QID. Allows the particular match group to search in the specified device for the event type. It must be a valid log source type ID, represented as an integer. If not specified, this parameter defaults to the log source type of the log source to which the extension is attached.</td>
</tr>
</tbody>
</table>

Match groups can have these entities:

- “Matcher (matcher)” on page 111
- “Single-event modifier (event-match-single)” on page 122
- “Multi-event modifier (event-match-multiple)” on page 121

### Matcher (matcher)

A matcher entity is a field that is parsed, for example, EventName, and is paired with the appropriate pattern and group for parsing.

Matchers have an associated order. If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found or a failure occurs.

### Table 66. Description of matcher parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>field (Required)</td>
<td>The field to which you want the pattern to apply, for example, EventName, or SourceIp. You can use any of the field names that are listed in the List of valid matcher field names table.</td>
</tr>
<tr>
<td>pattern-id (Required)</td>
<td>The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of the pattern that is previously defined in a pattern ID parameter (Table 64 on page 110).</td>
</tr>
<tr>
<td>order (Required)</td>
<td>The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the EventName field, the one with the lowest order is attempted first.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>capture-group (Optional)</td>
<td>Referenced in the regular expression inside parenthesis (). These captures are indexed starting at one and processed from left to right in the pattern. The capture-group field must be a positive integer less than or equal to the number of capture groups that are contained in the pattern. The default value is zero, which is the entire match. For example, you can define a single pattern for a source IP address and port; where the SourceIp matcher can use a capture group of 1, and the SourcePort matcher can use a capture group of 2, but only one pattern needs to be defined. This field has a dual purpose when combined with the enable-substitutions parameter. To see an example, review the extension document example.</td>
</tr>
<tr>
<td>enable-substitutions (Optional)</td>
<td>Boolean When you set to true, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. This parameter changes the meaning of the capture-group parameter. The capture-group parameter creates the new value, and group substitutions are specified by using \x where x is a group number, 1 - 9. You can use groups multiple times, and any free-form text can also be inserted into the value. For example, to form a value out of group 1, followed by an underscore, followed by group 2, an @, and then group 1 again, the appropriate capture-group syntax is shown in the following code: capture-group=&quot;\1_\2@\1&quot; In another example, a MAC address is separated by colons, but in QRadar, MAC addresses are usually hyphen-separated. The syntax to parse and capture the individual portions is shown in the following example: capture-group=&quot;\1:\2:\3:\4:\5:\6&quot; If no groups are specified in the capture-group when substitutions are enabled, a direct text replacement occurs. Default is false.</td>
</tr>
</tbody>
</table>
Table 66. Description of matcher parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext-data</td>
<td>An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the List of valid matcher field names.</td>
</tr>
</tbody>
</table>

The following table lists valid matcher field names.

Table 67. List of valid matcher field names

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventName (Required)</td>
<td>The event name to be retrieved from the QID to identify the event. Note: This parameter doesn't appear as a field in the Log Activity tab.</td>
</tr>
</tbody>
</table>
| EventCategory cat (LEEF) | An event category for any event with a category not handled by an event-match-single entity or an event-match-multiple entity. Combined with EventName, EventCategory is used to search for the event in the QID. The fields that are used for QIDmap lookups require an override flag to be set when the devices are already known to QRadar, for example,  
<event-match-single event-name="Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity="OverrideAndNeverSend" />  
The force-qidmap-lookup-on-fixup="true" is the flag override. Note: This parameter doesn't appear as a field in the Log Activity tab. |
| SourceIp src (LEEF) | The source IP address for the message. |
| SourcePort srcPort (LEEF) | The source port for the message. |
### Table 67. List of valid matcher field names (continued)

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SourceIpPreNAT srcPreNAT (LEEF)</td>
<td>The source IP address for the message before Network Address Translation (NAT) occurs.</td>
</tr>
<tr>
<td>SourceIpPostNAT srcPostNAT (LEEF)</td>
<td>The source IP address for the message after NAT occurs.</td>
</tr>
<tr>
<td>SourceMAC srcMAC (LEEF)</td>
<td>The source MAC address for the message.</td>
</tr>
<tr>
<td>SourcePortPreNAT srcPreNATPort (LEEF)</td>
<td>The source port for the message before NAT occurs.</td>
</tr>
<tr>
<td>SourcePortPostNAT srcPostNATPort (LEEF)</td>
<td>The source port for the message after NAT occurs.</td>
</tr>
<tr>
<td>DestinationIp dst (LEEF)</td>
<td>The destination IP address for the message.</td>
</tr>
<tr>
<td>DestinationPort dstPort (LEEF)</td>
<td>The destination port for the message.</td>
</tr>
<tr>
<td>DestinationIpPreNAT dstPreNAT (LEEF)</td>
<td>The destination IP address for the message before NAT occurs.</td>
</tr>
<tr>
<td>DestinationIpPostNAT dstPostNAT (LEEF)</td>
<td>The destination IP address for the message after NAT occurs.</td>
</tr>
<tr>
<td>DestinationPortPreNAT dstPreNATPort (LEEF)</td>
<td>The destination port for the message before NAT occurs.</td>
</tr>
<tr>
<td>DestinationPortPostNAT dstPostNATPort (LEEF)</td>
<td>The destination port for the message after NAT occurs.</td>
</tr>
<tr>
<td>DestinationMAC dstMAC (LEEF)</td>
<td>The destination MAC address for the message.</td>
</tr>
<tr>
<td>Field name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DeviceTime</td>
<td>The time and format that is used by the device. This date and time stamp represent the time that the event was sent, according to the device. This parameter doesn't represent the time that the event arrived. The DeviceTime field supports the ability to use a custom date and time stamp for the event by using the ext-data Matcher attribute. The following list contains examples of date and time stamp formats that you can use in the DeviceTime field:</td>
</tr>
<tr>
<td></td>
<td>• ext-data=&quot;dd/MMM/YYYY:hh:mm:ss&quot; 11/Mar/2015:05:26:00</td>
</tr>
<tr>
<td></td>
<td>• ext-data=&quot;MMM dd YYYY / hh:mm:ss&quot; Mar 11 2015 / 05:26:00</td>
</tr>
<tr>
<td></td>
<td>• ext-data=&quot;hh:mm:ss:dd/MMM/YYYY&quot; 05:26:00:11/Mar/2015</td>
</tr>
<tr>
<td></td>
<td>For more information about the possible values for the data and time stamp format, see the Joda-Time web page (<a href="http://www.joda.org/joda-time/key_format.html">http://www.joda.org/joda-time/key_format.html</a>). DeviceTime is the only event field that uses the ext-data optional parameter.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol for the message; for example, TCP, UDP, or ICMP.</td>
</tr>
<tr>
<td>UserName</td>
<td>The user name for the message.</td>
</tr>
<tr>
<td>HostName</td>
<td>The host name for the message. Typically, this field is associated with identity events.</td>
</tr>
<tr>
<td>GroupName</td>
<td>The group name for the message. Typically, this field is associated with identity events.</td>
</tr>
<tr>
<td>IdentityIp</td>
<td>The identity IP address for the message.</td>
</tr>
<tr>
<td>IdentityMac</td>
<td>The identity MAC address for the message.</td>
</tr>
<tr>
<td>IdentityIpv6</td>
<td>The IPv6 identity IP address for the message.</td>
</tr>
<tr>
<td>NetBIOSName</td>
<td>The NetBIOS name for the message. Typically, this field is associated with identity events.</td>
</tr>
<tr>
<td>ExtraIdentityData</td>
<td>Any user-specific data for the message. Typically, this field is associated with identity events.</td>
</tr>
<tr>
<td>Field name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SourceIpv6</td>
<td>The IPv6 source IP address for the message.</td>
</tr>
<tr>
<td>DestinationIpv6</td>
<td>The IPv6 destination IP address for the message.</td>
</tr>
</tbody>
</table>

**JSON matcher (json-matcher)**

A JSON-matcher (json-matcher) entity is a field that is parsed and is paired with the appropriate pattern and group for parsing. This entity is new in IBM QRadar V7.3.1.

If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found.

**Table 68. Description of JSON matcher parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>field (Required)</td>
<td>The field to which you want the pattern to apply; for example, EventName or SourceIp. You can use any of the field names that are listed in the List of valid matcher field names table.</td>
</tr>
<tr>
<td>pattern-id (Required)</td>
<td>The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of an already defined pattern. (Table 64 on page 110)</td>
</tr>
<tr>
<td>order (Required)</td>
<td>The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the EventName field, the one with the lowest order is attempted first. The regular regex matchers and JSON matchers are combined into one list. The different types of matchers are attempted based on their orders, and the process stops when one of the matchers is able to parse out data from the payload.</td>
</tr>
<tr>
<td>enable-substitutions</td>
<td>Boolean</td>
</tr>
<tr>
<td></td>
<td>When set to true, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. Wherever the pattern is in the form of a multi-keypath, set the enable-substitutions value to '='true' so that each keypath in the pattern and expression is replaced with the value that is found by the payload. For example, if the JSON payload contains the first_name and last_name fields, but no full_name field, you can define an expression that contains multiple keypaths, such as {&quot;last_name&quot;}, {&quot;first_name&quot;}. The captured value for this expression is smith, john. Default is false.</td>
</tr>
</tbody>
</table>
Table 68. Description of JSON matcher parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext-data (Optional)</td>
<td>An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the List of valid JSON matcher field names.</td>
</tr>
</tbody>
</table>

The following table lists valid JSON matcher field names.

Table 69. List of valid JSON matcher field names

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventName (Required)</td>
<td>The event name to be retrieved from the QID to identify the event. <strong>Note:</strong> This parameter doesn't appear as a field in the Log Activity tab.</td>
</tr>
<tr>
<td>EventCategory</td>
<td>An event category for any event with a category that is not handled by an event-match-single entity or an event-match-multiple entity. Combined with EventName, EventCategory is used to search for the event in the QID. The fields that are used for QIDmap lookups require an override flag to be set when the devices are already known to the QRadar system, for example:</td>
</tr>
</tbody>
</table>

```xml
<event-match-single event-name="Successfully logged in"
force-qidmap-lookup-on-fixup="true"
device-event-category="CiscoNAC"
severity="4" send-identity="OverrideAndNeverSend" />
```

The `force-qidmap-lookup-on-fixup="true"` is the flag override. **Note:** This parameter doesn't appear as a field in the Log Activity tab. |
<p>| SourceIp | The source IP address for the message. |
| SourcePort | The source port for the message. |
| SourceIpPreNAT | The source IP address for the message before Network Address Translation (NAT) occurs. |</p>
<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SourceIpPostNAT</td>
<td>The source IP address for the message after NAT occurs.</td>
</tr>
<tr>
<td>SourceMAC</td>
<td>The source MAC address for the message.</td>
</tr>
<tr>
<td>SourcePortPreNAT</td>
<td>The source port for the message before NAT occurs.</td>
</tr>
<tr>
<td>SourcePortPostNAT</td>
<td>The source port for the message after NAT occurs.</td>
</tr>
<tr>
<td>DestinationIp</td>
<td>The destination IP address for the message.</td>
</tr>
<tr>
<td>DestinationPort</td>
<td>The destination port for the message.</td>
</tr>
<tr>
<td>DestinationIpPreNAT</td>
<td>The destination IP address for the message before NAT occurs.</td>
</tr>
<tr>
<td>DestinationIpPostNAT</td>
<td>The destination IP address for the message after NAT occurs.</td>
</tr>
<tr>
<td>DestinationPortPreNAT</td>
<td>The destination port for the message before NAT occurs.</td>
</tr>
<tr>
<td>DestinationPortPostNAT</td>
<td>The destination port for the message after NAT occurs.</td>
</tr>
<tr>
<td>DestinationMAC</td>
<td>The destination MAC address for the message.</td>
</tr>
<tr>
<td>Field name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| DeviceTime         | The time and format that is used by the device. This date and time stamp represent the time that the event was sent, according to the device. This parameter doesn't represent the time that the event arrived. The DeviceTime field supports the ability to use a custom date and time stamp for the event by using the ext-data Matcher attribute. The following list contains examples of date and time stamp formats that you can use in the DeviceTime field:  
  - ext-data="dd/MMM/YYYY:hh:mm:ss"  
    11/Mar/2015:05:26:00  
  - ext-data="MMM dd YYYY / hh:mm:ss"  
    Mar 11 2015 / 05:26:00  
  - ext-data="hh:mm:ss:dd/MMM/YYYY"  
    05:26:00:11/Mar/2015  
  For more information about the possible values for the data and time stamp format, see the Java SimpleDateFormat web page (https://docs.oracle.com/javase/8/docs/api/java/text/SimpleDateFormat.html). DeviceTime is the only event field that uses the ext-data parameter. |
| Protocol           | The protocol for the message; for example, TCP, UDP, or ICMP.                                                                                   |
| UserName           | The user name for the message.                                                                                                                 |
| HostName           | The host name for the message. Typically, this field is associated with identity events.                                                       |
| GroupName          | The group name for the message. Typically, this field is associated with identity events.                                                       |
| IdentityIp         | The identity IP address for the message.                                                                                                       |
| IdentityMac        | The identity MAC address for the message.                                                                                                      |
| IdentityIpv6       | The IPv6 identity IP address for the message.                                                                                                  |
| NetBIOSName        | The NetBIOS name for the message. Typically, this field is associated with identity events.                                                      |
| ExtraIdentityData  | Any user-specific data for the message. Typically, this field is associated with identity events.                                                 |
| SourceIpv6         | The IPv6 source IP address for the message.                                                                                                   |
Table 69. List of valid JSON matcher field names (continued)

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DestinationIpv6</td>
<td>The IPv6 destination IP address for the message.</td>
</tr>
</tbody>
</table>

LEEF matcher (leef-matcher)

A LEEF-matcher (leef-matcher) entity is a field that is parsed and is paired with the appropriate pattern of type 'LeefKey' for parsing. This entity is new in IBM QRadar V7.3.2.

If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found.

Table 70. Description of LEEF matcher parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>field (Required)</td>
<td>The field to which you want the pattern to apply; for example, EventName or SourceIp. You can use any of the field names that are listed in the Table 67 on page 113table.</td>
</tr>
<tr>
<td>pattern-id (Required)</td>
<td>The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of an already defined pattern. (Table 64 on page 110)</td>
</tr>
<tr>
<td>order (Required)</td>
<td>The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the EventName field, the one with the lowest order is attempted first. The regular regex, JSON, LEEF, and CEF matchers are combined into one list. The different types of matchers are attempted based on their orders, and the process stops when one of the matchers is able to parse out data from the payload.</td>
</tr>
<tr>
<td>enable-substitutions</td>
<td>Boolean</td>
</tr>
<tr>
<td></td>
<td>When set to true, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. Default is false.</td>
</tr>
<tr>
<td>ext-data (Optional)</td>
<td>An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the Table 67 on page 113.</td>
</tr>
</tbody>
</table>
CEF matcher (cef-matcher)

A CEF-matcher (cef-matcher) entity is a field that is parsed and is paired with the appropriate pattern of type 'CefKey' for parsing. This entity is new in IBM QRadar V7.3.2.

If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>field (Required)</td>
<td>The field to which you want the pattern to apply; for example, EventName or SourceIp. You can use any of the field names that are listed in the Table 67 on page 113.</td>
</tr>
<tr>
<td>pattern-id (Required)</td>
<td>The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of an already defined pattern. (Table 64 on page 110)</td>
</tr>
<tr>
<td>order (Required)</td>
<td>The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the EventName field, the one with the lowest order is attempted first. The regular regex, JSON, LEEF, and CEF matchers are combined into one list. The different types of matchers are attempted based on their orders, and the process stops when one of the matchers is able to parse out data from the payload.</td>
</tr>
<tr>
<td>enable-substitutions (Optional)</td>
<td>Boolean When set to true, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. Default is false.</td>
</tr>
<tr>
<td>ext-data (Optional)</td>
<td>An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the Table 67 on page 113.</td>
</tr>
</tbody>
</table>

Multi-event modifier (event-match-multiple)

The multi-event modifier (event-match-multiple) matches a range of event types and then modifies them as specified by the pattern-id parameter and the capture-group-index parameter.

This match is not done against the payload, but is done against the results of the EventName matcher previously parsed out of the payload.
This entity allows mutation of successful events by changing the device event category, severity, or the method the event uses to send identity events. The capture-group-index must be an integer value (substitutions are not supported) and pattern-ID must reference an existing pattern entity. All other properties are identical to their counterparts in the single-event modifier.

**Single-event modifier (event-match-single)**

Single-event modifier (event-match-single) matches and then modifies exactly one type of event, as specified by the required, case-sensitive EventName parameter.

This entity allows mutation of successful events by changing the device event category, severity, or the method for sending identity events.

When events that match this event name are parsed, the device category, severity, and identity properties are imposed upon the resulting event.

You must set an event-name attribute and this attribute value matches the value of the EventName field. In addition, an event-match-single entity consists of these optional properties:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>device-event-category</td>
<td>A new category for searching for a QID for the event. This parameter is an optimizing parameter because some devices have the same category for all events.</td>
</tr>
<tr>
<td>severity</td>
<td>The severity of the event. This parameter must be an integer value 1 - 10.</td>
</tr>
<tr>
<td></td>
<td>If a severity of less than 1 or greater than 10 is specified, the system defaults to 5.</td>
</tr>
<tr>
<td></td>
<td>If not specified, the default is whatever is found in the QID.</td>
</tr>
</tbody>
</table>
Table 72. Description of single-event parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>send-identity</td>
<td>Specifies the sending of identity change information from the event. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• UseDSMResults If the DSM returns an identity event, the event is passed on. If the DSM does not return an identity event, the extension does not create or modify the identity information. This option is the default value if no value is specified.</td>
</tr>
<tr>
<td></td>
<td>• SendIfAbsent If the DSM creates identity information, the identity event is passed through unaffected. If no identity event is produced by the DSM, but there is enough information in the event to create an identity event, an event is generated with all the relevant fields set.</td>
</tr>
<tr>
<td></td>
<td>• OverrideAndAlwaysSend Ignores any identity event that is returned by the DSM and creates a new identity event, if there is enough information.</td>
</tr>
<tr>
<td></td>
<td>• OverrideAndNeverSend Suppress any identity information that is returned by the DSM. Suggested option unless you are processing events that you want to go into asset updates.</td>
</tr>
</tbody>
</table>

Extension document template

The example of an extension document provides information about how to parse one particular type of Cisco FWSM so that events are not sent with an incorrect event name.

For example, if you want to resolve the word session, which is embedded in the middle of the event name:

Nov 17 09:28:26 192.0.2.1 %FWSM-session-0-302015: Built UDP connection for faddr <IP_address1>/80 gaddr <IP_address2>/31696 laddr <IP_address3>/2157 duration 0:00:00 bytes 57498 (TCP FINs)

This condition causes the DSM to not recognize any events and all the events are unparsed and associated with the generic logger.

Although only a portion of the text string (302015) is used for the QID search, the entire text string (%FWSM-session-0-302015) identifies the event as coming from a Cisco FWSM. Since the entire text string is not valid, the DSM assumes that the event is not valid.

Extension document example for parsing one event type

An FWSM device has many event types and many with unique formats. The following extension document example indicates how to parse one event type.
**Note:** The pattern IDs do not have to match the field names that they are parsing. Although the following example duplicates the pattern, the `SourceIp` field and the `SourceIpPreNAT` field can use the exact same pattern in this case. This situation might not be true in all FWSM events.

```xml
<device-extension xmlns="event_parsing/device_extension">
  <!-- Do not remove the 'allEventNames' value -->
  <pattern id="EventName-Fakeware_Pattern" xmlns=""">
    <matcher field="EventName" order="1" pattern-id="EventName-Fakeware_Pattern" capture-group="1"/>
    <matcher field="SourceIp" order="1" pattern-id="SourceIp-Fakeware_Pattern" capture-group="1"/>
    <matcher field="SourcePort" order="1" pattern-id="SourcePort-Fakeware_Pattern" capture-group="1"/>
    <matcher field="SourceMAC" order="1" pattern-id="SourceMAC-Fakeware_Pattern" capture-group="1"/>
    <matcher field="DestinationIp" order="1" pattern-id="DestinationIp-Fakeware_Pattern" capture-group="1"/>
    <matcher field="DestinationPort" order="1" pattern-id="DestinationPort-Fakeware_Pattern" capture-group="1"/>
    <matcher field="Protocol" order="1" pattern-id="Protocol-Fakeware_Pattern" capture-group="1" />
    <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
  </match-group>
</device-extension>
```

**Parsing basics**

The preceding extension document example demonstrates some of the basic aspects of parsing:

- **IP addresses**
- **Ports**
- **Protocol**
- **Multiple fields that use the same pattern with different groups**

This example parses all FWSM events that follow the specified pattern. The fields that are parsed might not be present in those events when the events include different content.

The information that was necessary to create this configuration that was not available from the event:

- The event name is only the last 6 digits (302015) of the `%FWSM-session-0-302015` portion of the event.
- The FWSM has a hardcoded device event category of Cisco Firewall.
- The FWSM DSM uses the Cisco Pix QIDmap and therefore includes the `device-type-id-override="6"` parameter in the match group. The Pix firewall log source type ID is 6.

**Note:** If the QID information is not specified or is unavailable, you can modify the event mapping. For more information, see the Modifying Event Mapping section in the IBM QRadar User Guide.

**Event name and device event category**

An event name and a device event category are required when the QIDmap is searched. This device event category is a grouping parameter within the database that helps define like events within a device. The `event-match-multiple` at the end of the match group includes hardcoding of the category. The
event-match-multiple uses the EventNameId pattern on the parsed event name to match up to 6 digits. This pattern is not run against the full payload, just that portion parsed as the EventName field.

The EventName pattern references the %FWSM portion of the events; all Cisco FWSM events contain the %FWSM portion. The pattern in the example matches %FWSM followed by any number (zero or more) of letters and dashes. This pattern match resolves the word session that is embedded in the middle of the event name that needs to be removed. The event severity (according to Cisco), followed by a dash and then the true event name as expected by QRadar. The \( \backslash d\{6\} \) string is the only string within the EventNameFWSM pattern that has a capture group.

The IP addresses and ports for the event all follow the same basic pattern: an IP address followed by a colon followed by the port number. This pattern parses two pieces of data (the IP address and the port), and specifies different capture groups in the matcher section.

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

**IP address and port patterns**

The IP address and port patterns are four sets of one to three digits, separated by periods followed by a colon and the port number. The IP address section is in a group, as is the port number, but not the colon. The matcher sections for these fields reference the same pattern name, but a different capture group (the IP address is group 1 and the port is group 2).

The protocol is a common pattern that searches the payload for the first instance of TCP, UDP, ICMP, or GRE. The pattern is marked with the case-insensitive parameter so that any occurrence matches.

Although a second protocol pattern does not occur in the event that is used in the example, there is a second protocol pattern that is defined with an order of two. If the lowest-ordered protocol pattern does not match, the next one is attempted, and so on. The second protocol pattern also demonstrates direct substitution; there are no match groups in the pattern, but with the enable-substitutions parameter enabled, the text TCP can be used in place of protocol=6.

**Creating a log source extensions document to get data into QRadar**

You create log source extensions (LSX) when log sources don't have a supported DSM, or to repair an event that has missing or incorrect information, or to parse an event when the associated DSM fails to produce a result.

**When to create a log source extension**

For log sources that don't have an official DSM, use a Universal DSM (uDSM) to integrate log sources. A log source extension (also known as a device extension) is then applied to the uDSM to provide the logic for parsing the logs. The LSX is based on Java regular expressions and can be used against any protocol type, such as syslog, JDBC, and Log File. Values can be extracted from the logs and mapped to all common fields within IBM QRadar.

When you use log source extensions to repair missing or incorrect content, any new events that are produced by the log source extensions are associated to the log source that failed to parse the original payload. Creating an extension prevents unknown or uncategorized events from being stored as unknown in QRadar.
Using the DSM Editor to quickly create a log source extension

For IBM QRadar V7.2.8 and later, you can use the DSM Editor to create log source extensions. The DSM Editor provides real-time feedback so that you know whether the log source extension that you are creating has problems. You use the DSM Editor to extract fields, define custom properties, categorize events, and define new QID definitions. You can use the DSM Editor to define your own Log Source Type, which eliminates the need to use a Universal DSM. For more information about the DSM Editor, see the IBM QRadar Administration Guide.

Process for manually creating a log source extension

Alternatively, to manually create a log source extension, complete the following steps:

1. Ensure that a log source is created in QRadar.
   Use Universal DSM for the log source type to collect events from a source when the log source type not listed as a QRadar supported DSM.
   For IBM QRadar V7.2.8 and later, you don't need to use the Universal DSM to create a new log source type. If you want, you can use the DSM Editor only to create the new log source type, and then you manually create the log source. You can attach an LSX to a supported log source type, such as Windows, Bluecoat, Cisco, and others that are listed as QRadar supported DSMs.

2. To determine what fields are available, use the Log Activity tab to export the logs for evaluation.

3. Use the extension document example template to determine the fields that you can use.
   It is not necessary to use all of the fields in the template. Determine the values in the log source that can be mapped to the fields in extension document template.

4. Remove any unused fields and their corresponding Pattern IDs from the log source extension document.

5. Upload the extension document and apply the extension to the log source.

6. Map the events to their equivalents in the QIDmap.
   This manual action on the Log Activity tab is used to map unknown log source events to known QRadar events so that they can be categorized and processed.

Related concepts

Examples of log source extensions on QRadar forum
You can create log source extensions (LSX) for log sources that don't have a supported DSM. To help you create your own log source extensions (also known as DSM extensions), you modify existing ones that were created.

“Extension document template” on page 123
The example of an extension document provides information about how to parse one particular type of Cisco FWSM so that events are not sent with an incorrect event name.

Common regular expressions

Use regular expressions to match patterns of text in the log source file. You can scan messages for patterns of letters, numbers, or a combination of both. For example, you can create regular expressions that match source and destination IP addresses, ports, MAC addresses, and more.

The following codes show several common regular expressions:

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

The escape character, or "\", is used to denote a literal character. For example, "." character means "any single character" and matches A, B, 1, X, and so on. To match the "." characters, a literal match, you must use "."
Table 73. Common regex expressions

<table>
<thead>
<tr>
<th>Type</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}</td>
</tr>
<tr>
<td>MAC Address</td>
<td>(:[0-9a-fA-F]{2}:){5}[0-9a-fA-F]{2}</td>
</tr>
<tr>
<td>Port Number</td>
<td>\d{1,5}</td>
</tr>
<tr>
<td>Protocol</td>
<td>(TCP</td>
</tr>
<tr>
<td>Device Time</td>
<td>\w{3}\s\d{2}:\d{2}:\d{2}</td>
</tr>
<tr>
<td>Whitespace</td>
<td>\s</td>
</tr>
<tr>
<td>Tab</td>
<td>\t</td>
</tr>
<tr>
<td>Match Anything</td>
<td>.*?</td>
</tr>
</tbody>
</table>

**Tip:** To ensure that you don't accidentally match another characters, escape any non-digit or non-alpha character.

**Building regular expression patterns**

To create a log source extension, you use regular expressions (regex) to match strings of text from the unsupported log source.

**About this task**

The following example shows a log entry that is referenced in the steps.

```
May 20 17:24:59 kernel: DROP MAC=<MAC_address>
SRC=<Source_IP_address> DST=<Destination_IP_address> LEN=351 TOS=0x00 PREC=0x00 TTL=64 ID=9582
PROTO=UDP SPT=67 DPT=68 LEN=331
```

```
May 20 17:24:59 kernel: PASS MAC=<MAC_address>
SRC=<Source_IP_address> DST=<Destination_IP_address> LEN=351 TOS=0x00 PREC=0x00 TTL=64
ID=9583 PROTO=TCP SPT=1057 DPT=80 LEN=331
```

```
May 20 17:24:59 kernel: REJECT
MAC=<MAC_address> SRC=<Source_IP_address> DST=<Destination_IP_address> LEN=351
TOS=0x00 PREC=0x00 TTL=64 ID=9584 PROTO=TCP SPT=25212 DPT=6881 LEN=331
```

**Procedure**

1. Visually analyze the unsupported log source to identify unique patterns.
   These patterns are later translated into regular expressions.
2. Find the text strings to match.
   **Tip:** To provide basic error checking, include characters before and after the values to prevent similar values from being unintentionally matched. You can later isolate the actual value from the extra characters.
3. Develop pseudo-code for matching patterns and include the space character to denote the beginning and end of a pattern.

   You can ignore the quotes. In the example log entry, the event names are DROP, PASS, and REJECT. The following list shows the usable event fields.
   - EventName: " kernel: VALUE "
   - SourceMAC: " MAC=VALUE "
   - SourceIp: " SRC=VALUE "
   - DestinationIp: " DST=VALUE "
   - Protocol: " PROTO=VALUE "

Chapter 11. Log source extensions 127
- SourcePort: " SPT=VALUE "
- DestinationPort: " DPT=VALUE "

4. Substitute a space with the \s regular expression.

You must use an escape character for non-digit or non-alpha characters. For example, = becomes \= and : becomes \\.

5. Translate the pseudo-code to a regular expression.

<table>
<thead>
<tr>
<th>Field</th>
<th>Pseudo-code</th>
<th>Regular expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventName</td>
<td>&quot; kernel: VALUE &quot;</td>
<td>\skernel\s.*\s</td>
</tr>
<tr>
<td>SourceMAC</td>
<td>&quot; MAC=VALUE &quot;</td>
<td>\sMAC=(?:[0-9a-fA-F]\s){5}[0-9a-fA-F]\s</td>
</tr>
<tr>
<td>SourceIP</td>
<td>&quot; SRC=VALUE &quot;</td>
<td>\sSRC=\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}\s</td>
</tr>
<tr>
<td>DestinationIP</td>
<td>&quot; DST=VALUE &quot;</td>
<td>\sDST=\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}\s</td>
</tr>
<tr>
<td>Protocol</td>
<td>&quot; PROTO=VALUE &quot;</td>
<td>\sPROTO=(TCP</td>
</tr>
<tr>
<td>SourcePort</td>
<td>&quot; SPT=VALUE &quot;</td>
<td>\sSPT=\d{1,5}\s</td>
</tr>
<tr>
<td>DestinationPort</td>
<td>&quot; DPT=VALUE &quot;</td>
<td>\sDPT=\d{1,5}\s</td>
</tr>
</tbody>
</table>

6. Specify capture groups.

A capture group isolates a certain value in the regular expression.

For example, in the SourcePort pattern in the previous example, you can’t pass the entire value since it includes spaces and SRC=<code>. Instead, you specify only the port number by using a capture group. The value in the capture group is what is passed to the relevant field in IBM QRadar.

Insert parenthesis around the values you that you want capture:

<table>
<thead>
<tr>
<th>Field</th>
<th>Regular expression</th>
<th>Capture group</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventName</td>
<td>\skernel\s.*\s</td>
<td>\skernel\s.*\s</td>
</tr>
<tr>
<td>SourceMAC</td>
<td>\sMAC=(?:[0-9a-fA-F]\s){5}[0-9a-fA-F]\s</td>
<td>\sMAC=(?:[0-9a-fA-F]\s){5}[0-9a-fA-F]\s</td>
</tr>
<tr>
<td>SourceIP</td>
<td>\sSRC=\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}\s</td>
<td>\sSRC=\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}\s</td>
</tr>
<tr>
<td>DestinationIP</td>
<td>\sDST=\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}\s</td>
<td>\sDST=\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}\s</td>
</tr>
<tr>
<td>Protocol</td>
<td>\sPROTO=(TCP</td>
<td>UDP</td>
</tr>
<tr>
<td>SourcePort</td>
<td>\sSPT=\d{1,5}\s</td>
<td>\sSPT=\d{1,5}\s</td>
</tr>
<tr>
<td>DestinationPort</td>
<td>\sDPT=\d{1,5}\s</td>
<td>\sDPT=\d{1,5}\s</td>
</tr>
</tbody>
</table>

7. Migrate the patterns and capture groups into the log source extensions document.

The following code snippet shows part of the document that you use:

```xml
<device-extension xmlns="event_parsing/device_extension">
  <pattern id="EventNameFWSM_Pattern" xmlns="">
    <![CDATA[\skernel\s.*\s]]>
  </pattern>
  <pattern id="SourceIp_Pattern" xmlns="">
    <![CDATA[gaddr \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}]/\(\[\d\]{1,5}\)]]>
  </pattern>
  <pattern id="SourceIpPreNAT_Pattern" xmlns="">
    <![CDATA[gaddr \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}]/\(\[\d\]{1,5}\)]]>
  </pattern>
</device-extension>
```

128 IBM QRadar : QRadar DSM Configuration Guide
Uploading extension documents to QRadar

You can create multiple extension documents and then upload them and associated them to various log source types. The logic from the log source extension (LSX) is then used to parse the logs from the unsupported log source.

Extension documents can be stored anywhere before you upload to IBM QRadar.

Procedure

1. On the Admin tab, click Log Source Extensions.
2. Click Add.
3. Assign a name.
4. If you are using the Universal DSM, don't select the extension document as the default for a Log Source Type.
   
   By selecting the Universal DSM as the default, it affects all associated log sources. A Universal DSM can be used to define the parsing logic for multiple custom and unsupported event sources.
5. If you want to apply this log source extension to more than one instance of a log source type, select the log source type from the available Log Source Type list and click the add arrow to set it as the default.

   Setting the default log source type applies the log source extension to all events of a log source type, including those log sources that are automatically discovered.

   Ensure that you test the extension for the log source type first to ensure that the events are parsed correctly.
6. Click Browse to locate the LSX that you saved and then click Upload.

   QRadar validates the document against the internal XSD and verifies the validity of the document before the extension document is uploaded to the system.
7. Click Save and close the window.
8. Associate the log source extension to a log source.
   
   a) From the Admin tab, click Data Sources > Log Sources.
   
   b) Double-click the log source type that you created the extension document for.
   
   c) From the Log Source Extension list, select the document that you created.
   
   d) Click Save and close the window.

Parsing issues and examples

When you create a log source extension, you might encounter some parsing issues. Use these XML examples to resolving specific parsing issues.

Converting a protocol

The following example shows a typical protocol conversion that searches for TCP, UDP, ICMP, or GRE anywhere in the payload. The search pattern is surrounded by any word boundary, for example, tab, space, end of line. Also, the character case is ignored:
**Making a single substitution**

The following example shows a substitution that parses the source IP address, and then overrides the result and sets the IP address to 192.0.2.1, ignoring the IP address in the payload.

This example assumes that the source IP address matches something similar to `SrcAddress=203.0.113.1` followed by a comma:

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

<matcher field="SourceIp" order="1" pattern-id="SourceIp_AuthenOK" capture-group="192.0.2.1" enable-substitutions="true"/>
```

**Generating a colon-separated MAC address**

QRadar detects MAC addresses in a colon-separated form. Because all devices might not use this form, the following example shows how to correct that situation:

```xml
<pattern id="SourceMACWithDashes" xmlns="">
  <![CDATA[
   SourceMAC=(\[0-9a-fA-F]{2})-(\[0-9a-fA-F]{2})-(\[0-9a-fA-F]{2})-(\[0-9a-fA-F]{2})-(\[0-9a-fA-F]{2})-(\[0-9a-fA-F]{2})
  ]]>  
</pattern>

<matcher field="SourceMAC" order="1" pattern-id="SourceMACWithDashes" capture-group="\1:2:3:4:5:6"/>
```

In the preceding example, `SourceMAC=12-34-1a-2b-3c-4d` is converted to a MAC address of `12:34:1a:2b:3c:4d`.

If the dashes are removed from the pattern, the pattern converts a MAC address and has no separators. If spaces are inserted, the pattern converts a space-separated MAC address.

**Combining IP address and port**

Typically an IP address and port are combined into one field, which is separated by a colon.

The following example uses multiple capture groups with one pattern:

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

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

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

**Modifying an Event Category**

A device event category can be hardcoded, or the severity can be adjusted.

The following example adjusts the severity for a single event type:

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

**Suppressing identity change events**

A DSM might unnecessarily send identity change events.

The following examples show how to suppress identity change events from being sent from a single event type and a group of events.

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

// Never send any identity for an event with an event name starting with 7, followed by one to five other digits:
```
Formatting event dates and time stamps

A log source extension can detect several different date and time stamp formats on events. Because device manufacturers do not conform to a standard date and time stamp format, the ext-data optional parameter is included in the log source extension to allow the DeviceTime to be reformatted. The following example shows how an event can be reformatted to correct the date and time stamp formatting:

Multiple Log Formats in a Single Log Source

Occasionally, multiple log formats are included in a single log source.

For example, there are 2 log formats: one for firewall events, and one for authentication events. You must write multiple patterns for parsing the events. You can specify the order to be parsed. Typically, the more frequent events are parsed first, followed by the less frequent events. You can have as many patterns as required to parse all of the events. The order variable determines what order the patterns are matched in.

The following example shows multiple formats for the following fields EventName and UserName. Separate patterns are written to parse each unique log type. Both of the patterns are referenced when you assign the value to the normalized fields.
Parsing a CSV log format

A CSV-formatted log file can use a single parser that has multiple capture groups. It is not always necessary to create multiple Pattern IDs when you parse this log type.

About this task

The following log sample is used:

<table>
<thead>
<tr>
<th>Event</th>
<th>User</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Login</td>
<td>&lt;Username&gt;</td>
<td>&lt;Source_IP_address&gt;</td>
<td>1024</td>
<td>&lt;Destination_IP_address&gt;</td>
<td>22</td>
</tr>
<tr>
<td>Successful Login</td>
<td>&lt;Username&gt;</td>
<td>&lt;Source_IP_address&gt;</td>
<td>1743</td>
<td>&lt;Destination_IP_address&gt;</td>
<td>110</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>&lt;Username&gt;</td>
<td>&lt;Source_IP_address&gt;</td>
<td>1028</td>
<td>&lt;Destination_IP_address&gt;</td>
<td>23</td>
</tr>
</tbody>
</table>

Procedure

1. Create a parser that matches all relevant values by using the previous patterns.

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

2. Place the capture groups around each value:

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

3. Map the field that each capture group is mapped to, incrementing the value as you move.

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

4. Include the values in the log source extension by mapping the capture group to the relevant event.

   The following code shows a partial example of mapping the capture group to the relevant event.

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

5. Upload the log source extension.

6. Map the events.
Chapter 12. Log source extension management

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

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

- Log sources that properly parse the event. Properly parsed events are assigned to the correct log source type and category. In this case, no intervention or extension is required.
- Log sources that parse events, but have a value Unknown in the Log Source parameter. Unknown events are log source events where the log source type is identified, but the payload information cannot be understood by the DSM. The system cannot determine an event identifier from the available information to properly categorize the event. In this case, the event can be mapped to a category or a log source extension can be written to repair the event parsing for unknown events.
- Log sources that cannot identify the log source type and have a value of Stored event in the Log Source parameter. Stored events require you to update your DSM files or write a log source extension to properly parse the event. After the event parses, you can then map the events.

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

Adding a log source extension

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

**Procedure**

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

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

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

7. Click **Save**.

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

**What to do next**
On the **Log Activity** tab, verify that the parsing patterns for events is applied correctly. If the log source categorizes events as **Stored**, the parsing pattern in the log source extension requires adjustment. You can review the extension file against log source events to locate any event parsing issues.
Part 3. DSMs
Chapter 13. 3Com Switch 8800

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

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>3Com</td>
</tr>
<tr>
<td>DSM name</td>
<td>Switch 8800 Series</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-3ComSwitch_qradar-version_build-number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>v3.01.30</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>Status and network condition events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom event properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>3Com website (<a href="http://www.3com.com">http://www.3com.com</a>)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>3COM Switch 8800</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks

Adding a DSM
Configure your 3COM Switch 8800
Configure your 3COM Switch 8800 to forward syslog events to IBM QRadar.

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.

**Configuring your 3COM Switch 8800**

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

**Procedure**

1. Log in to 3COM Switch 8800.
2. To enable the information center, type the following command:
   ```bash
   info-center enable
   ```
3. To configure the log host, type the following command:
   ```bash
   info-center loghost QRadar_ip_address facility informational language english
   ```
4. To configure the ARP and IP information modules, type the following commands.
   ```bash
   info-center source arp channel loghost log level informational
   info-center source ip channel loghost log level informational
   ```
Chapter 14. AhnLab Policy Center

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>AhnLab</td>
</tr>
<tr>
<td>DSM</td>
<td>AhnLab Policy Center</td>
</tr>
<tr>
<td>RPM file names</td>
<td>DSM-AhnLabPolicyCenter-QRadar-Release_Build-Number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>4.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>AhnLabPolicyCenterJdbc</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>Spyware detection, Virus detection, Audit</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td>Ahnlab website (<a href="https://global.ahnlab.com/">https://global.ahnlab.com/</a>)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>AhnLab Policy Center APC</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>AhnLabPolicyCenterJdbc</td>
</tr>
<tr>
<td>Access credentials</td>
<td>Use the access credentials of the DB2 server.</td>
</tr>
<tr>
<td>Log Source Language</td>
<td>If you use QRadar v7.2 or later, you must select a log source language.</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 15. Akamai Kona

The IBM QRadar DSM for Akamai Kona collects event logs from your Akamai Kona platforms. The following table identifies the specifications for the Akamai KONA DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Akamai</td>
</tr>
<tr>
<td>Product</td>
<td>Kona</td>
</tr>
<tr>
<td>DSM RPM name</td>
<td>DSM-AkamaiKona-QRadar_Version-Build_Number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTP Receiver, Akamai Kona REST API</td>
</tr>
<tr>
<td>Event Format</td>
<td>JSON</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All security events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

The two configuration options for Akamai Kona are “Configure an Akamai Kona log source by using the HTTP Receiver protocol” on page 141 and “Configuring an Akamai Kona log source by using the Akamai Kona REST API protocol” on page 142.

Related tasks
Adding a DSM
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.

“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configure an Akamai Kona log source by using the HTTP Receiver protocol

Collect events from Akamai Kona in QRadar by using the HTTP Receiver protocol.

Collect events by using the HTTP Receiver Protocol:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - DSMCommon RPM
   - HTTPReceiver Protocol RPM
   - Akamai KONA DSM RPM
2. Configure your Akamai KONA system to communicate with QRadar. For more information, contact Akamai.

3. If you plan to configure the log source to use the **HTTPs** and **Client Authentication** options, copy the Akamai KONA certificate to the target QRadar Event Collector.

4. For each Akamai KONA server that you want to integrate, create a log source on the QRadar Console. Configure all the required parameters. Use this table to configure Akamai Kona specific parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log source type</td>
<td>Akamai KONA</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>HTTP Receiver</td>
</tr>
<tr>
<td>Client Certificate Path</td>
<td>The absolute file path to the client certificate on the target QRadar Event Collector. Ensure that the Akamai KONA certificate is already copied to the Event Collector. If you select the <strong>HTTPs</strong> and <strong>Client Authentication</strong> option from the <strong>Communication Type</strong> list, the <strong>Client Certificate Path</strong> parameter is required.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The destination port that is configured on the Akamai KONA system. <strong>Important</strong>: Do not use port 514. Port 514 is used by the standard Syslog listener.</td>
</tr>
<tr>
<td>Message Pattern</td>
<td>The <strong>Message Pattern</strong> <code>{&quot;type</code> is for JSON format events.</td>
</tr>
</tbody>
</table>

For more information about this protocol, see “**HTTP Receiver protocol configuration options**” on page 54.

**Restriction**: This integration requires you to open a non-standard port in your firewall for incoming Akamai connections. Use an internal proxy to route the incoming Akamai connections. Do not point the Akamai data stream directly to the QRadar Console. For more information about opening a non-standard port in your firewall, consult your Network security professionals.

**Related tasks**
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Akamai Kona log source by using the Akamai Kona REST API protocol**

Collect logs from Akamai Kona REST API:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - Akamai Kona REST API RPM
   - DSMCommon RPM
• Akamai KONA DSM RPM

2. Configure Akamai Kona to send Security events to QRadar by using the Akamai Kona REST API protocol.

3. Configure Akamai Kona to communicate with QRadar.

   **Note:** The Akamai KONA DSM supports only JSON formatted events. Akamai’s sample CEF and Syslog connector does not work with the Akamai KONA DSM.

4. Add a log source in QRadar.

The following table describes the log source parameters that require specific values for Akamai KONA DSM event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Akamai KONA</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Akamai Kona REST API</td>
</tr>
<tr>
<td>Host</td>
<td>The <strong>Host</strong> value is provided during the SIEM OPEN API provisioning in the Akamai Luna Control Center. The <strong>Host</strong> is a unique base URL that contains information about the appropriate rights to query the security events. This parameter is a password field because part of the value contains secret information.</td>
</tr>
<tr>
<td>Client Token</td>
<td><strong>Client Token</strong> is one of the two security parameters. This token is paired with <strong>Client Secret</strong> to make the client credentials. This token can be found after you provision the Akamai SIEM OPEN API.</td>
</tr>
<tr>
<td>Client Secret</td>
<td><strong>Client Secret</strong> is one of the two security parameters. This secret is paired with <strong>Client Token</strong> to make the client credentials. This token can be found after you provision the Akamai SIEM OPEN API.</td>
</tr>
<tr>
<td>Access Token</td>
<td><strong>Access Token</strong> is a security parameter that is used with client credentials to authorize API client access for retrieving the security events. This token can be found after you provision the Akamai SIEM OPEN API.</td>
</tr>
<tr>
<td>Security Configuration ID</td>
<td><strong>Security Configuration ID</strong> is the ID for each security configuration that you want to retrieve security events for. This ID can be found in the SIEM Integration section of your Akamai Luna portal. You can specify multiple configuration IDs in a comma-separated list. For example: configID1,configID2.</td>
</tr>
</tbody>
</table>
## Table 79. Akamai KONA DSM log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses Akamai Kona by using a proxy, enable <strong>Use Proxy</strong>. If the proxy requires authentication, configure the <strong>Proxy Server</strong>, <strong>Proxy Port</strong>, <strong>Proxy Username</strong>, and <strong>Proxy Password</strong> fields. If the proxy does not require authentication, configure the <strong>Proxy Server</strong> and <strong>Proxy Port</strong> fields.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate</td>
<td>Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The time interval between log source queries to the Akamai SIEM API for new events. The time interval can be in hours (H), minutes (M), or days (D). The default is 1 minute.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second. The default is 5000.</td>
</tr>
</tbody>
</table>

For more information about this protocol, see “Akamai Kona REST API protocol configuration options” on page 31.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 Akamai Kona to communicate with QRadar

You need to configure your Akamai Kona platform to make the security events available for QRadar. Make sure that you have access to your Akamai Luna Control center (https://control.akamai.com) to configure and provision the SIEM integration.

This online documentation contains all the steps and procedure for the configurations: https://developer.akamai.com/tools/siem-integration/docs/siem.htm. Follow steps 1 - 3 to successfully provision the integration.

**Note:** Record the values for the Host, Client Token, Client Secret, Access Token, and Security Configuration Key. You need these values when you configure a log source in QRadar.
Creating an event map for Akamai Kona events

Event mapping is required for a number of Akamai Kona events. Because of the customizable nature of policy rules, some events might not contain a predefined IBM QRadar Identifier (QID) map to categorize security events.

About this task
You can individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track recurring events from your network devices. Until you map an event, all events that are displayed in the Log Activity tab for Akamai Kona are categorized as unknown. Unknown events are easily identified as the Event Name column and Low Level Category columns display Unknown.

As your device forwards events to QRadar, it can take time to categorize all of the events for a device, as some events might not be generated immediately by the event source appliance or software. It is helpful to know how to quickly search for unknown events. When you know how to search for unknown events, you might want to repeat this search until you are satisfied that most of your events are identified.

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 the log source group or Other. Log sources that are not assigned to a group are categorized as Other.
6. From the Log Source list, select your Akamai Kona log source.
7. Click Add Filter.
   The Log Activity tab is displayed with a filter for your log source.
8. From the View list, select Last Hour.
   Any events that are generated by the Akamai Kona DSM in the last hour are displayed. Events that are displayed as unknown in the Event Name column or Low Level Category column require event mapping in QRadar.
   Note: You can save your existing search filter by clicking Save Criteria.

What to do next
Modify the event map. For more information about modifying the event map for Akamai Kona, see “Modifying the event map for Akamai Kona” on page 145

Modifying the event map for Akamai Kona
Modifying an event map allows for the manual categorization of events to a IBM QRadar Identifier (QID) map. Any event that is categorized to a log source can be remapped to a new QRadar Identifier (QID).

About this task
Akamai Kona events that do not have a defined log source can't be mapped to a QRadar Identifier (QID) map by a mapped event. Events without a log source display as SIM Generic Log in the Log Source column.
Procedure
1. On the Event Name column, double-click an unknown event for Akamai Kona.
   The detailed event information is displayed.
2. Click Map Event.
3. 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 categorization.
   - For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the IBM QRadar Administration Guide.
   - From the Low-Level Category list, select a low-level event categorization.
   - From the Log Source Type list, select a log source type.
   The Log Source Type list gives the option to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, Akamai Kona provides all events. You might select another product that likely captures similar events.
4. To search for a QID by name, type a name in the QID/Name field.
   The QID/Name field gives the option to filter the full list of QIDs for a specific word, for example, policy.
5. Click Search.
   A list of QIDs are displayed.
6. Select the QID that you want to associate to your unknown event.
7. Click OK.
   QRadar maps any additional events that are forwarded from your device with the same QID that matches the event payload. The event count increases each time that the event is identified by QRadar.
   If you update an event with a new QRadar Identifier (QID) map, past events that are stored in QRadar are not updated. Only new events are categorized with the new QID.

Sample event messages
Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when using the Akamai Kona REST API protocol for the Akamai KONA DSM:

**Note:** Each event might contain multiple Event IDs and Names.
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>The application is not available - Deny Rule</td>
<td>Warning</td>
<td>{&quot;type&quot;:&quot;akamai_siem&quot;,&quot;format&quot;:&quot;json&quot;,&quot;version&quot;:&quot;1.0&quot;,&quot;attackData&quot;:{&quot;configId&quot;:&quot;&lt;Config Id&gt;&quot;,&quot;policyId&quot;:&quot;&lt;Policy Id&gt;&quot;,&quot;clientIP&quot;:&quot;192.0.2.0&quot;,&quot;rules&quot;:&quot;970901&quot;,&quot;ruleVersions&quot;:&quot;1&quot;,&quot;ruleMessages&quot;:&quot;Application is not Available (HTTP 5XX)&quot;,&quot;ruleTags&quot;:&quot;AKAMAI/BOT/UNKNOWN_BOT&quot;,&quot;ruleData&quot;:&quot;Vector Score: 4, DENY threshold: 2, Alert Rules: 3990001:970901, Deny Rule: , Last Matched Message: Application is not Available (HTTP 5XX)&quot;,&quot;ruleSelectors&quot;:&quot;,&quot;ruleActions&quot;:&quot;monitor&quot;},&quot;httpMessage&quot;:{&quot;requestId&quot;:&quot;&lt;Request Id&gt;&quot;,&quot;start&quot;:&quot;1517337032&quot;,&quot;protocol&quot;:&quot;HTTP/1.1&quot;,&quot;method&quot;:&quot;GET&quot;,&quot;host&quot;:&quot;siem-sample.csi.edgesuite.net&quot;,&quot;port&quot;:&quot;80&quot;,&quot;path&quot;:&quot;path&quot;,&quot;requestHeaders&quot;:&quot;User-Agent: curl/7.35.0Host: siem-sample.csi.edgesuite.netAccept: */*edge_maprule: ksd&quot;,&quot;status&quot;:&quot;403&quot;,&quot;bytes&quot;:&quot;298&quot;,&quot;responseHeaders&quot;:&quot;Server: AkamaiGHostMime-Version: 1.0Content-Type: text/htmlContent-Length: 298Expires: Tue, 30 Jan 2018 18:30:32 GMTDate: Tue, 30 Jan 2018 18:30:32 GMTConnection: close&quot;},&quot;geo&quot;:{&quot;continent&quot;:&quot;&lt;Continent&gt;&quot;,&quot;country&quot;:&quot;&lt;Country&gt;&quot;,&quot;city&quot;:&quot;&lt;City&gt;&quot;,&quot;regionCode&quot;:&quot;&lt;Region Code&gt;&quot;,&quot;asn&quot;:&quot;&lt;asn&gt;&quot;}}</td>
</tr>
<tr>
<td>Anomaly Score Exceeded for Outbound</td>
<td>Suspicious Activity</td>
<td>{&quot;type&quot;:&quot;akamai_siem&quot;,&quot;format&quot;:&quot;json&quot;,&quot;version&quot;:&quot;1.0&quot;,&quot;attackData&quot;:{&quot;configId&quot;:&quot;&lt;Config Id&gt;&quot;,&quot;policyId&quot;:&quot;&lt;Policy Id&gt;&quot;,&quot;clientIP&quot;:&quot;192.0.2.0&quot;,&quot;rules&quot;:&quot;OUTBOUND-ANOMALY&quot;,&quot;ruleVersions&quot;:&quot;4&quot;,&quot;ruleMessages&quot;:&quot;Anomaly Score Exceeded for Outbound&quot;,&quot;ruleTags&quot;:&quot;AKAMAI/POLICY/OUTBOUND_ANOMALY&quot;,&quot;ruleData&quot;:&quot;curl_85D6E381D300243323148F63983BD735&quot;,&quot;ruleSelectors&quot;:&quot;,&quot;ruleActions&quot;:&quot;alert&quot;},&quot;httpMessage&quot;:{&quot;requestId&quot;:&quot;&lt;Request Id&gt;&quot;,&quot;start&quot;:&quot;1517337032&quot;,&quot;protocol&quot;:&quot;HTTP/1.1&quot;,&quot;method&quot;:&quot;GET&quot;,&quot;host&quot;:&quot;siem-sample.csi.edgesuite.net&quot;,&quot;port&quot;:&quot;80&quot;,&quot;path&quot;:&quot;path&quot;,&quot;requestHeaders&quot;:&quot;User-Agent: curl/7.35.0Host: siem-sample.csi.edgesuite.netAccept: */*edge_maprule: ksd&quot;,&quot;status&quot;:&quot;403&quot;,&quot;bytes&quot;:&quot;298&quot;,&quot;responseHeaders&quot;:&quot;Server: AkamaiGHostMime-Version: 1.0Content-Type: text/htmlContent-Length: 298Expires: Tue, 30 Jan 2018 18:30:32 GMTDate: Tue, 30 Jan 2018 18:30:32 GMTConnection: close&quot;},&quot;geo&quot;:{&quot;continent&quot;:&quot;&lt;Continent&gt;&quot;,&quot;country&quot;:&quot;&lt;Country&gt;&quot;,&quot;city&quot;:&quot;&lt;City&gt;&quot;,&quot;regionCode&quot;:&quot;&lt;Region Code&gt;&quot;,&quot;asn&quot;:&quot;&lt;asn&gt;&quot;}}</td>
</tr>
</tbody>
</table>
Chapter 16. Amazon AWS CloudTrail

The IBM QRadar DSM for Amazon AWS CloudTrail supports audit events that are collected from Amazon S3 buckets, and from a Log group in the AWS CloudWatch Logs.

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Amazon</td>
</tr>
<tr>
<td>DSM</td>
<td>Amazon AWS CloudTrail</td>
</tr>
<tr>
<td>RPM name</td>
<td>DSM-AmazonAWSCloudTrail-QRadar_version-Build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Amazon AWS S3 REST API, Amazon Web Services</td>
</tr>
<tr>
<td>Event format</td>
<td>JSON</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Event versions 1.0, 1.02, 1.03, 1.04, and 1.05</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Amazon AWS CloudTrail log source by using the Amazon AWS S3 REST API protocol” on page 150
If you want to collect AWS CloudTrail logs from Amazon S3 buckets, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

“Configuring an Amazon AWS CloudTrail log source by using Amazon Web Services” on page 163
If you want to collect AWS CloudTrail logs from Amazon CloudWatch logs, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using Amazon Web Services.

“Configuring security credentials for your AWS user account” on page 168
You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

**Configuring an Amazon AWS CloudTrail log source by using the Amazon AWS S3 REST API protocol**

If you want to collect AWS CloudTrail logs from Amazon S3 buckets, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

**Procedure**

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - Amazon AWS S3 REST API Protocol RPM
   - DSMCommon RPM
   - Amazon Web Service RPM
   - Amazon AWS CloudTrail DSM RPM
2. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the AmazonS3ReadOnlyAccess policy.
3. Configure the security credentials for your AWS user account.
4. Add an Amazon AWS CloudTrail log source on the QRadar Console.

**Restriction:**

A log source can retrieve data from only one region, so use a different log source for each region. Include the region folder name in the file path for the Directory Prefix event collection method to configure the log source.

The following table describes the common parameter values to collect audit events from Amazon AWS CloudTrail by using the Directory Prefix collection method or the SQS event collection method. These collection methods use the Amazon AWS S3 REST API protocol.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Amazon AWS CloudTrail</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Amazon AWS S3 REST API</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique name for the log source. The Log Source Identifier can be any valid value and does not need to reference a specific server. The Log Source Identifier can be the same value as the Log Source Name. If you have more than one Amazon AWS CloudTrail log source that is configured, you might want to identify the first log source as awscloudtrail1, the second log source as awscloudtrail2, and the third log source as awscloudtrail3.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Authentication Method**     | **Access Key ID / Secret Key**  
  Standard authentication that can be used from anywhere.  
  For more information about configuring security credentials, see “Configuring security credentials for your AWS user account” on page 168.  
  **Assume IAM Role**  
  Authenticate with keys and then temporarily assume a role for access. This option is available only when you use the SQS Event Notifications collection method.  
  For more information about creating IAM users and assigning roles, see “Creating an Identity and Access Management (IAM) user in the AWS Management Console when using the Amazon AWS S3 REST API” on page 155  
  **EC2 Instance IAM Role**  
  If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata that is assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container. |
| Event Format                  | Select **AWS Cloud Trail JSON**. The log source retrieves JSON formatted events.                                                                                                                                                                                                                                             |
| Region Name                   | The region that the SQS Queue or the AWS S3 bucket is in.  
  Example: us-east-1, eu-west-1, ap-northeast-3                                                                                                                                                                                                                                  |
| Use as a Gateway Log Source   | Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.                                                                                                                                                                  |
| Show Advanced Options         | Select this option if you want to customize the event data.                                                                                                                                                                                                                                                                           |
| File Pattern                  | This option is available when you set **Show Advanced Options** to Yes.  
  Type a regex for the file pattern that matches the files that you want to pull; for example, .*? `\.json\..gz` |

<p>| Table 82. Amazon AWS S3 REST API protocol common log source parameters when using the Directory Prefix method or the SQS method (continued) |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Directory</strong></td>
<td>This option is available when you set <strong>Show Advanced Options</strong> to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API protocol attempts to retrieve events.</td>
</tr>
<tr>
<td><strong>S3 Endpoint URL</strong></td>
<td>This option is available when you set <strong>Show Advanced Options</strong> to Yes. The endpoint URL that is used to query the AWS S3 REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is <a href="http://s3.amazonaws.com">http://s3.amazonaws.com</a></td>
</tr>
<tr>
<td><strong>Use Proxy</strong></td>
<td>If QRadar accesses the Amazon Web Service by using a proxy, enable <strong>Use Proxy</strong>. If the proxy requires authentication, configure the <strong>Proxy Server</strong>, <strong>Proxy Port</strong>, <strong>Proxy Username</strong>, and <strong>Proxy Password</strong> fields. If the proxy does not require authentication, configure the <strong>Proxy Server</strong> and <strong>Proxy Port</strong> fields.</td>
</tr>
<tr>
<td><strong>Recurrence</strong></td>
<td>How often a poll is made to scan for new data. If you are using the SQS event collection method, <strong>SQS Event Notifications</strong> can have a minimum value of 10 (seconds). Because SQS Queue polling can occur more often, a lower value can be used. If you are using the Directory Prefix event collection method, <strong>Use a Specific Prefix</strong> has a minimum value of 60 (seconds) or 1M. Because every listBucket request to an AWS S3 bucket incurs a cost to the account that owns the bucket, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15 M = 15 minutes, 30 = seconds.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>The maximum number of events per second that are sent to the flow pipeline. The default is 5000. Ensure that the <strong>EPS Throttle</strong> value is higher than the incoming rate or data processing might fall behind.</td>
</tr>
</tbody>
</table>

The following table describes the specific parameter values to collect audit events from Amazon AWS CloudTrail by using the Directory Prefix event collection method:
Table 83. Amazon AWS S3 REST API protocol log source-specific parameters when using the Directory Prefix method

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 Collection Method</td>
<td>Select <strong>Use a Specific Prefix</strong>.</td>
</tr>
<tr>
<td>Bucket Name</td>
<td>The name of the AWS S3 bucket where the log files are stored.</td>
</tr>
</tbody>
</table>
| Directory Prefix           | The root directory location on the AWS S3 bucket from where the CloudTrail logs are retrieved; for example, AWSLogs/<AccountNumber>/CloudTrail/<RegionName>/  
                             | To pull files from the root directory of a bucket, you must use a forward slash (/) in the **Directory Prefix** file path.  
                             | **Note:**  
                             | • Changing the **Directory Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull.  
                             | • The **Directory Prefix** file path cannot begin with a forward slash (/) unless only the forward slash is used to collect data from the root of the bucket.  
                             | • If the **Directory Prefix** file path is used to specify folders, you must not begin the file path with a forward slash (for example, use folder1/folder2 instead). |
| Signature Version          | Select **AWSSIGNATUREV2** or **AWSSIGNATURE4**.  
                             | **AWSSIGNATUREV2** does not support all Amazon AWS regions.  
                             | **AWSSIGNATURE4** supports all regions. If you are using a region that is supported only by **AWSSIGNATURE4**, you must choose **AWSSIGNATURE4** from the list. |
Table 83. Amazon AWS S3 REST API protocol log source-specific parameters when using the Directory Prefix method (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Automatically Acquire Server Certificate(s) | Select **Yes** for QRadar to automatically download the server certificate and begin trusting the target server. You can use this option to initialize a newly created log source, obtain new certificates, or replace expired certificates. Select **No** to download the certificate manually. Complete the following steps:  
  a. Access your Amazon AWS CloudTrail S3 bucket.  
  b. Export the certificate as a DER-encoded binary certificate to your desktop system. The file extension must be .DER.  
  c. Copy the certificate to the /opt/QRadar/conf/trusted_certificates directory on the QRadar host where you plan to configure the log source. |

The following table describes the parameters that require specific values to collect audit events from Amazon AWS CloudTrail by using the SQS event collection method:

Table 84. Amazon AWS S3 REST API protocol log source-specific parameters when using the SQS method

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 Collection Method</td>
<td>Select <strong>SQS Event Notifications</strong>.</td>
</tr>
<tr>
<td>SQS Queue URL</td>
<td>The full URL that begins with <em>https://</em>, for the SQS Queue that is set up to receive notifications for ObjectCreated events from S3.</td>
</tr>
</tbody>
</table>

5. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console Login</td>
<td>General Audit Event</td>
<td>{&quot;eventVersion&quot;: &quot;1.02&quot;, &quot;userIdentity&quot;: {&quot;type&quot;: &quot;IAMUser&quot;, &quot;principalId&quot;: &quot;XXXXXXXXXXXXXXXXXXXXX&quot;, &quot;arn&quot;: &quot;arn:aws:iam::&lt;Account_number&gt;:user/ xx.accountId&quot;: &quot;&lt;Account_number&gt;&quot;}, &quot;userName&quot;: &quot;&lt;Username&gt;&quot;, &quot;eventTime&quot;: &quot;2016-05-04T14:10:58Z&quot;, &quot;eventSource&quot;: &quot;f.amazonaws.com&quot;, &quot;eventName&quot;: &quot;ConsoleLogin&quot;, &quot;awsRegion&quot;: &quot;us-east-1&quot;, &quot;sourceIPAddress&quot;: &quot;&lt;Source_IP_address&gt; Agent&quot;: &quot;Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.1.1 Safari/537.36&quot;, &quot;requestParameters&quot;: null, &quot;responseElements&quot;: {&quot;ConsoleLogin&quot;: &quot;Success&quot;}, &quot;additionalEventData&quot;: {&quot;LoginTo&quot;: &quot;www.webpage.com&quot;, &quot;MobileVersion&quot;: &quot;No&quot;, &quot;MFAUsed&quot;: &quot;No&quot;}, &quot;eventID&quot;: &quot;xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx&quot;, &quot;eventType&quot;: &quot;AwsConsoleSignIn&quot;, &quot;recipientAccountId&quot;: &quot;&lt;Account_ID&gt;&quot;}</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 security credentials for your AWS user account” on page 168
You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

“Creating an Identity and Access Management (IAM) user in the AWS Management Console when using the Amazon AWS S3 REST API” on page 155

Creating an Identity and Access Management (IAM) user in the AWS Management Console when using the Amazon AWS S3 REST API

An Amazon administrator must create a user and then apply the AmazonS3ReadOnlyAccess policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

Note: Alternatively, you can assign more granular permissions to the bucket. The minimum required permissions are s3:listBucket and s3:getObject.

For more information about permissions that are related to bucket operations, go to the AWS documentation website (https://docs.aws.amazon.com/AmazonS3/latest/dev/using-with-s3-actions.html#using-with-s3-actions-related-to-buckets).

Procedure

1. Create a user:
   a) Log in to the AWS Management Console as an administrator.
   b) Create an Amazon AWS IAM user and then apply the AmazonS3ReadOnlyAccess policy.
2. Find the S3 bucket name and directory prefix that you use to configure a log source in QRadar:
   a) Click Services.
b) From the list, select CloudTrail.
c) From the Trails page, click the name of the trail.
d) Note the name of the S3 bucket that is displayed in the S3 bucket field.
e) Click the Edit icon.
f) Click the Advanced icon.
g) Note the location path for the S3 bucket that is displayed underneath the Log file prefix field.

What to do next
Configure the log source in QRadar. The S3 bucket name is the value for the Bucket name field. The location path for the S3 bucket is the value for Directory prefix field. For more information about configuring the log source, see “Configuring an Amazon AWS CloudTrail log source by using the Amazon AWS S3 REST API protocol” on page 150

Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Create an SQS queue and configure S3 ObjectCreated notifications
You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when using the Amazon AWS S3 REST API protocol.

Complete the following procedures:
1. Finding or creating the S3 Bucket that contains the data that you want to collect.
2. Creating the SQS queue that is used to receive the ObjectCreated notifications from the S3 Bucket that you used in Step 1.
3. Setting up SQS queue permissions.
4. Creating ObjectCreated notifications.

Related tasks
“Finding or creating the S3 bucket that contains the data that you want to collect” on page 156
“Creating the SQS queue that is used to receive ObjectCreated notifications” on page 157
“Setting up SQS queue permissions” on page 157
“Creating ObjectCreated notifications” on page 158
You must create ObjectCreated notifications for the folders that you want to monitor in the S3 bucket.

“Configuring an Amazon AWS CloudTrail log source by using the Amazon AWS S3 REST API protocol” on page 150
If you want to collect AWS CloudTrail logs from Amazon S3 buckets, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

Finding or creating the S3 bucket that contains the data that you want to collect
You must find or create the S3 bucket that contains the data that you want to collect.

Procedure
1. Log in to the AWS Management Console as an administrator.
2. Click Services, and then navigate to the Simple Queue Service Management Console.
3. From the Region column in the S3 buckets list, note the region where the bucket that you want to collect data from is located.
4. Enable the check box beside the bucket name, and then from the panel that opens to the right, click Copy Bucket ARN to copy the value to the clipboard. Save this value or leave it on the clipboard. You
will need this value when you complete the “Creating the SQS queue that is used to receive ObjectCreated notifications” on page 157 procedure.

**What to do next**
Complete the “Creating the SQS queue that is used to receive ObjectCreated notifications” on page 157 procedure.

**Creating the SQS queue that is used to receive ObjectCreated notifications**
You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when using the Amazon AWS S3 REST API protocol.

**Before you begin**
You must complete the Finding or creating the S3 Bucket that contains the data that you want to collect procedure.

The SQS Queue must be in the same region as the AWS S3 bucket that the queue is collecting from.

**Procedure**
1. Log in to the AWS Management Console as an administrator.
2. Click Services, and then navigate to the Simple Queue Service Management Console.
3. In the top right of the window, change the region to where the bucket is located. You noted this value when you completed the “Finding or creating the S3 bucket that contains the data that you want to collect” on page 156 procedure.
4. Select Create New Queue, and then type a value for the Queue Name.
5. Click Standard Queue, and then select Configure Queue at the bottom of the window. Change the default values for the following Queue Attributes.
   - Default Visibility Timeout - 60 seconds (Lower can be used. However, in the case of load balanced collection, duplicate events might occur with values of less than 30 seconds. This value can't be 0.)
   - Message Retention Period - 14 days (Lower can be used. However, in the event of an extended collection, data might be lost.)

   Use the default value for the remaining Queue Attributes.

   More options such as Redrive Policy or SSE can be used depending on the requirements for your AWS environment. These values should not affect collection of data.
6. Select Create Queue.

**What to do next**
Complete the Setting up SQS queue permissions procedure.

**Setting up SQS queue permissions**
You must set up SQS queue permissions for users to access the queue.

**Procedure**
1. Log in to the AWS Management Console as an administrator.
2. Go to the SQS Management Console, and then select the queue that you created from the list.
3. From the Properties window, select Details. Record the ARN field value. You need this value when you complete the “Creating ObjectCreated notifications” on page 158 procedure.
   
   Example: arn:aws:sqs:us-east-1:123456789012:MyTestQueue
4. Optional: Use the Permissions Editor.
   a) From the Properties window, select Permissions > Add a Permission, and then configure the following options.
Table 86. Add a permission parameters

<table>
<thead>
<tr>
<th>Effect</th>
<th>Click Allow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal</td>
<td>Click Everybody (*)</td>
</tr>
<tr>
<td>Actions</td>
<td>From the list, select SendMessage</td>
</tr>
</tbody>
</table>

b) Click **Add Conditionals (Optional)**, and then configure the following parameters:

Table 87. Add Conditionals (Optional) parameters

<table>
<thead>
<tr>
<th>Qualifier</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>ARNLike</td>
</tr>
<tr>
<td>Key</td>
<td>aws:SourceArn</td>
</tr>
<tr>
<td>Value</td>
<td>ARN of the S3 bucket that contains the data from Step 4.a.</td>
</tr>
</tbody>
</table>

c) Click **Add Condition**.

d) Click **Add Permission** at the bottom of the window.


a) In the **Properties** window, at the bottom, select **Edit Policy Document (Advanced)**.

b) Copy and paste the following JSON policy into the **Edit Policy Document** window:

```json
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:123456789012:MySQSQueueName",
      "Condition": {
        " ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::my-test-s3bucket"
        }
      }
    }
  ]
}
```

6. Change the *Resource* in this policy document to match the ARN of your SQS queue from step 3, and the "aws:SourceArn" to match the ARN of your bucket that you recorded when you completed the “Finding or creating the S3 bucket that contains the data that you want to collect” on page 156 procedure.

7. Click **Review Policy**. Ensure the data is correct, and then click **Save Changes**.

**What to do next**
Complete the “Creating ObjectCreated notifications” on page 158 procedure.

**Creating ObjectCreated notifications**
You must create ObjectCreated notifications for the folders that you want to monitor in the S3 bucket.

**Procedure**

1. Log in to the AWS Management Console as an administrator.
2. Click the **Properties** tab.
3. In the **Events** pane, click **Add notification** and then configure the parameters for the new event.

   The following table shows a sample of a ObjectCreated notification parameter configuration:
Table 88. Sample new ObjectCreated notification parameter configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name of your choosing.</td>
</tr>
<tr>
<td>Events</td>
<td>Select <strong>All object create events</strong>.</td>
</tr>
<tr>
<td>Prefix</td>
<td>AWSLogs/</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> You can choose a prefix that contains the data that you want to find, depending on where the CloudTrail data is located and what data that you want to go to the queue. For example; AWSLogs/, CustomPrefix/AWSLogs/, AWSLogs/123456789012/.</td>
</tr>
<tr>
<td>Suffix</td>
<td>json.gz</td>
</tr>
<tr>
<td>Send to</td>
<td>SQS queue</td>
</tr>
</tbody>
</table>
|                   | **Tip:** You can send the data from different folders to the same or different queues to suit your collection or QRadar tenant needs. Choose one or more of the following methods:  
|                   | • Different folders that go to different queues  
|                   | • Different folders from different buckets that go to the same queue  
|                   | • Everything from a single bucket that goes to a single queue  
|                   | • Everything from multiple buckets that go to a single queue       |
| SQS               | SecureQueue_TEST.                                                   |

In the preceding sample parameter configuration, notifications are created for AWSLogs/ in the root of the bucket, which is the default CloudTrail location. When you use this configuration, All ObjectCreated events trigger a notification. If there are multiple accounts and regions in the bucket, everything gets processed. In this example, json.gz files are specified because CloudTrail uses this extension. For types other than CloudTrail, you can omit the extension or choose an extension that matches the data you are looking for in the folders that you have events setup for.

After approximately 5 minutes, the queue that contains data displays.

4. In the **Messages Available** column, you can view the number of messages.
5. From the **SecureQueue TEST** list, select **View/Delete Messages** to view the messages.

Sample message:

```json
{
  "Records": [
    {
      "eventVersion": "2.1",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-2",
      "eventTime": "2018-12-19T01:51:03.251Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "AWS:AIZLCFC5TZD36YHNZY"
      },
      "requestParameters": {
        "sourceIPAddress": "52.46.82.38"
      },
      "responseElements": {
        "x-amz-request-id": "6C05F1349AA50D21",
        "x-amz-id-2": "9e0KovdAUJwnYu1qnEv+uzr0T0vQ+U0pkPnFY6E6agmJ5n745"...
    }
  ]
}```
6. Set a **User** or **Role** permission to access the SQS queue and for permission to download from the target bucket. The user or user role must have permission to read and delete from the SQS queue. After QRadar reads the notification and then downloads and processes the target file, the message must be deleted from the queue.

**Sample Policy:**

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sqs:DeleteMessage",
            "sqs:ReceiveMessage",
            "s3:GetObject"
         ],
         "Resource": [
            "arn:aws:s3:::myBucketName/AWSLogs/*",
            "arn:aws:sqs:us-east-2:429269239926:SecureQueue_TEST"
         ]
      }
   ]
}
```

You can add multiple buckets. To ensure that all objects are accessed, you must have a trailing /* at the end of the folder path that you added.

You can add this policy directly to a user, a user role, or you can create a minimal access user with **sts:AssumeRole** only. When you configure a log source in QRadar, configure the **assume Role ARN** parameter for QRadar to assume the role. To ensure that all files waiting to be processed in a single run (emptying the queue) can finish without retries, use the default value of 1 hour for the **API Session Duration** parameter.

When using assumed roles, ensure that the ARN of the user assuming the rule is in the **Trusted Entities** for that role. From the **Trusted entities** pane, you can view the trusted entities that can assume the role. In addition, the user must have permission to assume roles in that (or any) account. Only my test user, **no.permissions.user**, can have this permission.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": "sts:AssumeRole",
         "Resource": "*"
      }
   ]
}
```
The following table shows a sample Amazon AWS CloudTrail log source configuration in QRadar:

<table>
<thead>
<tr>
<th>Log Source Type</th>
<th>Amazon AWS CloudTrail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Amazon AWS S3 REST API</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>iClope</td>
</tr>
<tr>
<td>[ AWS Authentication Configuration ]</td>
<td></td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Assume IAM Role</td>
</tr>
<tr>
<td>Access Key ID</td>
<td>AMAPPTQYWRGKLQRF</td>
</tr>
<tr>
<td>Secret Key</td>
<td></td>
</tr>
<tr>
<td>Assume Role ARN</td>
<td>arn:aws:iam::4200000235</td>
</tr>
<tr>
<td>Assume Role Session Name</td>
<td>QRadarAWS</td>
</tr>
<tr>
<td>[ AWS S3 Collection Configuration ]</td>
<td></td>
</tr>
<tr>
<td>Event Format</td>
<td>AWS Cloud Trail JSON</td>
</tr>
<tr>
<td>S3 Collection Method</td>
<td>S3 Event Notification</td>
</tr>
<tr>
<td>S3 Queue URL</td>
<td><a href="https://qs.s3-east-2.amazonaws.com">https://qs.s3-east-2.amazonaws.com</a></td>
</tr>
<tr>
<td>Region Name</td>
<td>us-east-2</td>
</tr>
</tbody>
</table>

![Figure 5. Sample Amazon AWS CloudTrail log source configuration](image)

**Troubleshooting Amazon AWS S3 REST API log source integrations**

You configured a log source in QRadar to collect Amazon AWS logs, but the log source status is **Warn** and events are not generated as expected.

**Symptom:**

Error that is shown in /var/log/qradar.error:

```
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.semsources.sources.amazonawsrest AMAZONAWSRESTProvider2 9154] com.q1labs.semsources.sources.amazonawsrest.utils.SimpleRESTFileLister: [ERROR] [NOT:00000030000] [x.x.x.x/- -] [-/- -]IOException encountered when trying to list files from remote Amazon S3 bucket.
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.semsources.sources.amazonawsrest AMAZONAWSRESTProvider2 9154] javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: Server certificate not recognized
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.semsources.sources.amazonawsrest AMAZONAWSRESTProvider2 9154] at com.ibm.jsse2.j.a(j.java:15)
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.semsources.sources.amazonawsrest AMAZONAWSRESTProvider2 9154] at com.ibm.jsse2.j.a(j.java:15)
```

**Cause:**

This error was probably caused by exporting the Amazon SSL certificate from the incorrect URL or by not using the **Automatically Acquire Server Certificate(s)** option when you configured the log source.

**Environment:**

All QRadar versions.

**Diagnosing the problem:**

Verify that the certificate that is on the whitelist does not intersect with the server certificate that is provided by the connection. The server certificate that is sent by Amazon covers the *.s3.amazonaws.com domain. You must export the certificate for the following URL:

https://<bucketname>.s3.amazonaws.com

Chapter 16. Amazon AWS CloudTrail 161
The stack trace in QRadar indicates the issue with the Amazon AWS S3 REST API Protocol. In the following example, QRadar is rejecting an unrecognized certificate. The most common cause is that the certificate is not in the correct format or is not placed in the correct directory on the correct QRadar appliance.

```log
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.sem.sources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN] [NOT:0000004000][x.x.x.x/- -] [-/- -] Rejecting SSL/TLS connection because server presented unrecognized certificate.
The chain sent by the server is:
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.sem.sources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN] [NOT:0000004000][x.x.x.x/- -] [-/- -] Subject = CN=*.s3.amazonaws.com, O=Amazon.com Inc., L=Seattle, ST=Washington, C=US
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.sem.sources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN] [NOT:0000004000][x.x.x.x/- -] [-/- -] Subject = CN=q1.us.ibm.com, OU=IBM, O=IBM, L=John, ST=Doe, C=IN, EMAILADDRESS=jdoe@us.ibm.com
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.sem.sources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN] [NOT:0000004000][x.x.x.x/- -] [-/- -] Subject = EMAILADDRESS=q1sales@us.ibm.com, O=IBM Corp, L=Waltham, ST=Massachusetts, C=US
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.sem.sources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN] [NOT:0000004000][x.x.x.x/- -] [-/- -] Subject = CN=syslogTLS_Server, CN=*
[ecs-ec] [Amazon AWS S3 REST API Protocol Provider Thread: class com.q1labs.sem.sources.sources.amazonawsrest.AmazonAWSRESTProvider29154]
com.q1labs.frameworks.crypto.Q1X509TrustManager: [WARN] [NOT:0000004000][x.x.x.x/- -] [-/- -] The current certificate white list is:
Resolving the problem:
If you downloaded the certificate automatically when you created the log source, verify the following steps:

1. You configured the correct Amazon S3 endpoint URL and the correct bucket name.
2. You selected the Yes option for Automatically Acquire server Certificate(s).
3. You saved the log source.

Note: The log source automatically downloads the .DER certificate file to the /opt/qradar/conf/trusted_certificates directory. To verify that the correct certificate is downloaded and working, complete the following steps:

1. From the Navigation menu, click Enable/Disable to disable the log source.
2. Enable the Amazon AWS CloudTrail log source.

If you manually downloaded the certificate, you must move the .DER certificate file to the correct QRadar appliance. The correct QRadar appliance is assigned in the Target Event Collector field in the Amazon AWS CouldTrail log source.

Note:
The certificate must have a .DER extension. The .DER extension is case-sensitive and must be in uppercase. If the certificate is exported in lowercase, then the log source might experience event collection issues.

1. Access your AWS CloudTrail S3 bucket at https://<bucketname>.s3.amazonaws.com
2. Use Firefox to export the SSL certificate from AWS as a DER certificate file.
3. Copy the DER certificate file to the /opt/qradar/conf/trusted_certificates directory on the QRadar appliance that manages the Amazon AWS CloudTrail log source.
   
   **Note:** The QRadar appliance that manages the log source is identified by the **Target Event Collect** field in the Amazon AWS CloudTrail log source. The QRadar appliance has a copy of the DER certificate file in the /opt/qradar/conf/trusted_certificates folder.

4. Log in to QRadar as an administrator.
5. Click the **Admin** tab.
6. Click the **Log Sources** icon.
7. Select the **Amazon AWS CloudTrail** log source.
8. From the navigation menu, click **Enable/Disable** to disable, then re-enable the Amazon AWS CloudTrail log source.
   
   **Note:** Forcing the log source from disabled to enabled connects the protocol to the Amazon AWS bucket as defined in the log source. A certificate check takes place as part of the first communication.

9. If you continue to have issues, verify that the Amazon AWS bucket name in the **Log Source Identifier** field is correct. Ensure that the Remote Directory path is correct in the log source configuration.

---

**Configuring an Amazon AWS CloudTrail log source by using Amazon Web Services**

If you want to collect AWS CloudTrail logs from Amazon CloudWatch logs, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using Amazon Web Services.

**Procedure**

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol Common
   - Amazon AWS S3 REST API Protocol RPM
   - Amazon Web Services Protocol RPM
   - DSMCommon RPM
   - Amazon AWS CloudTrail DSM RPM

2. Create an Amazon Identity and Access Management (IAM) user and then apply the **CloudWatchLogsReadOnlyAccess** policy.

3. Create and configure the log group of the Amazon CloudWatch Logs to retrieve CloudTrail Logs in QRadar.

4. Configure Amazon AWS CloudTrail to send log files to CloudWatch Logs.

5. Configure security credentials for your AWS user account.

6. Add an Amazon AWS CloudTrail log source on the QRadar Console.

   The following table describes the parameters that require specific values to collect audit events from Amazon AWS CloudTrail by using Amazon Web Services:
Table 89. Amazon Web Services log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Type Amazon AWS CloudTrail for the Log Source Type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Select Amazon Web Services from the Protocol Configuration list.</td>
</tr>
</tbody>
</table>
| Authentication Method      | **Access Key ID / Secret Key**  
  Standard authentication that can be used from anywhere.  

**EC2 Instance IAM Role**  
If your QRadar managed host is running in an AWS EC2 instance, choosing this option uses the IAM role from the metadata that is assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.  

*Access Key*  
The Access Key ID that was generated when you configured the security credentials for your AWS user account.  
If you selected **Access Key ID / Secret Key**, the **Access Key** parameter displays.  

*Secret Key*  
The Secret Key that was generated when you configured the security credentials for your AWS user account.  
If you selected **Access Key ID / Secret Key**, the **Secret Key** parameter displays.  

*Regions*  
Select the check box for each region that is associated with the Amazon Web Service that you want to collect logs from.  

*Other Regions*  
Type the names of any additional regions that are associated with the Amazon Web Service that you want to collect logs from. To collect from multiple regions use a comma-separated list, as shown in the following example:  
`region1,region2`  

*AWS Service*  
The name of the Amazon Web Service.  
From the **AWS Service** list, select **CloudWatch Logs**.  

*Log Group*  
The name of the log group in Amazon CloudWatch where you want to collect logs from.  
**Note**: A single log source collects CloudWatch logs from 1 log group at a time. If you want to collect logs from multiple log groups, create a separate log source for each log group.  

*Log Stream (Optional)*  
The name of the log stream within a log group. If you want to collect logs from all log streams within a log group, leave this field blank.  

*Filter Pattern (Optional)*  
Type a pattern for filtering the collected events. This pattern is not a regex filter. Only the events that contain the exact value that you specified are collected from CloudWatch Logs. If you type ACCEPT as the Filter Pattern value, only the events that contain the word ACCEPT are collected, as shown in the following example.  

```
{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}
```
Table 89. Amazon Web Services log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Extract Original Event** | To forward only the original event that was added to the CloudWatch logs to QRadar, select this option. CloudWatch logs wrap the events that they receive with extra metadata. The original event is the value for the message key that is extracted from the CloudWatch log. The following CloudWatch logs event example shows the original event that is extracted from the CloudWatch log in bold text:  

```json
{LogStreamName: 1234567890_CloudTrail_us-east-2,Timestamp: 1505744407363,Message: {"eventVersion":"1.05","userIdentity": {"type":"IAMUser","principalId":"AAAABBBCCDDDBBBCC","arn": "arn:aws:iam::1234567890:user/QRadar-ITeam","accountId":"1234567890","accessKeyId": "AAAABBBBCCCCDDDD","userName": "User-Name", "sessionContext": {"attributes": {"mfaAuthenticated": "false","creationDate": "2017-09-18T13:22:10Z"}, "invokedBy": "signin.amazonaws.com","eventTime": "2017-09-18T14:10:15Z","eventSource": "cloudtrail.amazonaws.com","eventName": "DescribeTrails","awsRegion": "us-east-1","sourceIPAddress": "127.0.0.1","userAgent": "signin.amazonaws.com","requestParameters": {"includeShadowTrails":false,"trailNameList": []}, "responseElements": null,"requestID": "11b1a00-7a7a-11a1-1a11-44a4aa1a","eventID": "ad914e00-1111-491d-bbbb-a0dd3845b302","eventType": "AwsApiCall","recipientAccountId": "1234567890"}, IngestionTime: 1505744407506, EventId: 33579222361111112247912667222222513333}}
```                                                                                                                                                                                                                                                                                    |
| **Use As A Gateway Log Source** | If you do not want to define a custom log source identifier for events, ensure that this check box is clear.                                                                                                                                                                                                                                                                                                                                                               |
| **Log Source Identifier Pattern** | If you selected **Use As A Gateway Log Source**, use this option to define a custom Log Source Identifier for events that are being processed. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier displays. The following examples show multiple key-value pair functions.  

**Patterns**  

```
VPC=\sREJECT\sFAILURE
$1=\s(REJECT)\sOK
VPC-$1-$2=\s(ACCEPT)\s(OK)
```

**Events**  

```
{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}
```

**Resulting custom log source identifier**  

VPC-ACCEPT-OK
Table 89. Amazon Web Services log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Proxy</strong></td>
<td>If QRadar accesses the Amazon Web Service by using a proxy, select this option.</td>
</tr>
<tr>
<td></td>
<td>If the proxy requires authentication, configure the <strong>Proxy Server</strong>, <strong>Proxy Port</strong>, <strong>Proxy Username</strong>, and <strong>Proxy Password</strong> fields.</td>
</tr>
<tr>
<td></td>
<td>If the proxy does not require authentication, configure the <strong>Proxy Server</strong> and <strong>Proxy Port</strong> fields.</td>
</tr>
<tr>
<td><strong>Automatically Acquire Server Certificate(s)</strong></td>
<td>Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.</td>
</tr>
<tr>
<td></td>
<td>You can use this option to initialize a newly created log source and obtain certificates, or to replace expired certificates.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>The upper limit for the maximum number of events per second (EPS). The default is 5000.</td>
</tr>
<tr>
<td></td>
<td>If the <strong>Use As A Gateway Log Source</strong> option is selected, this value is optional.</td>
</tr>
<tr>
<td></td>
<td>If the <strong>EPS Throttle</strong> parameter value is left blank, no EPS limit is imposed by QRadar.</td>
</tr>
</tbody>
</table>

7. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

The actual CloudTrail logs are wrapped in a CloudWatch logs JSON payload:

Table 90. Amazon CloudTrail Logs sample message supported by the Amazon AWS CloudTrail DSM

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe Trails</td>
<td>Read Activity</td>
<td>{LogStreamName: 1234567890_CloudTrail_us-east-2, Timestamp: 150574407363, Message: {&quot;eventVersion&quot;:&quot;1.05&quot;,&quot;userIdentity&quot;:{&quot;type&quot;:&quot;IAMUser&quot;,&quot;principalId&quot;:&quot;AIDAIEGANDWTHAAUMATYA&quot;,&quot;arn&quot;:&quot;arn:aws:iam::1234567890:user/QRadar-ITeam&quot;,&quot;accountId&quot;:&quot;1234567890&quot;,&quot;accessKeyId&quot;:&quot;AAAABBBCCCDDE&quot;,&quot;userName&quot;:&quot;QRadar-ITeam&quot;,&quot;sessionContext&quot;:{&quot;attributes&quot;:{&quot;mfaAuthenticated&quot;:false,&quot;creationDate&quot;:&quot;2017-09-18T13:22:10Z&quot;},&quot;invokedBy&quot;:&quot;signin.amazonaws.com&quot;},&quot;eventTime&quot;:&quot;2017-09-18T14:10:15Z&quot;,&quot;eventSource&quot;:&quot;cloudtrail.amazonaws.com&quot;,&quot;eventName&quot;:&quot;DescribeTrails&quot;,&quot;awsRegion&quot;:&quot;us-east-1&quot;,&quot;sourceIPAddress&quot;:&quot;127.0.0.1&quot;,&quot;userAgent&quot;:&quot;signin.amazonaws.com&quot;,&quot;requestParameters&quot;:[]},&quot;includeShadowTrails&quot;:false,&quot;trailNameList&quot;:[]},{&quot;responseElements&quot;:null,&quot;requestID&quot;:&quot;17b7a84c-99ca-11a1-9d83-43d5bce2d2fc&quot;,&quot;eventType&quot;:&quot;awsApiCall&quot;,&quot;recipientAccountId&quot;:&quot;1234567890&quot;},IngestionTime: 1505744407506,EventId: 335792223627111111111111222222222222}</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 security credentials for your AWS user account” on page 168
You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

“Creating an Identity and Access (IAM) user in the AWS Management Console when using Amazon Web Services” on page 167

Creating an Identity and Access (IAM) user in the AWS Management Console when using Amazon Web Services

An Amazon administrator must create a user and then apply the CloudWatchLogsReadOnlyAccess policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

Procedure
Create a user:
1. Log in to the AWS Management Console as an administrator.
2. Create an Amazon AWS IAM user and then apply the CloudWatchLogsReadOnlyAccess policy.

What to do next
Configure the log source in QRadar.

Related tasks
“Adding a log source” on page 4
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 log group of the Amazon CloudWatch logs to retrieve Amazon CloudTrail logs in QRadar

You must create a log group in Amazon CloudWatch logs to make the CloudTrail log available for QRadar polling.

Procedure
1. Log in to your CloudWatch console at this link: https://console.aws.amazon.com/cloudwatch
2. Select Logs from left navigation pane.
3. Click Actions > Create Log Group
4. Type the name of your Log Group. For example, CloudTrailAuditLogs.
5. Click Create log group.

You can find more information about working with Log Groups and Log Streams at this link: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Working-with-log-groups-and-streams.html

Configure Amazon AWS CloudTrail to send log files to CloudWatch Logs
You must configure CloudTrail to deliver the logs in a log group of the AWS CloudWatch logs.

Follow the procedures in the AWS online documentation Send Cloud Trail Events to Cloud Watch Logs (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/send-cloudtrail-events-to-cloudwatch-logs.html).
Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console (https://console.aws.amazon.com/iam/).
2. Select Users from left navigation pane and then select your user name from the list.
3. Click the Security Credentials tab.
4. In the Access Keys section, click Create access key.
5. From the window that displays after the access key and corresponding secret access key are created, download the .csv file that contains the keys or copy and save the keys.

   **Note:** Save the Access key ID and Secret access key and use them when you configure a log source in QRadar.

   **Note:** You can view the Secret access key only when it is created.

Related tasks

“Adding a log source” on page 4

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 17. Amazon GuardDuty

The IBM QRadar DSM for Amazon GuardDuty collects Amazon GuardDuty events from the log group of the Amazon CloudWatch logs services.

The following table identifies the specifications for the Amazon GuardDuty DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Amazon</td>
</tr>
<tr>
<td>DSM name</td>
<td>Amazon GuardDuty</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-AmazonGuardDuty-QRadar_version-buildbuild_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>GuardDuty Schema Version 2.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>Event format</td>
<td>JSON</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Amazon GuardDuty Findings</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Amazon GuardDuty Documentation: <a href="https://aws.amazon.com/documentation/guardduty/">https://aws.amazon.com/documentation/guardduty/</a></td>
</tr>
</tbody>
</table>

Configuring an Amazon GuardDuty log source by using the Amazon Web Services protocol

If you want to collect Amazon GuardDuty logs in QRadar, you need to configure a log source on the QRadar Console for Amazon AWS CloudTrail to communicate with QRadar by using the Amazon Web Services protocol.

Procedure

1. If automatic updates are not enabled, download the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - Amazon Web Services Protocol RPM
   - DSMCommon RPM
   - Amazon GuardDuty DSM RPM

2. Create an IAM role for the Lambda function, create and configure a Lambda function and then create a CloudWatch events rule to retrieve Amazon GuardDuty events into QRadar by completing the following steps:
   a) Create an IAM role for the Lambda function.
   b) Create a Lambda function.
   c) Create a CloudWatch events rule.
d) Configure the Lambda function.

3. Create a log group and log stream to retrieve Amazon GuardDuty events for QRadar.

4. Create an Identity and Access (IAM) user in the Amazon AWS user interface when using the Amazon Web Services protocol.

5. Add a Log source for Amazon GuardDuty on the QRadar Console. The following table describes the Amazon Web Services protocol parameters that require specific values for Amazon GuardDuty Logs collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log source type</td>
<td>Amazon GuardDuty</td>
</tr>
<tr>
<td>Protocol configuration</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>Authentication Method</td>
<td><strong>Access Key ID / Secret Key</strong></td>
</tr>
<tr>
<td></td>
<td>Standard authentication that can be used anywhere.</td>
</tr>
<tr>
<td></td>
<td><strong>EC2 Instance IAM Role</strong></td>
</tr>
<tr>
<td></td>
<td>If your QRadar managed host is running in an AWS EC2 instance, choose this option to use the IAM Role from the metadata assigned to the instance for authentication. No keys are required.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This method works only for managed hosts that run within an AWS EC2 container.</td>
</tr>
<tr>
<td>Access Key ID</td>
<td>If you selected <strong>Access Key ID / Secret Key</strong>, the Access Key ID parameter displays.</td>
</tr>
<tr>
<td></td>
<td>The Access Key ID was generated when you configured the security credentials for your AWS user account.</td>
</tr>
<tr>
<td></td>
<td>For more information about configuring the security credentials, see “Configuring security credentials for your AWS user account” on page 168.</td>
</tr>
<tr>
<td>Secret Access Key</td>
<td>If you selected <strong>Access Key ID / Secret Key</strong>, the Secret Access Key parameter displays.</td>
</tr>
<tr>
<td></td>
<td>The Secret Key was generated when you configured the security credentials for your AWS user account.</td>
</tr>
<tr>
<td></td>
<td>For more information about configuring the security credentials, see “Configuring security credentials for your AWS user account” on page 168.</td>
</tr>
<tr>
<td>Regions</td>
<td>Select the check box for each region that is associated with the Amazon Web Service that you want to collect logs from.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Other Regions</td>
<td>Type the names of any additional regions that are associated with the Amazon Web Service that you want to collect logs from.</td>
</tr>
<tr>
<td></td>
<td>To collect from multiple regions, use a comma-separated list, such as the following example: region1,region2</td>
</tr>
<tr>
<td>AWS Service</td>
<td>The name of the Amazon Web Service.</td>
</tr>
<tr>
<td></td>
<td>From the <strong>AWS Service</strong> list, select <strong>CloudWatch Logs</strong>.</td>
</tr>
<tr>
<td>Log Group</td>
<td>The name of the log group in Amazon CloudWatch where you want to collect logs from.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A single log source can collect CloudWatch logs from only one log group at a time. If you want to collect logs from multiple log groups, create a separate log source for each log group.</td>
</tr>
<tr>
<td>Log Stream (Optional)</td>
<td>The name of the log stream within a log group that you want to collect logs from.</td>
</tr>
<tr>
<td>Filter Pattern (Optional)</td>
<td>Type a pattern for filtering the collected events. This pattern is not a regex filter. Only the events that contain the exact value that you specify are collected from CloudWatch Logs.</td>
</tr>
<tr>
<td></td>
<td>If you enter <strong>ACCEPT</strong> as the Filter Pattern value, only events that contain the word <strong>ACCEPT</strong> are collected. The following example shows the effect of the <strong>ACCEPT</strong> value:</td>
</tr>
<tr>
<td></td>
<td><code>{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}</code></td>
</tr>
</tbody>
</table>
### Table 92. Amazon GuardDuty Web Services protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract Original Event</td>
<td>CloudWatch Logs wrap events that it receives with extra metadata. If you want only the original event that was added to the CloudWatch logs to be forwarded to QRadar, select this option. The original event is the value for the message key that is extracted from the CloudWatch Logs. The following CloudWatch logs event example shows the original event that is extracted from the CloudWatch log in bold text:</td>
</tr>
<tr>
<td>Use As A Gateway Log Source</td>
<td>Do not select this check box.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses the Amazon Web Service by using a proxy, enable Use Proxy. If the proxy requires authentication, configure the Proxy Server, Proxy Port, Proxy Username, and Proxy Password fields. If the proxy does not require authentication, configure the Proxy Server and Proxy Port fields.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificates</td>
<td>If you select Yes from the list, QRadar downloads the certificate and begins trusting the target server. This function can be used to initialize a newly created log source and obtain certificates initially, or to replace expired certificates.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second (EPS) that this log source can't exceed. The default is 5000. This value is optional if the Use As A Gateway Log Source is checked. If EPS Throttle is left blank, no limit is imposed by QRadar.</td>
</tr>
</tbody>
</table>

**Related tasks**

- “Creating an IAM role for the Lambda function” on page 173
  You need to create and configure a CloudWatch Events rule to get GuardDuty events and forward the events to the CloudWatch Logs. To do that you need to create an IAM role for the Lambda function.
- “Creating a CloudWatch events rule” on page 175
You need to configure a CloudWatch Events rule to get GuardDuty events and forward the events to the CloudWatch Logs.

“Configuring the Lambda function” on page 176
To do that you need to create an AWS Lambda Function that triggers the processing from CloudWatch Events to CloudWatch Logs.

“Creating a log group and log stream to retrieve Amazon GuardDuty events for QRadar” on page 177
You need to create a log group and log stream inside the log group in Amazon CloudWatch Logs to make the GuardDuty events available for QRadar polling.

“Creating an Identity and Access (IAM) user in the AWS Management Console when using Amazon Web Services” on page 167
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 an IAM role for the Lambda function
You need to create and configure a CloudWatch Events rule to get GuardDuty events and forward the events to the CloudWatch Logs. To do that you need to create an IAM role for the Lambda function.

About this task

Procedure
1. Go to your IAM console (https://console.aws.amazon.com/iam/).
2. Select Roles from the navigation pane.
3. If you have an existing role or roles, select the role name that you want to associate with the Lambda function and complete the following steps:
   a. Expand the Policy name and then click Edit policy.
   b. Click the JSON tab and then verify that the JSON entry matches the following JSON entry:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    }
  ]
}
```
4. If you don’t have an existing role, click Create role.
5. From the list of service or services that use the role, select Lambda.
6. Click Next: Permissions, and then select an appropriate policy.
7. Click Next: Review, and then type a role name in the Role name field. If you want, you can type a description in the Role description field.
8. Click Create role, and then select the new rule that you created.
9. If you want to add an existing policy, complete the following steps:
   a. Click Attach policies.
   b. Expand the Policy name and then click Edit policy.
c. Click the JSON tab and then verify that the JSON entry matches the following JSON entry:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams",
            "logs:PutLogEvents"
        ],
        "Resource": "arn:aws:logs:*:*:*"
    }
    ]
}
```

10. Click Attach policy.

11. If you want to add a new policy, complete the following steps:

   a. Click Add inline policy.

   b. Click the JSON tab, and then copy and paste the following JSON entry:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams",
            "logs:PutLogEvents"
        ],
        "Resource": "arn:aws:logs:*:*:*"
    }
    ]
}
```

12. Click Review Policy, and then type a name for the policy.

13. Click Create policy.

14. Verify that the role has the trust relationship. Click the Trust relationships tab.

15. Click Edit trust relationship and verify the following trust relationship:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "Service": "lambda.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }
    ]
}
```

**What to do next**

Create a Lambda function.

**Related tasks**

“Creating a Lambda function” on page 175
Creating a Lambda function

You need to create and configure a CloudWatch Events rule to get GuardDuty events and forward the events to the CloudWatch Logs. To do that you need to create an AWS Lambda Function that triggers the processing from CloudWatch Events to CloudWatch Logs.

Procedure

1. Go to your AWS Lambda console.
2. Click Create function.
3. In the Author from scratch pane, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You can use GuardDutyToCloudWatch or something more appropriate.</td>
</tr>
<tr>
<td>Runtime</td>
<td>Python 3.6</td>
</tr>
<tr>
<td>Role</td>
<td>Choose an existing role</td>
</tr>
<tr>
<td>Existing Role</td>
<td>Select the role that you created.</td>
</tr>
</tbody>
</table>

4. Click Create function.

What to do next

Create a CloudWatch events rule.

Related tasks

“Creating a CloudWatch events rule” on page 175

You need to configure a CloudWatch Events rule to get GuardDuty events and forward the events to the CloudWatch Logs.

Creating a CloudWatch events rule

You need to configure a CloudWatch Events rule to get GuardDuty events and forward the events to the CloudWatch Logs.

Before you begin

Ensure that you have created an IAM role for the Lambda function and an AWS Lambda Function that triggers the processing from CloudWatch Events to CloudWatch Logs.

Procedure

1. Log in to your CloudWatch console (https://console.aws.amazon.com/cloudwatch/).
2. Click Events > Rules in the navigation pane.
3. Click Create rule.
4. In the Create Rule pane, in Event Source, select the following field values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>GuardDuty</td>
</tr>
<tr>
<td>Event Type</td>
<td>All Events</td>
</tr>
</tbody>
</table>

5. In the Targets pane, click Add targets.
6. Select Lambda function.
7. In the **Function** field, select the function that you created when you completed the *Creating a Lambda function* procedure.

8. Click **Configure details** to open the **Configure rule details** pane.

9. In the **Configure rule details** pane, type a name, such as *GuardDutyToQRadar*.

10. Click **Create rule**.

**What to do next**
Configure the Lambda function.

**Related tasks**
“Creating a Lambda function” on page 175
You need to create and configure a CloudWatch Events rule to get GuardDuty events and forward the events to the CloudWatch Logs. To do that you need to create an AWS Lambda Function that triggers the processing from CloudWatch Events to CloudWatch Logs.

“Configuring the Lambda function” on page 176
To do that you need to create an AWS Lambda Function that triggers the processing from CloudWatch Events to CloudWatch Logs.

**Configuring the Lambda function**
To do that you need to create an AWS Lambda Function that triggers the processing from CloudWatch Events to CloudWatch Logs.

**Before you begin**
Ensure that you have completed the following tasks:

1. Creating an IAM role for the Lambda function
2. Creating a Lambda function
3. Creating a CloudWatch events rule

**Procedure**
1. Go to your AWS Lambda console.
2. Open the configuration section of your Lambda function. Click **Create function**.
3. If **CloudWatch Events** is not automatically added as a trigger source, then add it. The **Designer** tab then looks like the following figure:

   ![Designer tab in Lambda function](image)

   *Figure 6. Designer tab in Lambda function*

4. On the **Function code** pane, replace the default code in `lambda_function.py` with the following Python code:

   ```python
   import boto3
   import time
   import json
   
   print('Loading function')
   
   def lambda_handler(event, context):
       cloudwatch_events = boto3.client('events')
       cloudwatch_logs = boto3.client('logs')
   ```
logGroupFullName='GuardDutyLogGroup'
logStreamFullName='GuardDutyLogStream'

try:
    response = cloudwatch_logs.describe_log_streams(logGroupName=logGroupFullName,
                                                      logStreamNamePrefix=logStreamFullName)
except:
    cloudwatch_logs.create_log_group(logGroupName=logGroupFullName)
    cloudwatch_logs.create_log_stream(logGroupName=logGroupFullName, logStreamName=logStreamFullName,
                                       logStreamNamePrefix=logStreamFullName)
    response = cloudwatch_logs.describe_log_streams(logGroupName=logGroupFullName,
                                                      logStreamNamePrefix=logStreamFullName)
pass

record=json.dumps(event)
logStreams = response['logStreams']

try:
    logStream = logStreams[0]
except:
    cloudwatch_logs.create_log_stream(logGroupName=logGroupFullName, logStreamName=logStreamFullName)
    response = cloudwatch_logs.describe_log_streams(logGroupName=logGroupFullName,
                                                      logStreamNamePrefix=logStreamFullName)
    logStream = logStreams[0]
pass

token= None
if 'uploadSequenceToken' in logStream:
    token = logStream['uploadSequenceToken']

if sequenceToken is available use it to post new log to CloudWatch, otherwise post without sequenceToken optional parameter
if token:
    response = cloudwatch_logs.put_log_events(
        logGroupName=logGroupFullName,
        logStreamName=logStreamFullName,
        logEvents=[
            {
                'timestamp': int(round(time.time() * 1000)),
                'message': record
            },
        ],
        sequenceToken=token
    )
else:
    response = cloudwatch_logs.put_log_events(
        logGroupName=logGroupFullName,
        logStreamName=logStreamFullName,
        logEvents=[
            {
                'timestamp': int(round(time.time() * 1000)),
                'message': record
            },
        ]
    )

return {'records': record}

5. Click Save.

What to do next
The GuardDuty events are now forwarded automatically to your Amazon CloudWatch logs. Create a log
group and log stream inside the log group in Amazon CloudWatch Logs to make the GuardDuty events
available for QRadar polling.

Related tasks
“Creating a log group and log stream to retrieve Amazon GuardDuty events for QRadar” on page 177
You need to create a log group and log stream inside the log group in Amazon CloudWatch Logs to make
the GuardDuty events available for QRadar polling.

Creating a log group and log stream to retrieve Amazon GuardDuty events
for QRadar

You need to create a log group and log stream inside the log group in Amazon CloudWatch Logs to make
the GuardDuty events available for QRadar polling.

Procedure
1. Create a log group.
   a) Log in to your CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
   b) Select Logs from the navigation pane.
   c) Click Action > Create Log Group.
d) Type the name of your log group.
   For example, type GuardDutyLogGroup.

e) Click **Create Log Group**.

2. Create a log stream.
   a) Enter your log group that you created in step one.
   b) Click **Create Log Stream**.
   c) Type the name for your log stream.
      For example, type GuardDutyLogStream.
   d) Click **Create Log Stream**.

**What to do next**
For more information about this procedure, see the AWS online documentation (https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Working-with-log-groups-and-streams.html).

Create an IAM user in the Amazon AWS user interface.

**Related tasks**
“Creating an Identity and Access (IAM) user in the AWS Management Console when using Amazon Web Services” on page 167

---

**Creating an Identity and Access (IAM) user in the AWS Management Console when using Amazon Web Services**

An Amazon administrator must create a user and then apply the CloudWatchLogsReadOnlyAccess policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

**Procedure**
Create a user:
   a) Log in to the AWS Management Console as an administrator.
   b) Create an Amazon AWS IAM user and then apply the CloudWatchLogsReadOnlyAccess policy.

**What to do next**
Configure the log source in QRadar.

**Related tasks**
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

---

**Sample event message**
Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when you use the Amazon Web Services protocol for the Amazon GuardDuty DSM:
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan:EC2/PhishingDomainRequest!DNS</td>
<td>Trojan Detected</td>
<td></td>
</tr>
</tbody>
</table>
    
    ```json
    ```

Chapter 17. Amazon GuardDuty
Chapter 18. Ambiron TrustWave ipAngel

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Ambiron</td>
</tr>
<tr>
<td>DSM name</td>
<td>Ambiron TrustWave ipAngel</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-AmbironTrustwaveIpAngel-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V4.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Snort-based events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Ambiron website (<a href="http://www.apache.org">http://www.apache.org</a>)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>
Chapter 19. Amazon VPC Flow Logs

The IBM QRadar integration for Amazon VPC (Virtual Private Cloud) Flow Logs collects VPC flow logs from an Amazon S3 bucket by using an SQS queue.

To integrate Amazon VPC Flow Logs with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the following RPMs on your QRadar Console.
   • Protocol Common RPM
   • AWS S3 REST API PROTOCOL RPM
2. Configure your Amazon VPC Flow Logs to publish the flow logs to an S3 bucket.
3. Create the SQS queue that is used to receive ObjectCreated notifications from the S3 bucket that you used in Step 2.
4. Create security credentials for your AWS user account.
5. Add an Amazon VPC Flow Logs log source on the QRadar Console.

   **Note:** A Flow Processor must be available and licensed to receive the flow logs. Unlike other log sources, AWS VPC Flow Log events are not sent to Log Activity, they are sent to Network Activity.

The following table describes the parameters that require specific values to collect events from Amazon VPC Flow Logs:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Universal DSM</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Amazon AWS S3 REST API</td>
</tr>
</tbody>
</table>
| Log Source Identifier      | Type a unique name for the log source
   The Log Source Identifier can be any valid value and does not need to reference a specific server. The Log Source Identifier can be the same value as the Log Source Name. If you have more than one Amazon VPC flow Logs log source that is configured, you might want to identify the first log source as vpcflowlogs1, the second log source as vpcflowlogs2, and the third log source as vpcflowlogs3. |
Table 96. Amazon VPC Flow Logs log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| **Authentication Method**         | **Access Key ID / Secret Key**  
Standard authentication that can be used from anywhere.  
For more information about configuring security credentials, see “Configuring security credentials for your AWS user account” on page 168.  
**Assume IAM Role**  
Authenticate with keys and then temporarily assume a role for access. This option is available only when you use the SQS Event Notifications collection method.  
For more information about creating IAM users and assigning roles, see “Creating an Identity and Access Management (IAM) user in the AWS Management Console when using the Amazon AWS S3 REST API” on page 155  
**EC2 Instance IAM Role**  
If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container. |
| **Event Format**                  | AWS VPC Flow Logs                                                                                                                                 |
| **S3 Collection Method**          | SQS Event Notifications                                                                                                                                 |
| **VPC Flow Destination Hostname** | The host name of the Flow Processor where you want to send the logs.                                                                 |
| **VPC Flow Destination Port**     | The port for the Flow Processor where you want to send the VPC logs.                                                                 |
| **SQS Queue URL**                 | The full URL that begins with https://, for the SQS Queue that is set up to receive notifications for ObjectCreated events from S3. |
| **Region Name**                   | The region that is associated with the SQS queue and S3 bucket.  
Example: us-east-1, eu-west-1, ap-northeast-3 |
| **Show Advanced Options**         | The default is No. Select Yes if you want to customize the event data.                                                                 |
| **File Pattern**                  | This option is available when you set Show Advanced Options to Yes.  
Type a regex for the file pattern that matches the files that you want to pull; for example, .*?
\.json\.*gz \n\n\n184 IBM QRadar : QRadar DSM Configuration Guide
### Table 96. Amazon VPC Flow Logs log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| **Local Directory** | This option is available when you set **Show Advanced Options** to Yes.  
The local directory on the Target Event Collector.  
The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events. |
| **S3 Endpoint URL** | This option is available when you set **Show Advanced Options** to Yes.  
The endpoint URL that is used to query the AWS REST API.  
If your endpoint URL is different from the default, type your endpoint URL. The default is http://s3.amazonaws.com |
| **Use Proxy**      | If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**.  
If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields.  
If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields. |
| **Recurrence**     | How often the Amazon AWS S3 REST API Protocol connects to the Amazon cloud API, checks for new files, and if they exist, retrieves them. 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.  
Type a time interval to determine how frequently the remote directory is scanned for new event log files. The minimum value is 1 minute. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15 M = 15 minutes. |
| **EPS Throttle**    | The maximum number of events per second that are sent to the flow pipeline. The default is 5000.  
Ensure that the **EPS Throttle** value is higher than the incoming rate or data processing might fall behind. |

**Related concepts**

“Create the SQS queue that is used to receive ObjectCreated notifications” on page 187  
You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when using the Amazon AWS REST API protocol.

**Related tasks**

“Adding a DSM” on page 4  
“Publishing flow logs to an S3 bucket” on page 186
Complete these steps to publish flow logs to an S3 bucket.

“Configuring security credentials for your AWS user account” on page 168
You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Amazon VPC Flow Logs specifications

The following table describes the specifications for collecting Amazon VPC Flow Logs.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Amazon</td>
</tr>
<tr>
<td>DSM name</td>
<td>Universal DSM</td>
</tr>
<tr>
<td>RPM file name</td>
<td>AWS S3 REST API PROTOCOL</td>
</tr>
<tr>
<td>Supported versions</td>
<td>Flow logs v2</td>
</tr>
<tr>
<td>Protocol</td>
<td>AWS S3 REST API PROTOCOL</td>
</tr>
<tr>
<td>Event format</td>
<td>IPFIX by using QRadar Flow Sources</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Network Flows</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

Publishing flow logs to an S3 bucket

Complete these steps to publish flow logs to an S3 bucket.

Procedure
1. Log in to your AWS Management console, and then from the Services menu, navigate to the VPC Dashboard.
2. Enable the check box for the VPC ID that you want to create flow logs for.
3. Click the Flow Logs tab.
4. Click Create Flow Log, and then configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Select Accept, Reject, or All.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select Send to an S3 Bucket.</td>
</tr>
</tbody>
</table>
Table 98. Create Flow Log parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 Bucket ARN</td>
<td>Type the ARN for the S3 Bucket. Examples:</td>
</tr>
<tr>
<td></td>
<td>• arn:aws:s3:::myTestBucket</td>
</tr>
<tr>
<td></td>
<td>• arn:aws:s3:::myTestBucket/testFlows</td>
</tr>
</tbody>
</table>

5. Click **Create**.

For more information about publishing flow logs to Amazon S3, see the Publishing Flow Logs to Amazon S3 documentation on the AWS website (https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-s3.html).

What to do next
Complete the “Create the SQS queue that is used to receive ObjectCreated notifications” on page 187 procedure.

Create the SQS queue that is used to receive ObjectCreated notifications

You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when using the Amazon AWS REST API protocol.

To create the SQS queue and configure S3 ObjectCreated notifications, see the AWS S3 REST API documentation about “Creating ObjectCreated notifications” on page 158.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure
1. Log in to your IAM console (https://console.aws.amazon.com/iam/).
2. Select **Users** from left navigation pane and then select your user name from the list.
3. Click the **Security Credentials** tab.
4. In the **Access Keys** section, click **Create access key**.
5. From the window that displays after the access key and corresponding secret access key are created, download the .csv file that contains the keys or copy and save the keys.

   **Note:** Save the Access key ID and Secret access key and use them when you configure a log source in QRadar.

   **Note:** You can view the Secret access key only when it is created.

Related tasks
“Adding a log source” on page 4
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 20. APC UPS

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>APC</td>
</tr>
<tr>
<td>DSM name</td>
<td>APC UPS</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-APCUPS-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>UPS events, Battery events, Bypass events, Communication events, Input power events, Low battery condition events, SmartBoost events, SmartTrim events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>APC website (<a href="http://www.apc.com">http://www.apc.com</a>)</td>
</tr>
</tbody>
</table>

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 required to collect APC UPS events:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>APC UPS</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

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

**Related tasks**
- Adding a DSM
- 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.

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 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 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 21. Apache HTTP Server

The Apache HTTP Server DSM for IBM QRadar accepts Apache events by using syslog or syslog-ng. QRadar records all relevant HTTP status events. The following procedure applies to Apache DSMs operating on UNIX/Linux operating systems only.

Do not run both syslog and syslog-ng at the same time.

Select one of the following configuration methods:

• “Configuring Apache HTTP Server with syslog” on page 191
• “Configuring Apache HTTP Server with syslog-ng” on page 193

Configuring Apache HTTP Server with syslog

You can configure your Apache HTTP Server to forward events with the syslog protocol.

Procedure

1. Log in to the server that hosts Apache, as the root user.
2. Edit the Apache configuration file httpd.conf.
3. Add the following information in the Apache configuration file to specify the custom log format:

   LogFormat "%h %A %l %u %t "%r" %>s %p %b" <log format name>

   Where <log format name> is a variable name you provide to define the log format.
4. Add the following information in the Apache configuration file to specify a custom path for the syslog events:

   CustomLog "|/usr/bin/logger -t httpd -p <facility>..<priority>" <log format name>

   Where:
   • <facility> is a syslog facility, for example, local0.
   • <priority> is a syslog priority, for example, info or notice.
   • <log format name> is a variable name that you provide to define the custom log format. The log format name must match the log format that is defined in “Configuring Apache HTTP Server with syslog” on page 191.

   For example,

   CustomLog "|/usr/bin/logger -t httpd -p local1.info" MyApacheLogs
5. Type the following command to disable hostname lookup:

   HostnameLookups off
6. Save the Apache configuration file.
7. Edit the syslog configuration file.

   /etc/syslog.conf
8. Add the following information to your syslog configuration file:

   <facility>..<priority> <TAB><TAB>@<host>

   Where:
   • <facility> is the syslog facility, for example, local0. This value must match the value that you typed in “Configuring Apache HTTP Server with syslog” on page 191.

© Copyright IBM Corp. 2005, 2019
• `<priority>` is the syslog priority, for example, info or notice. This value must match the value that you typed in “Configuring Apache HTTP Server with syslog” on page 191.

• `<TAB>` indicates you must press the Tab key.

• `<host>` is the IP address of the QRadar Console or Event Collector.

9. Save the syslog configuration file.

10. Type the following command to restart the syslog service:

   /etc/init.d/syslog restart

11. Restart Apache to complete the syslog configuration.

   The configuration is complete. The log source is added to QRadar as syslog events from Apache HTTP Servers are automatically discovered. Events that are forwarded to QRadar by Apache HTTP Servers are displayed on the Log Activity tab of QRadar.

---

**Configuring a Log Source in IBM QRadar**

You can configure a log source manually for Apache HTTP Server events in IBM QRadar.

**About this task**

QRadar automatically discovers and creates a log source for syslog events from Apache HTTP Server. However, you can manually create a log source for QRadar to receive syslog events. These configuration steps are optional.

**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 Apache HTTP Server.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Apache installations.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

   The configuration is complete. For more information about Apache, see [http://www.apache.org/](http://www.apache.org/).
Configuring Apache HTTP Server with syslog-ng

You can configure your Apache HTTP Server to forward events with the syslog-ng protocol.

**Procedure**

1. Log in to the server that hosts Apache, as the root user.
2. Edit the Apache configuration file.
   
   /etc/httpd/conf/httpd.conf
3. Add the following information to the Apache configuration file to specify the **LogLevel**:

   LogLevel info

   The **LogLevel** might already be configured to the info level; it depends on your Apache installation.
4. Add the following to the Apache configuration file to specify the custom log format:

   LogFormat "%h %A %l %u %t "%r" %>s %p %b" <log format name>

   Where <log format name> is a variable name you provide to define the custom log format.
5. Add the following information to the Apache configuration file to specify a custom path for the syslog events:

   CustomLog "|/usr/bin/logger -t 'httpd' -u /var/log/httpd/apache_log.socket" <log format name>

   The log format name must match the log format that is defined in “Configuring Apache HTTP Server with syslog-ng” on page 193.
6. Save the Apache configuration file.
7. Edit the syslog-ng configuration file.
   
   /etc/syslog-ng/syslog-ng.conf
8. Add the following information to specify the destination in the syslog-ng configuration file:

   ```
   source s_apache {
       unix-stream("/var/log/httpd/apache_log.socket"
         max-connections(512)
         keep-alive(yes));
   }
   destination auth_destination { <udp|tcp> ("<IP address>" port(514)); };
   log{
       source(s_apache);
       destination(auth_destination);
   }
   ```

   Where:

   `<IP address>` is the IP address of the QRadar Console or Event Collector.
   
   `<udp|tcp>` is the protocol that you select to forward the syslog event.
9. Save the syslog-ng configuration file.
10. Type the following command to restart syslog-ng:

    ```
    service syslog-ng restart
    ```
11. You can now configure the log source in QRadar.

    The configuration is complete. The log source is added to QRadar as syslog events from Apache HTTP Servers are automatically discovered. Events that are forwarded to QRadar by Apache HTTP Servers are displayed on the **Log Activity** tab of QRadar.
Configuring a log source

You can configure a log source manually for Apache HTTP Server events in IBM QRadar.

About this task

QRadar automatically discovers and creates a log source for syslog-ng events from Apache HTTP Server. However, you can manually create a log source for QRadar to receive syslog events. These configuration steps are optional.

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 Apache HTTP Server.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Apache installations.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

   The configuration is complete. For more information about Apache, see http://www.apache.org/.
Chapter 22. Apple Mac OS X

The IBM QRadar DSM for Apple Mac OS X accepts events by using syslog.

QRadar records all relevant firewall, web server access, web server error, privilege escalation, and informational events.

To integrate Mac OS X events with QRadar, you must manually create a log source to receive syslog events.

To complete this integration, you must configure a log source, then configure your Mac OS X to forward syslog events. Syslog events that are forwarded from Mac OS X devices are not automatically discovered. Syslog events from Mac OS X can be forwarded to QRadar on TCP port 514 or UDP port 514.

Configuring a Mac OS X log source

IBM QRadar does not automatically discover or create log sources for syslog events from Apple Mac OS X.

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 Mac OS X.
9. From the Protocol Configuration list, select Syslog.
10. In the Log Source Identifier field, type the IP address or host name for the log source as an identifier for events from your Apple Mac OS X device.
11. Click Save.
12. On the Admin tab, click Deploy Changes.

The log source is added to QRadar. You are now ready to configure your Apple Mac OS X device to forward syslog events to QRadar.

Configuring syslog on your Apple Mac OS X

Configure syslog on systems that run Mac OS X operating systems by using a log stream script to send the MAC system logs to QRadar.

Procedure
1. Create an executable shell script with an .sh extension with the following naming convention:
   <FILE_NAME>.sh.
2. Add the following command to the file that you created:

   ```bash
   #!/bin/sh
   /Users/<PathToPerlScript>/logStream.pl -<Parameters1> <Value1> -<Parameters2> <Value2>
   ```

   The path is an absolute path that usually starts from /Users/....
You can use the following parameters for logStream.pl:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-H</td>
<td>The -H parameter defines the host name or IP to send the logs to.</td>
</tr>
<tr>
<td>-p</td>
<td>The -p parameter defines the port on the remote host, where a syslog receiver is listening. If this parameter is not specified, by default the logStream.pl script uses the TCP port 514 for sending events to QRadar.</td>
</tr>
<tr>
<td>-O</td>
<td>The -O parameter overrides the automatic host name from the OS's /bin/hostname command.</td>
</tr>
<tr>
<td>-s</td>
<td>The syslog header format default is 5424 (RFC5424 time stamp), but 3339 can be specified instead to output the time stamp in RFC3389 format.</td>
</tr>
<tr>
<td>-u</td>
<td>The -u parameter forces logStream to send events by using UDP.</td>
</tr>
<tr>
<td>-v</td>
<td>The -v parameter displays the version information for the logStream.</td>
</tr>
<tr>
<td>-x</td>
<td>The -x parameter is an exclusion filter in grep extended Regex format. For example: parentalcontrolsd</td>
</tr>
</tbody>
</table>

Example:

```
#!/bin/sh
/Users/.../logStream.pl -H 172.16.70.135
```

3. Save your changes.

4. From the terminal, go to the folder that contains the shell file that you created.

5. To make the perl file an executable file, type the following command:

```
chmod +x <FILE_NAME>.sh
```

6. In the terminal, create a file with a .plist file extension as in the following example:

```
<fileName>.plist
```

7. Add the following XML command to the file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"><plist version="1.0">
<dict>
  <key>Label</key>
  <string>com.logSource.app</string>
  <key>Program</key>
  <string>/Users/.../Path_to_Shell_Script_Created_In_Step1 .../shellScript.sh</string>
  <key>RunAtLoad</key>
  <true/>
</dict>
</plist>
```

The XML command holds data in key-value pair. The following table provides the key-value pairs:

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>com.logSource.app</td>
</tr>
</tbody>
</table>
**Table 104. Key-value pairs (continued)**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>/Users/...&lt;Path_To_Shell_Script_Created_In Step1&gt;.../shellScript.sh</td>
</tr>
<tr>
<td>RunAtLoad</td>
<td>True</td>
</tr>
</tbody>
</table>

**Note:**

The value of the Label key must be unique for each .plist file. For example, if you use the Label value com.logSource.app for one .plist file, you can't use the same value for another .plist file.

The Program key holds the path of the shell script that you want to run. The path is an absolute path that usually starts from /Users/....

The RunAtLoad key shows events when you want to run your shell program automatically.

8. Save your changes.

9. To make the .plist file an executable file, type the following command:

   chmod +x <fileName>.plist

10. Copy the file to /Library/LaunchDaemons/ by using the following command:

    sudo cp <Path_To_Your_plist_file> /Library/LaunchDaemons/

11. Restart your Mac system.

12. Log in to QRadar, and then from the Log Activity tab, verify that events are arriving from the Mac system. If events are arriving as Sim Generic, you must manually configure a log source for the Mac system.

**Example:** Consider the following event:


The log source parameter values for that event are:

**Table 105. Log source parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>MAC OS X</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>AAAA-MacBook-Pro.local</td>
</tr>
</tbody>
</table>
Chapter 23. Application Security DbProtect

The IBM QRadar DSM for Application Security DbProtect collects event from DbProtect devices that are installed with the Log Enhanced Event Format (LEEF) Service.

The following table identifies the specifications for the Application Security DbProtect DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Application Security, Inc</td>
</tr>
<tr>
<td>DSM name</td>
<td>DbProtect</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-AppSecDbProtect-QRadar_version-</td>
</tr>
<tr>
<td></td>
<td>build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>v6.2</td>
</tr>
<tr>
<td></td>
<td>v6.3</td>
</tr>
<tr>
<td></td>
<td>v6.3sp1</td>
</tr>
<tr>
<td></td>
<td>v6.3.1</td>
</tr>
<tr>
<td></td>
<td>v6.4</td>
</tr>
<tr>
<td>Protocol</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Application Security website (<a href="http://www.appsecinc.com/">http://www.appsecinc.com/</a>)</td>
</tr>
</tbody>
</table>

To send Application Security DbProtect events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Application Security DbProtect DSM RPM on your QRadar Console:

2. Configure your Application Security DbProtect device to communicate with QRadar. Complete the following steps:
   a. Install the DbProtect LEEF Relay Module.
   b. Configure the DbProtect LEEF Relay
   c. Configure DbProtect alerts.

3. If QRadar does not automatically detect the log source, add an Application Security DbProtect log source on the QRadar Console. Configure all required parameters, and use the following table for DbProtect-specific values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Application Security DbProtect</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

© Copyright IBM Corp. 2005, 2019
Installing the DbProtect LEEF Relay Module

To enable DbProtect to communicate with IBM QRadar, install the DbProtect LEEF Relay module on the same server as the DbProtect console.

**Before you begin**
Before you install the DbProtect LEEF Relay module on a Windows 2003 host, you must install Windows Imaging Components. The wic_x86.exe file contains the Windows Imaging Components and is on the Windows Server Installation CD. For more information, see your Windows 2003 Operating System documentation.

**About this task**
The LEEF Relay module for DbProtect translates the default events messages to Log Enhanced Event Format (LEEF) messages for QRadar. Before you can receive events in QRadar, you must install and configure the LEEF Service for your DbProtect device to forward syslog events. The DbProtect LEEF Relay requires that you install the .NET 4.0 Framework, which is bundled with the LEEF Relay installation.

**Procedure**
2. Save the setup file to the same host as your DbProtect console.
3. Click *Accept* to agree with the Microsoft .NET Framework 4 End-User License Agreement.
4. In the **DbProtect LEEF Relay module installation Wizard**, click **Next**.
5. To select the default installation path, click **Next**.
   If you change the default installation directory, make note of the file location.
6. On the **Confirm Installation** window, click **Next**.
7. Click **Close**.

**What to do next**
“Configuring the DbProtect LEEF Relay” on page 200

Configuring the DbProtect LEEF Relay

After you install the DbProtect LEEF Relay module, configure the service to forward events to IBM QRadar.

**Before you begin**
Stop the DbProtect LEEF Relay service before you edit any configuration values.

**Procedure**
1. Log in to the DbProtect LEEF Relay server.
2. Access the C:\Program Files (x86)\AppSecInc\AppSecLEEFConverter directory.
3. Edit the AppSecLEEFConverter.exe.config file. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SyslogListenerPort</td>
<td>The port number that the DbProtect LEEF Relay uses to listen for syslog messages from the DbProtect console.</td>
</tr>
<tr>
<td>SyslogDestinationHost</td>
<td>The IP address of your QRadar Console or Event Collector.</td>
</tr>
<tr>
<td>SyslogDestinationPort</td>
<td>514</td>
</tr>
</tbody>
</table>

200 IBM QRadar : QRadar DSM Configuration Guide
Parameter | Description
--- | ---
**LogFileName** | A file name for the DbProtect LEEF Relay to write debug and log messages. The LocalSystem user account that runs the DbProtect LEEF Relay service must have write privileges to the file path that you specify.

4. Save the configuration changes to the file.
5. On the desktop of the DbProtect console, select **Start > Run**.
6. Type the following command:
   ```
   services.msc
   ```
7. Click **OK**.
8. In the details pane of the **Services** window, verify the **DbProtect LEEF Relay** is started and set to **automatic startup**.
9. To change a service property, right-click the service name, and then click **Properties**.
10. Using the **Startup type** list, select **Automatic**.
11. If the **DbProtect LEEF Relay** is not started, click **Start**.

**What to do next**
“Configuring DbProtect alerts” on page 201

---

**Configuring DbProtect alerts**

Configure sensors on your DbProtect console to generate alerts.

**Procedure**

1. Log in to the DbProtect console.
2. Click the **Activity Monitoring** tab.
3. Click the **Sensors** tab.
4. Select a sensor and click **Reconfigure**.
5. Select a database instance and click **Reconfigure**.
6. Click **Next** until the **Sensor Manager Policy** window is displayed.
7. Select the **Syslog** check box and click **Next**.
8. In the **Send Alerts to the following Syslog console** field, type the IP address of your DbProtect console.
9. In the **Port** field, type the port number that you configured in the **SyslogListenerPort** field of the DbProtect LEEF Relay.
   **Tip:** By default, 514 is the default Syslog listen port for the DbProtect LEEF Relay.
10. Click **Add**.
11. Click **Next** until you reach the **Deploy to Sensor** window.
12. Click **Deploy to Sensor**.
Chapter 24. Arbor Networks

Several Arbor Networks DSMs can be integrated with IBM QRadar.

This section provides information on the following DSMs:

- “Arbor Networks Peakflow SP” on page 203
- “Arbor Networks Pravail” on page 207

Arbor Networks Peakflow SP

IBM QRadar can collect and categorize syslog and TLS syslog events from Arbor Networks Peakflow SP appliances that are in your network.

Arbor Networks Peakflow SP appliances store the syslog events locally.

To collect local syslog events, you must configure your Peakflow SP appliance to forward the syslog events to a remote host. QRadar automatically discovers and creates log sources for syslog events that are forwarded from Arbor Networks Peakflow SP appliances. QRadar supports syslog events that are forwarded from Peakflow V5.8 to V8.1.2.

To configure Arbor Networks Peakflow SP, complete the following steps:

1. On your Peakflow SP appliance, create a notification group for QRadar.
2. On your Peakflow SP appliance, configure the global notification settings.
3. On your Peakflow SP appliance, configure your alert notification rules.
4. If automatic updates are not enabled for QRadar, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console.
   - DSMCommon RPM
   - Arbor Networks Peakflow SP DSM RPM
5. Configure your Arbor Networks Peakflow SP appliance to send syslog or TLS syslog events to QRadar.
6. If QRadar does not automatically detect the log source, add an Arbor Networks Peakflow SP log source on the QRadar Console. The following tables describe the parameters that require specific values to collect events from Arbor Networks Peakflow SP:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Arbor Networks Peakflow SP</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Select <strong>Syslog</strong> or <strong>TLS Syslog</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique name for the log source.</td>
</tr>
</tbody>
</table>

Related concepts

“TLS syslog protocol configuration options” on page 93

Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Supported event types for Arbor Networks Peakflow SP**

The Arbor Networks Peakflow DSM for IBM QRadar collects events from several categories. Each event category contains low-level events that describe the action that is taken within the event category. For example, authentication events can have low-level categories of login successful or login failure.

The following list defines the event categories that are collected by QRadar from Peakflow SP appliances:

- Denial of Service (DoS) events
- Authentication events
- Exploit events
- Suspicious activity events
- System events

**Configuring a remote syslog in Arbor Networks Peakflow SP**

To collect events, you must configure a new notification group or edit existing groups to add IBM QRadar as a remote syslog destination.

**Procedure**

1. Log in to your Peakflow SP configuration interface as an administrator.
2. In the navigation menu, select **Administration > Notification > Groups**.
3. Click **Add Notification Group**.
4. In the **Destinations** field, type the IP address of your QRadar system.
5. In the **Port** field, type 514 as the port for your syslog destination.
6. From the **Facility** list, select a syslog facility.
7. From the **Severity** list, select info.
   - The informational severity collects all event messages at the informational event level and higher severity.
8. Click **Save**.
9. Click **Configuration Commit**.

**Configuring global notifications settings for alerts in Arbor Networks Peakflow SP**

Global notifications in Arbor Networks Peakflow SP provide system notifications that are not associated with rules.

**About this task**

This procedure defines how to add IBM QRadar as the default notification group and enable system notifications.

**Procedure**

1. Log in to the configuration interface for your Arbor Networks Peakflow SP appliance as an administrator.
2. In the navigation menu, select **Administration > Notification > Global Settings**.
3. In the **Default Notification Group** field, select the notification group that you created for QRadar syslog events.
4. Click **Save**.
5. Click **Configuration Commit** to apply the configuration changes.
6. Log in to the Arbor Networks Peakflow SP command-line interface as an administrator.
7. Type the following command to list the current alert configuration:

   services sp alerts system_errors show
8. Optional: Type the following command to list the fields names that can be configured:

   services sp alerts system_errors ?
9. Type the following command to enable a notification for a system alert:

   services sp alerts system_errors <name> notifications enable
   Where <name> is the field name of the notification.
10. Type the following command to commit the configuration changes:

    config write

**Configuring alert notification rules in Arbor Networks Peakflow SP**

To generate events, you must edit or add rules to use the notification group that IBM QRadar uses as a remote syslog destination.

**Procedure**

1. Log in to your Arbor Networks Peakflow SP configuration interface as an administrator.
2. In the navigation menu, select **Administration > Notification > Rules**.
3. Select one of the following options:
   - Click a current rule to edit the rule.
   - Click **Add Rule** to create a new notification rule.
4. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Type the IP address or host name as an identifier for events from your Peakflow SP installation. The log source identifier must be a unique value.</td>
</tr>
<tr>
<td><strong>Resource</strong></td>
<td>Type a CIDR address or select a managed object from the list of Peakflow resources.</td>
</tr>
<tr>
<td><strong>Importance</strong></td>
<td>Select the Importance of the rule.</td>
</tr>
<tr>
<td><strong>Notification Group</strong></td>
<td>Select the Notification Group that you assigned to forward syslog events to QRadar.</td>
</tr>
</tbody>
</table>

5. Repeat these steps to configure any other rules that you want to create.
6. Click **Save**.
7. Click **Configuration Commit** to apply the configuration changes.

QRadar automatically discovers and creates a log source for Arbor Networks Peakflow SP appliances. Events that are forwarded to QRadar are displayed on the **Log Activity** tab.
Configuring an Arbor Networks Peakflow SP log source

IBM QRadar automatically discovers and creates a log source for syslog events that are forwarded from Arbor Networks Peakflow SP. The following configuration steps to manually add the log source are optional.

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 Name field, type a name for your log source.
7. Optional: In the Log Source Description field, type a description for your log source.
8. From the Log Source Type list, select Arbor Networks Peakflow.
9. From the Protocol Configuration list, select Syslog.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>The IP address or host name is used as an identifier for events from your Peakflow SP installation. The log source identifier must be a unique value.</td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
<td>The credibility of the log source. 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.</td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
<td>The event collector to use as the target for the log source.</td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
<td>Enables the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the Coalescing Events list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td><strong>Incoming Event Payload</strong></td>
<td>The incoming payload encoder for parsing and storing the logs.</td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
<td>Enables the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Store Event Payload list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

11. Click Save.

Table 110. System parameters
12. On the **Admin** tab, click **Deploy Changes**.

## Arbor Networks Pravail

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Arbor Networks</td>
</tr>
<tr>
<td>DSM</td>
<td>Arbor Networks Pravail</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-ArborNetworksPravail-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded events</td>
<td>All relevant events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Arbor Networks website (<a href="http://www.arbornetworks.com">www.arbornetworks.com</a>)</td>
</tr>
</tbody>
</table>

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

1. If automatic updates are not enabled, download and install the most recent Arbor Networks Pravail 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 Pravail system, create a log source on the QRadar Console. Configure the required parameters, and use the following table for the Arbor Pravail specific parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Arbor Networks Pravail</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

### Related tasks

- Adding a DSM
- Configuring your Arbor Networks Pravail system to send events to IBM QRadar

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

- 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.

**Configuring your Arbor Networks Pravail system to send events to IBM QRadar**

To collect all audit logs and system events from Arbor Networks Pravail, you must add a destination that specifies 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:

<table>
<thead>
<tr>
<th>Table 113. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Host</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Severity</td>
</tr>
<tr>
<td>Alert Types</td>
</tr>
</tbody>
</table>

7. Click **Save**.
Chapter 25. Arpeggio SIFT-IT

The IBM QRadar SIFT-IT DSM accepts syslog events from Arpeggio SIFT-IT running on IBM i that are formatted as Log Event Extended Format (LEEF).

QRadar supports events from Arpeggio SIFT-IT 3.1 and later installed on IBM i version 5 revision 3 (V5R3) and later.

Arpeggio SIFT-IT supports syslog events from the journal QAUDJRN in LEEF format.

Example:
Jan 29 01:33:34 <Server> LEEF:1.0|Arpeggio|SIFT-IT|3.1|PW_U|sev=3
usrName=<Username> src=<Source_IP_address> srcPort=543 jJobNam=QBASE
jJobUsr=<Username> jJobNum=1664 jmtIP=<Source_IP_address> jmtPort=543
jSeqNo=4755 jPgm=QWTMCNML jPgmLib=QSYS jMsgId=PWU0000 jType=U jUser=ROOT
jDev=QPADEV000F jMsgTxt=Invalid user id <Username>. Device <Device_ID>.

Events that SIFT-IT sends to QRadar are determined with a configuration rule set file. SIFT-IT includes a default configuration rule set file that you can edit to meet your security or auditing requirements. For more information about configuring rule set files, see your SIFT-IT User Guide.

Configuring a SIFT-IT agent

Arpeggio SIFT-IT can forward syslog events in LEEF format with SIFT-IT agents.

About this task

A SIFT-IT agent configuration defines the location of your IBM QRadar installation, the protocol and formatting of the event message, and the configuration rule set.

Procedure

1. Log in to your IBM i.
2. Type the following command and press Enter to add SIFT-IT to your library list:
   ```
   ADDLIBLE SIFTITLIB0
   ```
3. Type the following command and press Enter to access the SIFT-IT main menu:
   ```
   GO SIFTIT
   ```
4. From the main menu, select 1. Work with SIFT-IT Agent Definitions.
5. Type 1 to add an agent definition for QRadar and press Enter.
6. In the SIFT-IT Agent Name field, type a name.
   For example, QRadar.
7. In the Description field, type a description for the agent.
   For example, Arpeggio agent for QRadar.
8. In the Server host name or IP address field, type the location of your QRadar Console or Event Collector.
9. In the Connection type field, type either *TCP, *UDP, or *SECURE.
   The *SECURE option requires the TLS protocol.
10. In the Remote port number field, type 514.
    By default, QRadar supports both TCP and UDP syslog messages on port 514.
11. In the Message format options field, type *QRadar.
12. Optional: Configure any additional parameters for attributes that are not QRadar specific.
The additional operational parameters are described in the *SIFT-IT User Guide*.

13. Press F3 to exit to the **Work with SIFT-IT Agents Description** menu.
14. Type 9 and press Enter to load a configuration rule set for QRadar.
15. In the **Configuration file** field, type the path to your QRadar configuration rule set file.
   Example:
   `/sifitit/Qradarconfig.txt`
16. Press F3 to exit to the **Work with SIFT-IT Agents Description** menu.
17. Type 11 to start the QRadar agent.

**What to do next**
Syslog events that are forwarded by Arpeggio SIFT-IT in LEEF format are automatically discovered by QRadar. In most cases, the log source is automatically created in QRadar after a few events are detected. If the event rate is low, you might be required to manually create a log source for Arpeggio SIFT-IT in QRadar.

Until the log source is automatically discovered and identified, the event type displays as Unknown on the **Log Activity** tab of QRadar. Automatically discovered log sources can be viewed on the **Admin** tab of QRadar by clicking the **Log Sources** icon.

**Related concepts**
“TLS syslog protocol configuration options” on page 93
Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

### Configuring a Arpeggio SIFT-IT log source

IBM QRadar automatically discovers and creates a log source for system authentication events forwarded from Arpeggio SIFT-IT.

**About this task**
This procedure is optional.

**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 **Arpeggio SIFT-IT**.
9. From the **Protocol Configuration** list, select **Syslog**.
10. In the **Log Source Identifier** field, type the IP address or host name for the log source as an identifier for events from your Arpeggio SIFT-IT installation.
11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
After you create your IBM QRadar agent definition, you can use your Arpeggio SIFT-IT software and QRadar integration to customize your security and auditing requirements.

You can customize the following security and auditing requirements:

- Create custom configurations in Arpeggio SIFT-IT with granular filtering on event attributes.
  
  For example, filtering on job name, user, file or object name, system objects, or ports. All events that are forwarded from SIFT-IT and the contents of the event payload in QRadar are easily searched.

- Configure rules in QRadar to generate alerts or offenses for your security team to identify potential security threats, data loss, or breaches in real time.

- Configuring processes in Arpeggio SIFT-IT to trigger real-time remediation of issues on your IBM i.

- Creating offenses for your security team from Arpeggio SIFT-IT events in QRadar with the Offenses tab or configuring email job logs in SIFT-IT for your IBM i administrators.

- Creating multiple configuration rule sets for multiple agents that run simultaneously to handle specific security or audit events.

  For example, you can configure one QRadar agent with a specific rule set for forwarding all IBM i events, then develop multiple configuration rule sets for specific compliance purposes. You can easily manage configuration rule sets for compliance regulations, such as FISMA, PCI, HIPPA, SOX, or ISO 27001. All of the events that are forwarded by SIFT-IT QRadar agents are contained in a single log source and categorized to be easily searched.
Chapter 26. Array Networks SSL VPN

The Array Networks SSL VPN DSM for IBM QRadar collects events from an ArrayVPN appliance by using syslog.

QRadar records all relevant SSL VPN events that are forwarded by using syslog on TCP port 514 or UDP port 514.

Configuring a log source

To send Array Networks SSL VPN events to IBM QRadar, you must manually create a log source.

About this task

QRadar does not automatically discover or create log sources for syslog events from Array Networks SSL VPN.

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 Array Networks SSL VPN Access Gateways.
9. From the Protocol Configuration list, select Syslog.
10. In the Log Source Identifier field, type the IP address or host name for the log source.
11. Click Save.
12. On the Admin tab, click Deploy Changes.

What to do next

You are now ready to configure your Array Networks SSL VPN appliance to forward remote syslog events to QRadar. For more information on configuring Array Networks SSL VPN appliances, see your Array Networks documentation.
Chapter 27. Aruba Networks

Several Aruba DSMs can be integrated with IBM QRadar.

This section provides information on the following DSMs:

- “Aruba ClearPass Policy Manager” on page 215
- “Aruba Mobility Controllers” on page 219

Aruba ClearPass Policy Manager

The IBM QRadar DSM for Aruba ClearPass Policy Manager can collect event logs from your Aruba ClearPass Policy Manager servers.

The following table identifies the specifications for the Aruba ClearPass Policy Manager DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Aruba Networks</td>
</tr>
<tr>
<td>DSM name</td>
<td>ClearPass</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-ArubaClearPass-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>6.5.0.71095 and later</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Session, Audit, System, Insight</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Aruba Networks website (<a href="http://www.arubanetworks.com/products/security/">http://www.arubanetworks.com/products/security/</a>)</td>
</tr>
</tbody>
</table>

To integrate Aruba ClearPass Policy Manager 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:
   - Aruba ClearPass DSM RPM
   - DSMCommon RPM

2. Configure your Aruba ClearPass Policy Manager device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add an Aruba ClearPass log source on the QRadar Console. The following table describes the parameters that require specific values for Aruba ClearPass Policy Manager event collection:
## Table 115. Aruba ClearPass Policy Manager log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Aruba ClearPass Policy Manager</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 Aruba ClearPass Policy Manager to communicate with QRadar

To collect syslog events from Aruba ClearPass Policy Manager, you must add an external syslog server for the QRadar host. You will then need to create one or more syslog filters for your syslog server.

**Before you begin**

For Session and Insight events, full event parsing works only for the default fields that are provided by Aruba ClearPass Policy Manager. Session and Insight events that are created by a user, and have different combinations of fields, might appear as **Unknown Session Log**, or **Unknown Insight Log**.

**Procedure**

1. Log in to your Aruba ClearPass Policy Manager server.
2. Start the Administration Console.
3. Click **External Servers > Syslog Targets**.
4. Click **Add**, and then configure the details for the QRadar host.
5. On the Administration Console, click **External Servers > Syslog Export Filters**
6. Click **Add**.
7. Select LEEF for the **Export Event Format Type**, and then select the **Syslog Server** that you added.
8. Click **Save**.

### Aruba Introspect

The IBM QRadar DSM for Aruba Introspect collects events from an Aruba Introspect device.

The following table describes the specifications for the Aruba Introspect DSM:

## Table 116. Aruba Introspect DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Aruba</td>
</tr>
<tr>
<td>DSM name</td>
<td>Aruba Introspect</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-ArubaIntrospect-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>1.6</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Name-value pair (NVP)</td>
</tr>
</tbody>
</table>
To integrate Aruba Introspect with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs, in the order that they are listed, on your QRadar Console:
   - DSMCommon RPM
   - ArubaIntrospect DSM RPM

2. Configure your Aruba Introspect device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add an Aruba Introspect log source on the QRadar Console. The following table describes the parameters that require specific values for Aruba Introspect event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Aruba Introspect</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>A unique identifier for the log source.</td>
</tr>
</tbody>
</table>

4. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

   The following table shows a sample event message for Aruba Introspect
### Table 118. Aruba Introspect sample event message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| Cloud Exfiltration  | Suspicious Activity| May 6 20:04:38 <Server>  
|                     |                    | May 7 03:04:38 lab-an-node  
|                     |                    | msg_type=alert detection_time=  
|                     |                    | "2016-05-06 20:04:23 -07:00"  
|                     |                    | alert_name="Large DropBox Upload" alert_type="Cloud Exfiltration" alert_category="Network Access" alert_severity=60  
|                     |                    | alert_confidence=20 attack_stage=Exfiltration user_name=<Username>  
|                     |                    | src_host_name=example.com  
|                     |                    | src_ip=<Source_IP_address>  
|                     |                    | dest_ip=Destination_IP_address1>, <Destination_IP_address2>,...  
|                     |                    | description="User <Username> on host example.com uploaded 324.678654 MB to Dropbox on May 05, 2016; compared with users in the whole Enterprise who uploaded an average of 22.851 KB during the same day"  
|                     |                    | alert_id=xxxxxxxxxxxxxxxxxxxxxx xxxxxxx_Large_DropBox.Upload |

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 Aruba Introspect to communicate with QRadar

Before IBM QRadar can collect events from Aruba Introspect, you must configure Aruba Introspect to send events to QRadar.

**Procedure**

1. Log in to the Aruba Introspect Analyzer.
2. Configure forwarding.
   a) Click **System Configuration > Syslog Destinations**.
   b) Configure the following forwarding parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Destination</td>
<td>IP or host name of the QRadar Event Collector.</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP or UDP</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
</tbody>
</table>

3. Configure notification.
   a) Click **System Configuration > Security Alerts / Emails > Add New**.
   b) Configure the following notification parameters:
## Table 120. Aruba Introspect Analyzer notification parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Alert Syslog Forwarding</td>
<td>Enable the Enable Alert Syslog Forwarding check box.</td>
</tr>
<tr>
<td>Sending Notification</td>
<td>As Alerts are produced.</td>
</tr>
<tr>
<td></td>
<td>You can customize this setting to send in batches instead of a live stream.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Your local time zone.</td>
</tr>
</tbody>
</table>

**Note:** Leave Query, Severity, and Confidence values as default to send all Alerts. These values can be customized to filter out and send only a subset of Alerts to QRadar.

### What to do next

To help you troubleshoot, you can look at the forwarding logs in the `/var/log/notifier.log` file.

When a new notification is created, as described in Step 3, alerts for the last week that match the Query, Severity, and Confidence fields are sent.

## Aruba Mobility Controllers

The Aruba Mobility Controllers DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant events that are forwarded by using syslog on TCP port 514 or UDP port 514.

### Configuring your Aruba Mobility Controller

You can configure the Aruba Wireless Networks (Mobility Controller) device to forward syslog events to IBM QRadar.

**Procedure**

1. Log in to Aruba Mobility Controller.
2. From the top menu, select **Configuration**.
3. From the **Switch** menu, select **Management**.
4. Click the **Logging** tab.
5. From the **Logging Servers** menu, select **Add**.
6. Type the IP address of the QRadar server that you want to collect logs.
7. Click **Add**.
8. Optional: Change the logging level for a module:
   a) Select the check box next to the name of the logging module.
   b) Choose the logging level that you want to change from the list that is displayed at the bottom of the window.
9. Click **Done**.
10. Click **Apply**.


Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Aruba Mobility Controllers.

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 Aruba Mobility Controller.
9. From the Protocol Configuration list, select Syslog.
10. In the Log Source Identifier field, type the IP address or host name for the log source.
11. Click Save.
12. On the Admin tab, click Deploy Changes.
Chapter 28. Avaya VPN Gateway

The IBM QRadar DSM for Avaya VPN Gateway can collect event logs from your Avaya VPN Gateway servers.

The following table identifies the specifications for the Avaya VPN Gateway DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Avaya Inc.</td>
</tr>
<tr>
<td>DSM</td>
<td>Avaya VPN Gateway</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-AvayaVPNGateway-7.1-799033.noarch.rpm</td>
</tr>
<tr>
<td></td>
<td>DSM-AvayaVPNGateway-7.2-799036.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>9.0.7.2</td>
</tr>
<tr>
<td>Protocol</td>
<td>syslog</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>OS, System Control Process, Traffic Processing, Startup, Configuration</td>
</tr>
<tr>
<td></td>
<td>Reload, AAA Subsystem, IPsec Subsystem</td>
</tr>
<tr>
<td>Automatically discovered</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td><a href="http://www.avaya.com">http://www.avaya.com</a></td>
</tr>
</tbody>
</table>

Avaya VPN Gateway DSM integration process

You can integrate Avaya VPN Gateway DSM with IBM QRadar.

About this task

To integrate Avaya VPN Gateway DSM with QRadar, use the following procedure:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   - Syslog protocol RPM
   - DSMCommon RPM
   - Avaya VPN Gateway RPM
2. For each instance of Avaya VPN Gateway, configure your Avaya VPN Gateway system to enable communication with QRadar.
3. If QRadar automatically discovers the log source, for each Avaya VPN Gateway server you want to integrate, create a log source on the QRadar Console.
Configuring your Avaya VPN Gateway system for communication with IBM QRadar

To collect all audit logs and system events from Avaya VPN Gateway, you must specify QRadar as the syslog server and configure the message format.

Procedure
1. Log in to your Avaya VPN Gateway command-line interface (CLI).
2. Type the following command:
   
   `/cfg/sys/syslog/add`
3. At the prompt, type the IP address of your QRadar system.
4. To apply the configuration, type the following command:
   
   `apply`
5. To verify that the IP address of your QRadar system is listed, type the following command:
   
   `/cfg/sys/syslog/list`

Configuring an Avaya VPN Gateway log source in IBM QRadar

To collect Avaya VPN Gateway 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 Avaya VPN Gateway.
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 29. BalaBit IT Security

The BalaBit Syslog-ng Agent application can collect and forward syslog events for the Microsoft Security Event Log DSM and the Microsoft ISA DSM in IBM QRadar.

BalaBit IT Security for Microsoft Windows Events

The Microsoft Windows Security Event Log DSM in IBM QRadar can accept Log Extended Event Format (LEEF) events from BalaBit's Syslog-ng Agent.

The BalaBit Syslog-ng Agent forwards the following Windows events to QRadar by using syslog:

- Windows security
- Application
- System
- DNS
- DHCP
- Custom container event logs

Before you can receive events from BalaBit IT Security Syslog-ng Agents, you must install and configure the agent to forward events.

Before you begin

Review the following configuration steps before you configure the BalaBit Syslog-ng Agent:

1. Install the BalaBit Syslog-ng Agent on your Windows host. For more information, see your BalaBit Syslog-ng Agent documentation.
2. Configure Syslog-ng Agent Events.
3. Configure QRadar as a destination for the Syslog-ng Agent.
4. Restart the Syslog-ng Agent service.
5. Optional. Configure the log source in QRadar.

Configuring the Syslog-ng Agent event source

Before you can forward events to IBM QRadar, you must specify what Windows-based events the Syslog-ng Agent collects.

Procedure

1. From the Start menu, select All Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent for Windows.
   The Syslog-ng Agent window is displayed.
2. Expand the Syslog-ng Agent Settings pane, and select Eventlog Sources.
3. Double-click Event Containers.
   The Event Containers Properties window is displayed.
4. From the Event Containers pane, select the Enable radio button.
5. Select a check box for each event type you want to collect:
   - Application - Select this check box if you want the device to monitor the Windows application event log.
   - Security - Select this check box if you want the device to monitor the Windows security event log.
• **System** - Select this check box if you want the device to monitor the Windows system event log.

**Note:** BalaBit's Syslog-ng Agent supports other event types, such as DNS or DHCP events by using custom containers. For more information, see your *BalaBit Syslog-ng Agent documentation*.

6. Click **Apply**, and then click **OK**.

The event configuration for your BalaBit Syslog-ng Agent is complete. You are now ready to configure QRadar as a destination for Syslog-ng Agent events.

### Configuring a syslog destination

The Syslog-ng Agent enables you to configure multiple destinations for your Windows based events.

**About this task**

To configure IBM QRadar as a destination, you must specify the IP address for QRadar, and then configure a message template for the LEEF format.

**Procedure**

1. From the **Start** menu, select **All Programs** > **Syslog-ng Agent for Windows** > **Configure syslog-ng Agent for Windows**.

The **Syslog-ng Agent** window is displayed.

2. Expand the **Syslog-ng Agent Settings** pane, and click **Destinations**.

3. Double-click **Add new server**.

The **Server Property** window is displayed.

4. Click the **Server** tab, and then click **Set Primary Server**.

5. Configure the following parameters:

   • **Server Name** - Type the IP address of your QRadar Console or Event Collector.
   
   • **Server Port** - Type 514 as the TCP port number for events to be forwarded to QRadar.

6. Click the **Messages** tab.

7. From the **Protocol** list, select **Legacy BSD Syslog Protocol**.

8. In the **Template** field, define a custom template message for the protocol by typing:

   ```
   <$[PRI]>$[BSDDATE] $[HOST] LEEF:$[MSG]
   ```

   The information that is typed in this field is space delimited.

9. In the **Event Message Format** pane, in the **Message Template** field, type or copy and paste the following text to define the format for the LEEF events:

   **Note:** It is suggested that you do not change the text.

   ```
   1.0|Microsoft|Windows|2k8r2|${EVENT_ID}|devTime=${R_YEAR}-${R_MONTH}-${R_DAY}T${R_HOUR}:${R_MIN}:${R_SEC}GMT${TZOFFSET} devTimeFormat=yyyy-MM-dd'T'HH:mm:ssz cat=${EVENT_TYPE} sev=${EVENT_LEVEL} resource=${HOST} usrName=${EVENT_USERNAME} application=${EVENT_SOURCE} message=${EVENT_MSG}
   ```

   **Note:** The LEEF format uses tab as a delimiter to separate event attributes from each other. However, the delimiter does not start until after the last pipe character for {Event_ID}. The following fields must include a tab before the event name: devTime, devTimeFormat, cat, sev, resource, usrName, application, and message.

   You might need to use a text editor to copy and paste the LEEF message format into the **Message Template** field.

10. Click **OK**.

The destination configuration is complete. You are now ready to restart the Syslog-ng Agent service.
Restarting the Syslog-ng Agent service
Before the Syslog-ng Agent can forward LEEF formatted events, you must restart the Syslog-ng Agent service on the Windows host.

Procedure
1. From the Start menu, select Run.
   The Run window is displayed.
2. Type the following text:
   services.msc
3. Click OK.
   The Services window is displayed.
4. In the Name column, right-click on Syslog-ng Agent for Windows, and select Restart.
   After the Syslog-ng Agent for Windows service restarts, the configuration is complete. Syslog events from the BalaBit Syslog-ng Agent are automatically discovered by IBM QRadar. The Windows events that are automatically discovered are displayed as Microsoft Windows Security Event Logs on the Log Activity tab.

Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from LEEF formatted messages.

About this task
These configuration steps are optional.

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 BalaBit Syslog-ng Agent log source.
7. In the Log Source Description field, type a description for the log source.
8. From the Log Source Type list, select Microsoft Windows Security Event Log.
10. Configure one of the following parameters from the table:

<table>
<thead>
<tr>
<th>Table 122. Syslog Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.
BalaBit IT Security for Microsoft ISA or TMG Events

You can integrate the BalaBit Syslog-ng Agent application to forward syslog events to IBM QRadar. The BalaBit Syslog-ng Agent reads Microsoft ISA or Microsoft TMG event logs, and forwards syslog events by using the Log Extended Event Format (LEEF).

The events that are forwarded by BalaBit IT Security are parsed and categorized by the Microsoft Internet and Acceleration (ISA) DSM for QRadar. The DSM accepts both Microsoft ISA and Microsoft Threat Management Gateway (TMG) events.

**Before you begin**

Before you can receive events from BalaBit IT Security Syslog-ng Agents you must install and configure the agent to forward events.

**Note:** This integration uses BalaBit's Syslog-ng Agent for Windows and BalaBit's Syslog-ng PE to parse and forward events to QRadar for the DSM to interpret.

Review the following configuration steps before you attempt to configure the BalaBit Syslog-ng Agent:

To configure the BalaBit Syslog-ng Agent, you must take the following steps:

1. Install the BalaBit Syslog-ng Agent on your Windows host. For more information, see your *BalaBit Syslog-ng Agent vendor documentation*.
2. Configure the BalaBit Syslog-ng Agent.
3. Install a BalaBit Syslog-ng PE for Linux or Unix in relay mode to parse and forward events to QRadar. For more information, see your *BalaBit Syslog-ng PE vendor documentation*.
4. Configure syslog for BalaBit Syslog-ng PE.
5. Optional. Configure the log source in QRadar.

**Configure the BalaBit Syslog-ng Agent**

Before you can forward events to IBM QRadar, you must specify the file source for Microsoft ISA or Microsoft TMG events in the Syslog-ng Agent collects.

If your Microsoft ISA or Microsoft TMG appliance is generating event files for the Web Proxy Server and the Firewall Service, both files can be added.

**Configuring the BalaBit Syslog-ng Agent file source**

Use the BalaBit Syslog-ng Agent file source to define the base log directory and files that are to be monitored by the Syslog-ng Agent.

**Procedure**

1. From the **Start** menu, select **All Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent for Windows**.
   
   The **Syslog-ng Agent** window is displayed.
2. Expand the **Syslog-ng Agent Settings** pane, and select **File Sources**.
3. Select the **Enable** radio button.
4. Click **Add** to add your Microsoft ISA and TMG event files.
5. From the **Base Directory** field, click **Browse** and select the folder for your Microsoft ISA or Microsoft TMG log files.
6. From the **File Name Filter** field, click **Browse** and select a log file that contains your Microsoft ISA or Microsoft TMG events.

   **Note:** The **File Name Filter** field supports the wild card (*) and question mark (?) characters, which help you to find log files that are replaced, when they reach a specific file size or date.
7. In the **Application Name** field, type a name to identify the application.
8. From the **Log Facility** list, select **Use Global Settings**.
9. Click **OK**.

   To add additional file sources, repeat steps 4 to 9.
10. Click **Apply**, and then click **OK**.

    The event configuration is complete. You are now ready to configure a syslog destinations and formatting for your Microsoft TMG and ISA events.

Web Proxy Service events and Firewall Service events are stored in individual files by Microsoft ISA and TMG.

### Configuring a BalaBit Syslog-ng Agent syslog destination

The event logs captured by Microsoft ISA or TMG cannot be parsed by the BalaBit Syslog-ng Agent for Windows, so you must forward your logs to a BalaBit Syslog-ng Premium Edition (PE) for Linux or UNIX.

**About this task**

To forward your TMG and ISA event logs, you must specify the IP address for your PE relay and configure a message template for the LEEF format. The BalaBit Syslog-ng PE acts as an intermediate syslog server to parse the events and to forward the information to IBM QRadar.

**Procedure**

1. From the **Start** menu, select **All Programs > syslog-ng Agent for Windows > Configure syslog-ng Agent for Windows**.

   The **Syslog-ng Agent** window is displayed.
2. Expand the **Syslog-ng Agent Settings** pane, and click **Destinations**.
3. Double-click **Add new Server**.
4. On the **Server** tab, click **Set Primary Server**.
5. Configure the following parameters:
   - For the **Server Name** type the IP address of your BalaBit Syslog-ng PE relay.
   - For the **Server Port** type 514 as the TCP port number for events that are forwarded to your BalaBit Syslog-ng PE relay.
6. Click the **Messages** tab.
7. From the **Protocol** list, select **Legacy BSD Syslog Protocol**.
8. From the **File Message Format** pane, in the **Message Template** field, type the following code:

   ```
   ${FILE_MESSAGE}${TZOFFSET}
   ```
9. Click **Apply**, and then click **OK**.

   The destination configuration is complete. You are now ready to filter comment lines from the event log.

### Filtering the log file for comment lines

The event log file for Microsoft ISA or Microsoft TMG might contain comment markers. Comments must be filtered from the event message.

**Procedure**

1. From the **Start** menu, select **All Programs > Syslog-ng Agent for Windows > Configure syslog-ng Agent for Windows**.

   The **Syslog-ng Agent** window is displayed.
2. Expand the **Syslog-ng Agent Settings** pane, and select **Destinations**.
3. Right-click on your IBM QRadar Syslog destination and select Event Filters > Properties.
   
   The Global event filters Properties window is displayed.

4. Configure the following values:
   
   • From the Global file filters pane, select Enable.
   
   • From the Filter Type pane, select Black List Filtering.

5. Click OK.

6. From the Filter List menu, double-click Message Contents.
   
   The Message Contents Properties window is displayed.

7. From the Message Contents pane, select Enable.

8. In the Regular Expression field, type the following regular expression:
   
   ^#

9. Click Add.

10. Click Apply, and then click OK.

   The event messages with comments are no longer forwarded.

   Note: You might need to restart Syslog-ng Agent for Windows service to begin syslog forwarding. For more information, see your BalaBit Syslog-ng Agent documentation.

### Configuring a BalaBit Syslog-ng PE Relay

The BalaBit Syslog-ng Agent for Windows sends Microsoft TMG and ISA event logs to a Balabit Syslog-ng PE installation, which is configured in relay mode.

#### About this task

The relay mode installation is responsible for receiving the event log from the BalaBit Syslog-ng Agent for Windows, parsing the event logs in to the LEEF format, then forwarding the events to IBM QRadar by using syslog.

To configure your BalaBit Syslog-ng PE Relay, you must:

1. Install BalaBit Syslog-ng PE for Linux or Unix in relay mode. For more information, see your BalaBit Syslog-ng PE vendor documentation.

2. Configure syslog on your Syslog-ng PE relay.

   The BalaBit Syslog-ng PE formats the TMG and ISA events in the LEEF format based on the configuration of your syslog.conf file. The syslog.conf file is responsible for parsing the event logs and forwarding the events to QRadar.

#### Procedure

1. Using SSH, log in to your BalaBit Syslog-ng PE relay command-line interface (CLI).

2. Edit the following file:

   `/etc/syslog-ng/etc/syslog.conf`

3. From the destinations section, add an IP address and port number for each relay destination.

   For example,

   ```
   # destinations destination d_messages { file("/var/log/messages"); };
   destination d_remote_tmfgfw { tcp("QRadar_IP" port(QRadar_PORT) log_disk_fifo_size(10000000) template(t_tmfgfw)); };
   destination d_remote_tmgweb { tcp("QRadar_IP" port(QRadar_PORT) log_disk_fifo_size(10000000) template(t_tmgweb)); };
   
   Where:
   
   QRadar_IP is the IP address of your QRadar Console or Event Collector.
   ```
QRadar_Port is the port number that is required for QRadar to receive syslog events. By default, QRadar receives syslog events on port 514.

4. Save the syslog configuration changes.
5. Restart Syslog-ng PE to force the configuration file to be read.

The BalaBit Syslog-ng PE configuration is complete. Syslog events that are forwarded from the BalaBit Syslog-ng relay are automatically discovered by QRadar as Microsoft Windows Security Event Logs on the Log Activity tab. For more information, see the IBM QRadar Users Guide.

**Note:** When you are using multiple syslog destinations, messages are considered to be delivered when they successfully arrive at the primary syslog destination.

### Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from LEEF formatted messages that are provided by your BalaBit Syslog-ng relay.

**About this task**

The following configuration steps are optional.

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   
   The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
   
   The **Log Sources** window is displayed.
5. Click **Add**.
   
   The **Add a log source** window is displayed.
6. In the **Log Source Name** field, type a name for the log source.
7. In the **Log Source Description** field, type a description for the log source.
8. From the **Log Source Type** list, select Microsoft **ISA**.
9. From the **Protocol Configuration** list, select **Syslog**.

   The **Syslog Protocol Configuration** is displayed.
10. Configure one of the following parameters from the table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for Microsoft ISA or Microsoft Threat Management Gateway events from the BalaBit Syslog-ng Agent.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

   The BalaBit IT Security configuration for Microsoft ISA and Microsoft TMG events is complete.
Chapter 30. Barracuda

IBM QRadar supports a range of Barracuda devices.
The devices QRadar supports are:

- “Barracuda Spam & Virus Firewall” on page 231
- “Barracuda Web Application Firewall” on page 232
- “Barracuda Web Filter” on page 234

Barracuda Spam & Virus Firewall

You can integrate Barracuda Spam & Virus Firewall with IBM QRadar.
The Barracuda Spam & Virus Firewall DSM for QRadar accepts both mail syslog events and web syslog events from Barracuda Spam & Virus Firewall appliances.

Mail syslog events contain the event and action that is taken when the firewall processes email. Web syslog events record information on user activity, and configuration changes that occur on your Barracuda Spam & Virus Firewall appliance.

Before you begin
Syslog messages are sent to QRadar from Barracuda Spam & Virus Firewall by using UDP port 514. You must verify that any firewalls between QRadar and your Barracuda Spam & Virus Firewall appliance allow UDP traffic on port 514.

Configuring syslog event forwarding
You can configure syslog forwarding for Barracuda Spam & Virus Firewall.

Procedure
1. Log in to the Barracuda Spam & Virus Firewall web interface.
2. Click the Advanced tab.
3. From the Advanced menu, select Advanced Networking.
4. In the Mail Syslog field, type the IP address of your QRadar Console or Event Collector.
5. Click Add.
6. In the Web Interface Syslog field, type the IP address of your QRadar Console or Event Collector.
7. Click Add.

Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Barracuda Spam & Virus Firewall appliances.

About this task
The following configuration steps are optional.

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.
5. In the **Log Source Name** field, type a name for your log source.
6. In the **Log Source Description** field, type a description for the log source.
7. From the **Log Source Type** list, select **Barracuda Spam & Virus Firewall**.
8. From the **Protocol Configuration** list, select **Syslog**.
9. In the **Log Source Identifier** field, type the IP address or host name for the log source.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

### Barracuda Web Application Firewall

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Barracuda</td>
</tr>
<tr>
<td>DSM name</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-BarracudaWebApplicationFirewall-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V7.0.x and later</td>
</tr>
<tr>
<td>Protocol type</td>
<td>Syslog</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>System, Web, Access, Audit</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>If LEEF-formatted payloads, the log source is automatically discovered. If custom-formatted payloads, the log source is not automatically discovered.</td>
</tr>
<tr>
<td>Included identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td>Barracuda Networks website (<a href="https://www.barracuda.com">https://www.barracuda.com</a>)</td>
</tr>
</tbody>
</table>

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 125. Barracuda Web Application Firewall log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Barracuda Web Application Firewall</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

---

**Configuring Barracuda Web Application Firewall to send syslog events to QRadar**

Configure your Barracuda Web Application Firewall appliance to send syslog events to IBM 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the QRadar Console or Event Collector</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>The IP address of your QRadar Console or Event Collector.</td>
</tr>
<tr>
<td>Port</td>
<td>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.</td>
</tr>
<tr>
<td>Connection Type</td>
<td>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.</td>
</tr>
<tr>
<td>Validate Server Certificate</td>
<td>No</td>
</tr>
</tbody>
</table>

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**.

**Configuring Barracuda Web Application Firewall to send syslog events to QRadar for devices that do not support LEEF**

If your device does not support LEEF, you can configure syslog forwarding for Barracuda Web Application Firewall.

**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 **Syslog Settings**.
5. Configure a syslog facility value for the following options:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Firewall Logs Facility</td>
<td>Select a syslog facility between Local0 and Local7.</td>
</tr>
<tr>
<td>Access Logs Facility</td>
<td>Select a syslog facility between Local0 and Local7.</td>
</tr>
<tr>
<td>Audit Logs Facility</td>
<td>Select a syslog facility between Local0 and Local7.</td>
</tr>
<tr>
<td>System Logs Facility</td>
<td>Select a syslog facility between Local0 and Local7.</td>
</tr>
</tbody>
</table>

Setting a syslog unique facility for each log type allows the Barracuda Web Application Firewall to divide the logs into different files.

6. Click **Save Changes**.
7. In the **Name** field, type the name of the syslog server.
8. In the **Syslog** field, type the IP address of your QRadar Console or Event Collector.
9. From the **Log Time Stamp** option, select **Yes**.
10. From the **Log Unit Name** option, select **Yes**.
11. Click **Add**.
12. From the **Web Firewall Logs Format** list box, select **Custom Format**.
13. In the **Web Firewall Logs Format** field, type the following custom event format:
    \[t=%t|ad=%ad|ci=%ci|cp=%cp|au=%au\]
14. From the **Access Logs Format** list box, select **Custom Format**.
15. In the **Access Logs Format** field, type the following custom event format:
    \[t=%t|p=%p|s=%s|id=%id|ai=%ai|ap=%ap|ci=%ci|cp=%cp|si=%si|sp=%sp|cu=%cu\]
16. From the **Access Logs Format** list box, select **Custom Format**.
17. In the **Access Logs Format** field, type the following custom event format:
    \[t=%t|trt=%trt|an=%an|li=%li|lp=%lp\]
18. Click **Save Changes**.
19. From the navigation menu, select **Basic > Administration**
20. From the System/Reload/Shutdown pane, click **Restart**.

**Results**
The syslog configuration is complete after your Barracuda Web Application Firewall restarts. Events that are forwarded to QRadar by Barracuda Web Application Firewall are displayed on the **Log Activity** tab.

**Barracuda Web Filter**

You can integrate Barracuda Web Filter appliance events with IBM QRadar.

The Barracuda Web Filter DSM for IBM QRadar accepts web traffic and web interface events in syslog format that are forwarded by Barracuda Web Filter appliances.

Web traffic events contain the events, and any actions that are taken when the appliance processes web traffic. Web interface events contain user login activity and configuration changes to the Web Filter appliance.

**Before you begin**
Syslog messages are forward to QRadar by using UDP port 514. You must verify that any firewalls between QRadar and your Barracuda Web Filter appliance allow UDP traffic on port 514.
Configuring syslog event forwarding

Configure syslog forwarding for Barracuda Web Filter.

Procedure
1. Log in to the Barracuda Web Filter web interface.
2. Click the Advanced tab.
3. From the Advanced menu, select Syslog.
4. From the Web Traffic Syslog field, type the IP address of your QRadar Console or Event Collector.
5. Click Add.
6. From the Web Interface Syslog field, type the IP address of your QRadar Console or Event Collector.
7. Click Add.

The syslog configuration is complete.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Barracuda Web Filter appliances.

About this task

The following configuration steps are optional.

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 Barracuda Web Filter.
10. Configure one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for</td>
</tr>
<tr>
<td></td>
<td>events from your Barracuda Web Filter appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The log source is added to QRadar. Events that are forwarded by Barracuda Web Filter are displayed on the Log Activity tab of QRadar.
Chapter 31. BeyondTrust PowerBroker

The IBM QRadar DSM for BeyondTrust PowerBroker logs all events to a multi-line format in a single event log that is viewed by using Beyond Trust's pblog utility.

To integrate BeyondTrust PowerBroker with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the BeyondTrust PowerBroker DSM RPM on your QRadar Console.

2. Configure BeyondTrust PowerBroker to communicate with QRadar. See Configuring BeyondTrust PowerBroker to communicate with QRadar.

3. If QRadar does not automatically detect the log source, add a BeyondTrust PowerBroker log source on the QRadar Console. The following tables describe the parameters that require specific values for BeyondTrust PowerBroker event collection:

<table>
<thead>
<tr>
<th>Table 127. Syslog log source parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>
| Store Event Payload               | Select this check box to enable or disable QRadar from storing the event payload.  
Automatically discovered log sources use the default value from the Store Event Payload list in the System Settings window, which is accessible on the Admin tab. However, when you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source. |

For more information about Syslog log source parameters, see Adding a log source.

<table>
<thead>
<tr>
<th>Table 128. TLS syslog log source parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

For more information about TLS syslog log source parameters, see TLS syslog protocol configuration options.

Related concepts
“TLS syslog protocol configuration options” on page 93
Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

“BeyondTrust PowerBroker DSM specifications” on page 239
The following table describes the specifications for the BeyondTrust PowerBroker DSM.

“Sample event messages” on page 240
Use these sample event messages as a way of verifying a successful integration with QRadar.

**Related tasks**
- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 BeyondTrust PowerBroker to communicate with QRadar” on page 238

BeyondTrust pblogs must be reformatted by using a script and then forwarded to IBM QRadar. You need to download and configure a script for your BeyondTrust PowerBroker appliance before you can forward events to QRadar.

### Configuring BeyondTrust PowerBroker to communicate with QRadar

BeyondTrust pblogs must be reformatted by using a script and then forwarded to IBM QRadar. You need to download and configure a script for your BeyondTrust PowerBroker appliance before you can forward events to QRadar.

**Procedure**

1. Download the following file from the IBM support website (http://www.ibm.com/support):
   
   `pbforwarder.pl.gz`

2. Copy the file to the device that hosts BeyondTrust PowerBroker.

   **Note:** Perl 5.8 must be installed on the device that hosts BeyondTrust PowerBroker.

3. Type the following command to extract the file:

   `gzip -d pbforwarder.pl.gz`

4. Type the following command to set the script file permissions:

   `chmod +x pbforwarder.pl`

5. Use SSH to log in to the device that hosts BeyondTrust PowerBroker.

   The credentials that are used need to have read, write, and execute permissions for the log file.

6. Type the appropriate command parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>The <code>-h</code> parameter defines the syslog host that receives the events from BeyondTrust PowerBroker. This is the IP address of your QRadar Console or QRadar Event Collector.</td>
</tr>
<tr>
<td>-t</td>
<td>The <code>-t</code> parameter defines that the command-line is used to tail the log file and monitor for new output from the listener. For PowerBroker, this command must be specified as &quot;pblog -l -t&quot;.</td>
</tr>
<tr>
<td>-p</td>
<td>The <code>-p</code> parameter defines the TCP port to be used when forwarding events. If nothing is specified, the default is port 514.</td>
</tr>
<tr>
<td>-H</td>
<td>The <code>-H</code> parameter defines the host name or IP address for the syslog header of all sent events. This should be the IP address of the BeyondTrust PowerBroker.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>-r</td>
<td>The -r parameter defines the directory name where you want to create the process ID (.pid) file. The default is /var/run. This parameter is ignored if -D is specified.</td>
</tr>
<tr>
<td>-l</td>
<td>The -l parameter defines the directory name where you want to create the lock file. The default is /var/lock. This parameter is ignored if -D is specified.</td>
</tr>
<tr>
<td>-D</td>
<td>The -D parameter defines that the script runs in the foreground. The default setting is to run as a daemon and log all internal messages to the local syslog server.</td>
</tr>
<tr>
<td>-f</td>
<td>The -f parameter defines the syslog facility and optionally, the severity for messages that are sent to the Event Collector. If no value is specified, user.info is used.</td>
</tr>
<tr>
<td>-a</td>
<td>The -a parameter enables an AIX® compatible ps method. This command is only needed when you run BeyondTrust PowerBroker on AIX systems.</td>
</tr>
<tr>
<td>-d</td>
<td>The -d parameter enables debug logging.</td>
</tr>
<tr>
<td>-v</td>
<td>The -v parameter displays the script version information.</td>
</tr>
</tbody>
</table>

7. Type the following command to start the pbforwarder.pl script:
   
   pbforwarder.pl -h <IP address> -t "pblog -l -t"
   
   Where <IP address> is the IP address of your QRadar or Event Collector.

8. Type the following command to stop the pbforwarder.pl script:
   
   kill -QUIT `cat /var/run/pbforwarder.pl.pid`

9. Type the following command to reconnect the pbforwarder.pl script:
   
   kill -HUP `cat /var/run/pbforwarder.pl.pid`

   QRadar automatically detects and creates a log source from the syslog events that are forwarded from a BeyondTrust PowerBroker.

### BeyondTrust PowerBroker DSM specifications

The following table describes the specifications for the BeyondTrust PowerBroker DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>BeyondTrust</td>
</tr>
<tr>
<td>DSM name</td>
<td>BeyondTrust PowerBroker</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-BeyondTrustPowerBroker-QRadar_version-build_number.noarch.rpm</td>
</tr>
</tbody>
</table>
### Table 130. BeyondTrust PowerBroker DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported versions</td>
<td>4.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog, TLS syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>System, Application</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>BeyondTrust web page [<a href="https://www.beyondtrust.com/products/powerbroker/">https://www.beyondtrust.com/products/powerbroker/</a>]</td>
</tr>
</tbody>
</table>

### Sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following tables provide sample event messages for the BeyondTrust PowerBroker DSM:

#### Table 131. BeyondTrust PowerBroker sample syslog message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finish pbrun terminated</td>
<td>Information</td>
<td><code>&lt;14&gt;Feb 15 13:23:09 qradar4292 pbforwarder.pl: DEVICETYPE = PowerBroker EVENTID = PB EVENTCAT = unknown DDATE = USER = SRC = DST = EVENT_HEADER = ac15208e4eaddff b1BB002 Finish pbrun terminated: signal 1 (Hangup) unknown signal code event = &quot;Finish&quot; exitdate = &quot;2011/10/30&quot; exitstatus = &quot;pbrun terminated: signal 1 (Hangup) unknown signal code&quot; exittime = &quot;21:01:49&quot; i18n_exitdate = &quot;10/30/11&quot; i18n_exittime = &quot;21:01:49&quot; logpid = 22085786 uniqueid = &quot;ac15208e4eadfffb1BB002&quot;</code></td>
</tr>
</tbody>
</table>

---

240 IBM QRadar : QRadar DSM Configuration Guide
Chapter 32. BlueCat Networks Adonis

The BlueCat Networks Adonis DSM for IBM QRadar accepts events that are forwarded in Log Enhanced Event Protocol (LEEF) by using syslog from BlueCat Adonis appliances that are managed with BlueCat Proteus.

QRadar supports BlueCat Networks Adonis appliances by using version 6.7.1-P2 and later.

You might be required to include a patch on your BlueCat Networks Adonis to integrate DNS and DHCP events with QRadar. For more information, see KB-4670 and your BlueCat Networks documentation.

Supported event types

IBM QRadar is capable of collecting all relevant events related to DNS and DHCP queries. This includes the following events:

• DNS IPv4 and IPv6 query events
• DNS name server query events
• DNS mail exchange query events
• DNS text record query events
• DNS record update events
• DHCP discover events
• DHCP request events
• DHCP release events

Event type format

The LEEF format consists of a pipe (|) delimited syslog header and a space delimited event payload. For example:

Aug 10 14:55:30 <Server> LEEF:1.0|BCN|Adonis|6.7.1|DNS_Query|cat=A_record|src=<Source_IP_address> url=test.example.com

If the syslog events forwarded from your BlueCat Adonis appliances are not formatted similarly to the sample above, you must examine your device configuration. Properly formatted LEEF event messages are automatically discovered by the BlueCat Networks Adonis DSM and added as a log source to IBM QRadar.

Before you begin

BlueCat Adonis must be configured to generate events in Log Enhanced Event Protocol (LEEF) and to redirect the event output to QRadar using syslog.

BlueCat Networks provides a script on their appliances to assist you with configuring syslog. To complete the syslog redirection, you must have administrative or root access to the command line interface of the BlueCat Adonis or your BlueCat Proteus appliance. If the syslog configuration script is not present on your appliance, contact your BlueCat Networks representative.
Configuring BlueCat Adonis

You can configure your BlueCat Adonis appliance to forward DNS and DHCP events to IBM QRadar SIEM.

**Procedure**

1. Using SSH, log in to your BlueCat Adonis appliance.
2. On the command-line interface type the following command to start the syslog configuration script:
   
   ```bash
   /usr/local/bluecat/QRadar/setup-QRadar.sh
   ```
3. Type the IP address of your QRadar Console or Event Collector.
4. Type yes or no to confirm the IP address.

   The configuration is complete when a success message is displayed.

   The log source is added to QRadar as BlueCat Networks Adonis syslog events are automatically discovered. Events that are forwarded to QRadar are displayed on the **Log Activity** tab. If the events are not automatically discovered, you can manually configure a log source.

Configuring a log source in IBM QRadar

IBM QRadar automatically discovers and creates a log source for syslog events from BlueCat Networks Adonis. However, you can manually create a log source for QRadar to receive syslog events.

**About this task**

The following configuration steps are optional.

**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 **BlueCat Networks Adonis**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type the IP address or host name for the log source as an identifier for events from your BlueCat Networks Adonis appliance.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

   The configuration is complete.
Chapter 33. Blue Coat

IBM QRadar supports a range of Blue Coat products.

Blue Coat SG

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Blue Coat</td>
</tr>
<tr>
<td>DSM name</td>
<td>Blue Coat SG Appliance</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-BlueCoatProxySG-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>SG v4.x and later</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>Log File Protocol</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td>Blue Coat website (<a href="http://www.bluecoat.com">http://www.bluecoat.com</a>)</td>
</tr>
</tbody>
</table>

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 either 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 Blue Coat SG specific parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Blue Coat SG Appliance</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Select either Log File or Syslog</td>
</tr>
</tbody>
</table>

The instructions provided describe how to configure Blue Coat SG using a custom name-value pair format. However, QRadar supports the following formats:
To use the custom log format that you created for IBM QRadar, you must associate the custom log format to a facility.

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

Configuring a Blue Coat SG Log Source
You can manually configure a Blue Coat SG log source in QRadar.

Configuring Blue Coat SG for FTP uploads
To collect Blue Coat SG events using FTP, configure the Blue Coat SC to upload events to a FTP server using the Blue Coat upload client.

Configuring Blue Coat SG for syslog
To allow syslog event collection, you must configure your Blue Coat SG appliance to forward syslog events to IBM 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.
4. Type a format name for the custom format.
5. Select Custom format string.
6. Type the following custom format:

```
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)
```

Attention: The line breaks 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.
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 250.

**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 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Name</td>
<td>A name for the log facility.</td>
</tr>
<tr>
<td>Log Format</td>
<td>The custom format you that created.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the log facility.</td>
</tr>
</tbody>
</table>

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 > Visual Policy 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

Configuring Blue Coat SG for FTP uploads
To collect Blue Coat SG events using FTP, configure the Blue Coat SC to upload events to a FTP server using the Blue Coat upload client.

Procedure
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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The IP address of the FTP server that you want to forward the Blue Coat events.</td>
</tr>
<tr>
<td>Port</td>
<td>The FTP port number.</td>
</tr>
<tr>
<td>Path</td>
<td>The directory path for the log files.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name to access the FTP server.</td>
</tr>
</tbody>
</table>
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 a Blue Coat SG Log Source
You can manually configure a Blue Coat SG log source in QRadar.

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. From the Log Source Type list, select the Blue Coat SG Appliance option.
8. From the Protocol Configuration list, select the Log File option.
9. Configure the following values:
### Table 135. Blue Coat SG log file protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>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.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. The underlying protocol that is 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.</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>Type the IP address or host name of the device that stores your event log files.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 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.</td>
</tr>
<tr>
<td>Remote User</td>
<td>Type the user name necessary to log in to the host that contains your event files. The user name can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Type the password necessary to log in to the host.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password necessary to log in to the host.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>If you select SCP or SFTP as the Service Type, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the Remote Password field is ignored.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>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 are 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.</td>
</tr>
<tr>
<td>Recursive</td>
<td>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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| FTP File Pattern          | If you select SFTP or FTP as the Service Type, this option gives you the option to configure the regular expression (regex) required to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing. The FTP file pattern that you specify must match the name you assigned to your event files. For example, to collect files that end with .log, type the following: 
  
  .*\.log
  
  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/](http://download.oracle.com/javase/tutorial/essential/regex/) |
| FTP Transfer Mode         | This option appears only if you select FTP as the Service Type. The FTP Transfer Mode parameter gives you the option 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: 
  
  You must select **NONE** for the Processor parameter and **LINEBYLINE** the Event Generator parameter when you use ASCII as the FTP 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. 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. |
<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>If the files located 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 processed.</td>
</tr>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>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.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>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.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>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.</td>
</tr>
</tbody>
</table>

10. Click **Save**.

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

### Configuring Blue Coat SG for syslog

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

**Before you begin**

**Note:** 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**.

---

**Table 135. Blue Coat SG log file protocol parameters (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>If the files located 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 processed.</td>
</tr>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>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.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>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.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 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>
<thead>
<tr>
<th>Table 136. Custom Format examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blue Coat ELFF Parameter</strong></td>
</tr>
<tr>
<td>sc-bytes</td>
</tr>
<tr>
<td>rs(Content-type)</td>
</tr>
</tbody>
</table>

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

Blue Coat Web Security Service

The IBM QRadar DSM for Blue Coat Web Security Service collects events from the Blue Coat Web Security Service.

The following table describes the specifications for the Blue Coat Web Security Service DSM:

<table>
<thead>
<tr>
<th>Table 137. Blue Coat Web Security Service DSM specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Specification</strong></td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>DSM name</td>
</tr>
<tr>
<td>RPM file name</td>
</tr>
<tr>
<td>Event format</td>
</tr>
<tr>
<td>Recorded event types</td>
</tr>
<tr>
<td>Automatically discovered?</td>
</tr>
<tr>
<td>Includes identity?</td>
</tr>
<tr>
<td>Includes custom properties?</td>
</tr>
<tr>
<td>More information</td>
</tr>
</tbody>
</table>

To integrate Blue Coat Web Security Service 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:
   - Protocol Common RPM
   - Blue Coat Web Security Service REST API Protocol RPM
   - Blue Coat Web Security Service DSM RPM
2. Configure Blue Coat Web Security Service to allow QRadar access to the Sync API.
3. Add a Blue Coat Web Security Service log source on the QRadar Console. The following table describes the parameters that require specific values for Blue Coat Web Security Service event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| Protocol Configuration            | The protocol that is used to receive events from the Blue Coat Web Security Service. You can specify the following protocol configuration options:  
|                                   | Blue Coat Web Security Service REST API (recommended)  
|                                   | Forwarded                                                                                   |
| API Username                      | The API user name that is used for authenticating with the Blue Coat Web Security Service. The API user name is configured through the Blue Coat Threat Pulse Portal. |
| Password                          | The password that is used for authenticating with the Blue Coat Web Security Service.     |
| Confirm Password                  | The password that is used for authenticating with the Blue Coat Web Security Service.     |
| Use Proxy                         | When you configure a proxy, all traffic for the log source travels through the proxy for QRadar to access the Blue Coat Web Security Service.  
|                                   | Configure the Proxy IP or Hostname, 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. |
| Automatically Acquire Server Certificate(s) | Select Yes for QRadar to automatically download the server certificate and begin trusting the target server. |
| Recurrence                        | You can specify the frequency of data collection. The format is M/H/D for Minutes/Hours/Days. The default is 5 M. |
| EPS Throttle                       | The upper limit for the maximum number of events per second (EPS). The default is 5000.   |

**Related tasks**

“Adding a log source” on page 4  
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 DSM” on page 4
Configuring Blue Coat Web Security Service to communicate with QRadar

To collect events from Blue Coat Web Security Service, you must create an API key for IBM QRadar. If an API key exists, Blue Coat Web Security Service is already configured.

Procedure
1. Log in to the Blue Coat Threat Pulse portal.
2. Switch to Service mode.
3. Click Account Maintenance > MDM, API Keys.
4. Click Add API key, type a user name and password for the API key, and then click Add.

You need the user name and password when you configure the log source for the API.
Chapter 34. Box

The IBM QRadar DSM for Box collects enterprise events from a Box enterprise account. The following table describes the specifications for the Box DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Box</td>
</tr>
<tr>
<td>DSM name</td>
<td>Box</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-BoxBox-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Box REST API</td>
</tr>
<tr>
<td>Event format</td>
<td>JSON</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Administrator and enterprise events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Box website (<a href="https://www.box.com/">https://www.box.com/</a>)</td>
</tr>
</tbody>
</table>

To integrate Box 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 in the order that they are listed:
   - Protocol Common RPM
   - Box REST API Protocol RPM
   - Box DSM RPM
2. Configure your Box enterprise account for API access.
3. The following table describes the parameters that require specific values for Box event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Box</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Box REST API</td>
</tr>
<tr>
<td>Client ID</td>
<td>Generated in the OAuth2 parameters pane of the Box administrator configuration.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Generated in the OAuth2 parameters pane of the Box administrator configuration.</td>
</tr>
<tr>
<td>Key ID</td>
<td>Generated in the Public Key Management pane after you submit the public key.</td>
</tr>
<tr>
<td>Enterprise ID</td>
<td>Used for access token request.</td>
</tr>
</tbody>
</table>
Table 140. Box log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Key File Name</td>
<td>The private key file name in the /opt/qradar/conf/trusted_certificates/box/ directory in QRadar.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses the Box API, by using a proxy, select the Use Proxy check box. If the proxy requires authentication, configure the Proxy Server, Proxy Port, Proxy Username, and Proxy Password fields. If the proxy does not require authentication, configure the Proxy Server and Proxy Port fields.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second. The default is 5000.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The time interval between log source queries to the Box API for new events. The time interval can be in hours (H), minutes (M), or days (D). The default is 10 minutes.</td>
</tr>
</tbody>
</table>

The following table shows a sample event message for Box:

Table 141. Box enterprise sample event message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGIN</td>
<td>User Login Success</td>
<td>{&quot;source&quot;:{&quot;type&quot;:&quot;user&quot;,&quot;id&quot;: &quot;&lt;UserID&gt;&quot;}, &quot;created_by&quot;:{&quot;type&quot;:&quot;user&quot;, &quot;id&quot;: &quot;&lt;UserID&gt;&quot;}, &quot;created_at&quot;: &quot;2016-01-07T10:54:30-08:00&quot;, &quot;event_id&quot;: &quot;363714450&quot;, &quot;event_type&quot;: &quot;LOGIN&quot;, &quot;ip_address&quot;: &quot;&lt;IP_address&gt;&quot;, &quot;type&quot;: &quot;event&quot;, &quot;session_id&quot;: null, &quot;additional_details&quot;:null}</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Box to communicate with QRadar**

To retrieve administrator logs from your Box enterprise account, you must configure Box and your IBM QRadar Console.

**Before you begin**

You must have a developer account.

Generate a private/public RSAkey pair for the JSON Web Token (JWT) assertion.

1. Open an SSH session to the QRadar Console.
   
   • For a private key, type the following command:
     
     ```bash
     openssl genrsa -out box_private_key.pem 2048
     ```
   
   • For a public key, type the following command:
     
     ```bash
     openssl rsa -pubout -in box_private_key.pem -out box_public_key.pem
     ```
   
   **Note:**

   Save a copy of the public key. You are required to paste the contents of the public key into the Add Public Key text box when you configure Box for API access.

   • Convert the private key to DER by typing the following command on one line:
     
     ```bash
     openssl pkcs8 -topk8 -inform PEM -outform DER -in box_private_key.pem -out box_private_key.der -nocrypt
     ```

   2. Store the private key in QRadar.
      
      a. Create a directory that is named box in the opt/qradar/conf/trusted_certificates/ directory in QRadar.
      
      b. Copy the private key .DER file to the opt/qradar/conf/trusted_certificates/box directory that you created. Do not store the private key in any other location.
      
      c. Configure the log source by using only the file name of the private key file in the opt/qradar/conf/trusted_certificates/box directory. Ensure that you type the file name correctly in the Private Key File Name field when you configure the log source.

      **Important:** Copy the private key to the opt/qradar/conf/trusted_certificates/box directory before you configure the log source. If you configure the log source before you store the private key, an error message is displayed.

**Procedure**

1. Log in to the Box Developers portal (http://developers.box.com/). You will now have access to the Admin and Box Consoles.
   
   a) Create an application for your QRadar appliance by clicking Create New App.
   
   b) Select Enterprise Integration, and then click Next.
   
   c) In the Authentication Method pane, select OAuth2.0 with JWT (Server Authentication), and then click Next.
   
   d) In the field, type a name for the App, and then click create App.
   
   e) Click View Your App.
   
   f) From the OAuth2 parameters pane, copy and record the client ID and the client secret. You need the client ID and the client secret when you add a log source in QRadar.

Chapter 34. Box 255
g) In the Application Access pane, select **Enterprise** property, and then configure the following parameters.

<table>
<thead>
<tr>
<th>Table 142. User Access Settings parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Authentication Type:</td>
</tr>
<tr>
<td>User Access:</td>
</tr>
<tr>
<td>Scopes:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

2. Submit the public key, and then generate the key ID.
   
   a) From the navigation menu, select **Configuration**.
   b) From the **Add and Manage Public Keys** list, select **Add a Public Key**.
   c) Open the public key file that you copied from QRadar, and then paste the contents of the public key file in the **Add Public Key** text box.
   d) Click **Verify and Save**, and then copy and record the **key ID**. You will need the **key ID** when you add the log source in QRadar.
   e) To ensure that the properties are stored on the server, scroll to the bottom of the page and then click **Save**.

3. Record your Box Enterprise ID.
   
   a) Log in to the Admin Console, and then click **Account Settings > Business Settings**.
   b) To locate your Enterprise ID, click the **Account Info** tab.

4. Authorize your application.
   
   a) Log in to the Box Console, and then click **Account Settings > Business Settings**.
   b) Click the **Apps** tab.
   c) In the **Custom Applications** pane, click **Authorize New App**.
   d) In the **App Authorization** window, type the API key, and then click **Next**. Verify that the access level is **All Users**. The API key is the **client ID** that you recorded.
   e) Click **Authorize**.

   For more information about configuring Box to communicate with QRadar, see the Box website [https://docs.box.com/docs/configuring-box-platform](https://docs.box.com/docs/configuring-box-platform).

**What to do next**

Verify that QRadar is configured to receive events from your Box DSM. If QRadar is configured correctly, no error messages appear in the **Edit a log source** window.
Chapter 35. Bridgewater

The Bridgewater Systems DSM for IBM QRadar accepts events by using syslog.
QRadar records all relevant events that are forwarded from Bridgewater AAA Service Controller devices by using syslog.

Configuring Syslog for your Bridgewater Systems Device

You must configure your Bridgewater Systems appliance to send syslog events to IBM QRadar.

Procedure

1. Log in to your Bridgewater Systems device command-line interface (CLI).
2. To log operational messages to the RADIUS and Diameter servers, open the following file:
   /etc/syslog.conf
3. To log all operational messages, uncomment the following line:
   local1.info /WideSpan/logs/oplog
4. To log error messages only, change the local1.info /WideSpan/logs/oplog line to the following line:
   local1.err /WideSpan/logs/oplog
   **Note:** RADIUS and Diameter system messages are stored in the /var/adm/messages file.
5. Add the following line:
   local1.*@<IP address>
   Where <IP address> is the IP address your QRadar Console.
6. The RADIUS and Diameter server system messages are stored in the /var/adm/messages file. Add the following line for the system messages:
   <facility>*@<IP address>
   Where:
   <facility> is the facility that is used for logging to the /var/adm/messages file.
   <IP address> is the IP address of your QRadar Console.
7. Save and exit the file.
8. Send a hang-up signal to the syslog daemon to make sure that all changes are enforced:
   kill -HUP `cat /var/run/syslog.pid`
   The configuration is complete. The log source is added to QRadar as Bridgewater Systems appliance events are automatically discovered. Events that are forwarded to QRadar by your Bridgewater Systems appliance are displayed on the Log Activity tab.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from a Bridgewater Systems appliance.

About this task

The following configuration steps are optional.
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 Bridgewater Systems AAA Service Controller.
9. From the Protocol Configuration list, select Syslog.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Bridgewater Systems appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

   The configuration is complete.
IBM QRadar can collect and categorize syslog system and audit events from Brocade switches and appliances that use Fabric OS V7.x.

To collect syslog events, you must configure your switch to forward syslog events. Each switch or appliance must be configured to forward events.

Events that you forward from Brocade switches are automatically discovered. A log source is configured for each switch or appliance that forwards events to QRadar.

**Configuring syslog for Brocade Fabric OS appliances**

To collect events, you must configure syslog on your Brocade appliance to forward events to IBM QRadar.

**Procedure**

1. Log in to your appliance as an admin user.
2. To configure an address to forward syslog events, type the following command:
   ```
   syslogdipadd <IP address>
   ```
   Where `<IP address>` is the IP address of the QRadar Console, Event Processor, Event Collector, or all-in-one system.
3. To verify the address, type the following command:
   ```
   syslogdipshow
   ```

**Results**

As the Brocade switch generates events the switch forwards events to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded by the Brocade appliance. It typically takes a minimum of 25 events to automatically discover a log source.

**What to do next**

Administrators can log in to the QRadar Console and verify that the log source is created on the QRadar Console and that the Log Activity tab displays events from the Brocade appliance.
Chapter 37. CA Technologies

IBM QRadar supports a number of CA Technologies DSMs.

CA ACF2

The CA Access Control Facility (ACF2) DSM collects events from a CA Technologies ACF2 image on an IBM z/OS mainframe by using IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.

To collect CA ACF2 events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html).

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 (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).

3. Create a log source in QRadar for CA ACF2.

4. If you want to create a custom event property for CA ACF2 in QRadar, for more information, see the IBM Security Custom Event Properties for IBM z/OS technical note (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf).

Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.

- The SCKRLOAD library must be APF-authorized.

- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html).

- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.

- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.

- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Create a log source for near real-time event feed
The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:
- IBM z/OS
- IBM CICS®
- IBM RACF®
- IBM DB2
- CA Top Secret
- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Select your DSM name from the list.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>

Creating a log source for Log File protocol
The Log File protocol enables IBM QRadar to retrieve archived log files from a remote host for the IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, and CA ACF2 DSM’s.

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 z/OS with zSecure writes log files to a specified directory as gzip archives. 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 that uses the Log File protocol. QRadar requires credentials to log in to the system that hosts your LEEF formatted event files and a polling interval.

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click **Add**.
5. In the **Log Source Name** field, type a name for the log source.
6. In the **Log Source Description** field, type a description for the log source.
7. From the **Log Source Type** list, select your DSM name.
8. From the **Protocol Configuration** list, select **Log File**.
9. Configure the Log File protocol parameters.

The following table describes the parameters that require specific values for the DSM event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested 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 that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify.</td>
</tr>
</tbody>
</table>
| **Service Type**         | From the **Service Type** list, select the protocol that 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 that is used to retrieve log files for the SCP and SFTP service type requires that the server that is 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 that stores 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 - 65535. The options include ports:  
  • 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. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote User</td>
<td>Type the user name or user ID necessary to log in to the system that contains your event files.</td>
</tr>
<tr>
<td></td>
<td>• If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length.</td>
</tr>
<tr>
<td></td>
<td>• If your log files are 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.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Type the password necessary to log in to the host.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password necessary to log in to the host.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>If you select SCP or SFTP as the Service Type, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the Remote Password field is ignored.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>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.</td>
</tr>
<tr>
<td>Recursive</td>
<td>If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear. If you configure SCP as the Service Type, the Recursive option is ignored.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>If you select SFTP or FTP as the Service Type, you can configure the regular expression (regex) needed to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing.</td>
</tr>
<tr>
<td></td>
<td>The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <code>&lt;product_name&gt;..&lt;timestamp&gt;.gz</code></td>
</tr>
<tr>
<td></td>
<td>The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with zOS and end with .gz, type the following code: zOS.*.*gz</td>
</tr>
<tr>
<td></td>
<td>Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions. (<a href="http://download.oracle.com/javase/tutorial/essential/regex/">http://download.oracle.com/javase/tutorial/essential/regex/</a>)</td>
</tr>
<tr>
<td>FTP Transfer Mode</td>
<td>This option displays only if you select FTP as the Service Type. From the list, select Binary.</td>
</tr>
<tr>
<td></td>
<td>The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.</td>
</tr>
<tr>
<td>SCP Remote File</td>
<td>If you select SCP as the Service Type you must type the file name of the remote file.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Recurrence</strong></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.</td>
</tr>
<tr>
<td><strong>Run On Save</strong></td>
<td>If you want the Log File protocol to run immediately after you click Save, select this check box.</td>
</tr>
<tr>
<td></td>
<td>After the Run On Save completes, the Log File protocol follows your configured start time and recurrence schedule.</td>
</tr>
<tr>
<td></td>
<td>Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>From the list, select gzip.</td>
</tr>
<tr>
<td></td>
<td>Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in zip, gzip, tar, or tar+gzip archive format.</td>
</tr>
<tr>
<td><strong>Ignore Previously Processed File(s)</strong></td>
<td>Select this check box to track and ignore files that are already processed by the Log File protocol.</td>
</tr>
<tr>
<td></td>
<td>QRadar examines the log files in the remote directory to determine whether a file is 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 are not previously processed are downloaded.</td>
</tr>
<tr>
<td></td>
<td>This option applies only to FTP and SFTP service types.</td>
</tr>
<tr>
<td><strong>Change Local Directory?</strong></td>
<td>Select this check box to define a local directory on your QRadar for storing downloaded files during processing.</td>
</tr>
<tr>
<td></td>
<td>It is suggested that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which gives you the option to configure the local directory to use for storing files.</td>
</tr>
<tr>
<td><strong>Event Generator</strong></td>
<td>From the Event Generator list, select LineByLine.</td>
</tr>
<tr>
<td></td>
<td>The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.</td>
</tr>
</tbody>
</table>
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

The DSM configuration is complete. If your DSM requires custom event properties, see the IBM Security Custom Event Properties for IBM z/OS technical note. (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomeventProperties.pdf)

**Integrate CA ACF2 with IBM QRadar by using audit scripts**

The CA Access Control Facility (ACF2) DSM collects events and audit transactions on the IBM mainframe with the Log File protocol.

QexACF2.load.trs is a TERSED file that contains a PDS loadlib with the QEXACF2 program. A TERSED file is similar to a zip file and requires you to use the TRSMAIN program to decompress the contents. The TRSMAIN program is available from IBM Support (www.ibm.com/support).

To upload a TRS file from a workstation, you must preallocate a file with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL=1024, BLKSIZE=6144. The file transfer type must be BINARY APPEND. If the transfer type is TEXT or TEXT APPEND, then the file cannot decompress properly.

After you upload the file to the mainframe into the allocated dataset, the TERSED file can be UNPACKED with the TRSMAIN utility by using the sample JCL also included in the tar package. A return code of 0008 from the TRSMAIN utility indicates that the dataset is not recognized as a valid TERSED file. This code (0008) error might be the result of the file not being uploaded to the mainframe with the correct DCB attributes, or because the transfer was not performed with the BINARY APPEND transfer mechanism.

After you have successfully UNPACKED the loadlib file, you can run the QEXACF2 program with the sample JCL file. The sample JCL file is contained in the tar collection. To run the QEXACF2 program, you must modify the JCL to your local naming conventions and JOB card requirements. You might also need to use the STEPLIB DD if the program is not placed in a LINKLISTED library.

To integrate CA ACF2 events into IBM QRadar:

1. The IBM mainframe records all security events as Service Management Framework (SMF) records in a live repository.
2. The CA ACF2 data is extracted from the live repository with the SMF dump utility. The SMF file contains all of the events and fields from the previous day in raw SMF format.
3. The QexACF2.load.trs program pulls data from the SMF formatted file. The QexACF2.load.trs program pulls only the relevant events and fields for QRadar and writes that information in a compressed format for compatibility. The information is saved in a location accessible by QRadar.
4. QRadar uses the Log File protocol source to retrieve the output file information on a scheduled basis. QRadar then imports and processes this file.

**Configuring CA ACF2 that uses audit scripts to integrate with IBM QRadar**

IBM QRadar uses scripts to audit events from CA ACF2 installations, which are collected by using the log file protocol.

**Procedure**

1. From the IBM support website (http://www.ibm.com/support), download the following compressed file:
   qexacf2_bundled.tar.gz
2. On a Linux operating system, extract the file:
   tar -zxvf qexacf2_bundled.tar.gz
   The following files are contained in the archive:
   • QexACF2.JCL.txt - Job Control Language file
   • QexACF2.load.trs - Compressed program library (requires IBM TRSMAIN)
3. Load the files onto the IBM mainframe by using the following methods:

Upload the sample QexACF2_trsmain_JCL.txt and QexACF2.JCL.txt files by using the TEXT protocol.

4. Upload the QexACF2.load.trs file by using a BINARY mode transfer and append to a preallocated data set. The QexACF2.load.trs file is a tersed file that contains the executable file (the mainframe program QexACF2). When you upload the .trs file from a workstation, preallocate 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.

**Note:** QexACF2 is a small C mainframe program that reads the output of the TSSUTIL (EARLOUT data) line by line. QexACF2 adds a header to each record that contains event information, for example, record descriptor, the date, and time. The program places each field into the output record, suppresses trailing blank characters, and delimits each field with the pipe character. This output file is formatted for QRadar and the blank suppression reduces network traffic to QRadar. This program does not consume CPU or I/O disk resources.

5. Customize the trsmain sample_JCL.txt file according to your installation-specific parameters.

**Example:** Jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

The trsmain sample_JCL.txt file uses the IBM utility TRSMAIN to extract the program that is stored in the QexACF2.load.trs file.

An example of the QexACF2_trsmain_JCL.txt file includes the following information:

```plaintext
//TRSMAIN JOB (yourvalidjobcard),Q1labs,
// MSGCLASS=V
// DEL EXEC PGM=IEFBR14
// D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXACF2.LOAD.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>.QEXACF2.LOAD.TRS
// OUTFILE DD DISP=(NEW,CATLG,DELETE),
// DSN=<yourhlq>.LOAD,
// SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA
```

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 QexACF2 program as a member.

6. You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in LINKLST. The program does not require authorization.

7. After you upload, copy the program to an existing link listed library or add a STEPLIB DD statement with the correct data set name of the library that will contain the program.

8. The QexACF2_jcl.txt file is a text file that contains a sample JCL. You must configure the job card to meet your configuration.

The QexACF2_jcl.txt sample file includes:

```plaintext
//QEXACF2 JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=8M
//*
//QEXACF2 JCL VERSION 1.0 OCTOBER, 2010
 //*
//******************************************************************************************
// Change below dataset names to sites specific datasets names*
//QEXACF2 JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=8M
//*
```
9. After the output file is created, schedule a job to transfer the output file to an interim FTP server. The output file is forwarded to an interim FTP server.

You must configure the following parameters in the sample JCL to successfully forward the output to an interim FTP server:

**Example:**

```bash
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=* //SYSPRINT DD SYSOUT=* //*/
```
Where:

- `<IPADDR>` is the IP address or host name of the interim FTP server to receive the output file.
- `<USER>` is the user name that is needed to access the interim FTP server.
- `<PASSWORD>` is the password that is needed to access the interim FTP server.
- `<THEIPOFTHEMAINFRAMEDEVICE>` is the destination of the mainframe or interim FTP server that receives the output.

**Example:**

```
PUT 'xxxxxx.xxxxxxx.OUTPUT.C320' /<IP_address>/ACF2/QEXACF2.OUTPUT.C320
```

- `<QEXOUTDSN>` is the name of the output file that is saved to the interim FTP server.

You are now ready to configure the Log File protocol.

10. Schedule QRadar to retrieve the output file from CA ACF2.

If the zOS platform is configured to serve files through FTP, SFTP, or allow SCP, then no interim FTP server is needed and QRadar can pull the output file directly from the mainframe. The following text must be commented out using `//*` or deleted from the QexACF2_jcl.txt file:

```
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<User>
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=* 
//SYSPRINT DD SYSOUT=* 
```

**What to do next**

You are now ready to configure the log source in QRadar.

---

### CA SiteMinder

The CA SiteMinder DSM collects and categorizes authorization events from CA SiteMinder appliances with syslog-ng.

The CA SiteMinder DSM accepts access and authorization events that are logged in `smaccess.log` and forwards the events to IBM QRadar by using syslog-ng.

**Configuring a log source**

CA SiteMinder with IBM QRadar does not automatically discover authorization events that are forwarded with syslog-ng from CA SiteMinder appliances.

**About this task**

To manually create a CA SiteMinder log source:

**Procedure**

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
   
   The **Data Sources** pane is displayed.
3. Click the **Log Sources** icon.
The Log Sources window is displayed.

4. In the Log Source Name field, type a name for your CA SiteMinder log source.
5. In the Log Source Description field, type a description for the log source.
6. From the Log Source Type list, select CA SiteMinder.
7. From the Protocol Configuration list, select Syslog.

The syslog protocol parameters are displayed.

**Note:** The log file protocol is displayed in the Protocol Configuration list, however, polling for log files is not a suitable configuration.

8. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for your CA SiteMinder appliance.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the log source. By default, this check box is selected.</td>
</tr>
<tr>
<td>Credibility</td>
<td>From the list, type the credibility value of the log source. The range is 0 - 10.</td>
</tr>
<tr>
<td></td>
<td>The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source device. Credibility increases if multiple sources report the same event. The default is 5.</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>From the list, select the Target Event Collector to use as the target for the log source.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>Select this check box to enable the log source to coalesce (bundle) events.</td>
</tr>
</tbody>
</table>
|                            | Automatically discovered log sources use the default value that is configured in the Coalescing Events list in the System Settings window, which is accessible on the Admin tab. However, when you create a new log source or update the configuration for an automatically discovered log source that you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar Administration Guide.
Table 146. Adding a syslog log source (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store Event Payload</td>
<td>Select this check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the Store Event Payload list in the System Settings window, which is accessible on the Admin tab. When you create a new log source or update the configuration for an automatically discovered log source that you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar Administration Guide.</td>
</tr>
</tbody>
</table>

9. Click **Save**.

   The **Admin** tab toolbar detects log source changes and displays a message to indicate when you need to deploy a change.

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

**What to do next**

You are now ready to configure syslog-ng on your CA SiteMinder appliance to forward events to QRadar.

**Configuring Syslog-ng for CA SiteMinder**

You must configure your CA SiteMinder appliance to forward syslog-ng events to your QRadar Console or Event Collector.

**About this task**

IBM QRadar can collect syslog-ng events from TCP or UDP syslog sources on port 514.

To configure syslog-ng for CA SiteMinder:

**Procedure**

1. Using SSH, log in to your CA SiteMinder appliance as a root user.
2. Edit the syslog-ng configuration file.
   
   /etc/syslog-ng.conf
   
3. Add the following information to specify the access log as the event file for syslog-ng:
   
   ```
   source s_siteminder_access
   { file("/opt/apps/siteminder/sm66/siteminder/log/smaccess.log"); };
   ```

4. Add the following information to specify the destination and message template:
   
   ```
   destination d_remote_q1_siteminder {
   udp("<QRadar IP>" port(514) template ("$PROGRAM $MSG\n");
   };
   ```

   Where `<QRadar IP>` is the IP address of the QRadar Console or Event Collector.

5. Add the following log entry information:
   
   ```
   log {
   source(s_siteminder_access);
   destination(d_remote_q1_siteminder);
   };
   ```
6. Save the syslog-ng.conf file.
7. Type the following command to restart syslog-ng:

```
service syslog-ng restart
```

After the syslog-ng service restarts, the CA SiteMinder configuration is complete. Events that are forwarded to QRadar by CA SiteMinder are displayed on the Log Activity tab.

---

**CA Top Secret**

The CA Top Secret DSM collects events from a CA Technologies Top Secret image on an IBM z/OS mainframe by using IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.

To collect CA Top Secret events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html).
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 (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).
3. Create a log source in QRadar for CA Top Secret.

**Before you begin**

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.

**Related tasks**
- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 log source for Log File protocol**

The Log File protocol enables IBM QRadar to retrieve archived log files from a remote host for the IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, and CA ACF2 DSM's.

**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 z/OS with zSecure writes log files to a specified directory as gzip archives. 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 that uses the Log File protocol. QRadar requires credentials to log in to the system that hosts your LEEF formatted event files and a polling interval.

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. In the **Log Source Name** field, type a name for the log source.
6. In the **Log Source Description** field, type a description for the log source.
7. From the **Log Source Type** list, select your DSM name.
8. From the **Protocol Configuration** list, select **Log File**.
9. Configure the Log File protocol parameters.

The following table describes the parameters that require specific values for the DSM event collection:

<table>
<thead>
<tr>
<th><strong>Table 147. Log File protocol parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Log Source Identifier</strong></td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
</tbody>
</table>
| Service Type           | From the Service Type list, select the protocol that 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 that is used to retrieve log files for the SCP and SFTP service type requires that the server that is 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 that stores 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 - 65535.  
The options include ports:  
• 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. |
| Remote User            | Type the user name or user ID necessary to log in to the system that contains your event files.  
• If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length.  
• If your log files are 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 gives you the option to define an SSH private key file. When you provide an SSH Key File, the Remote Password field is ignored. |
| 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.                                                              |
| Recursive              | If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear.  
If you configure SCP as the Service Type, the Recursive option is ignored. |
### Table 147. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP File Pattern</td>
<td>If you select <strong>SFTP</strong> or <strong>FTP</strong> as the <strong>Service Type</strong>, you can configure the regular expression (regex) needed to filter the list of files that are specified in the <strong>Remote Directory</strong>. All matching files are included in the processing. The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <code>&lt;product_name&gt;.*&lt;timestamp&gt;\.gz</code>. The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with zOS and end with .gz, type the following code: <code>zOS.*\.*gz</code>. Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see <a href="http://download.oracle.com/javase/tutorial/essential/regex/">Lesson: Regular Expressions</a>.</td>
</tr>
<tr>
<td>FTP Transfer Mode</td>
<td>This option displays only if you select <strong>FTP</strong> as the <strong>Service Type</strong>. From the list, select <strong>Binary</strong>. The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.</td>
</tr>
<tr>
<td>SCP Remote File</td>
<td>If you select <strong>SCP</strong> as the <strong>Service Type</strong> you must type the file name of the remote file.</td>
</tr>
<tr>
<td>Start Time</td>
<td>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.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>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.</td>
</tr>
<tr>
<td>Run On Save</td>
<td>If you want the Log File protocol to run immediately after you click <strong>Save</strong>, select this check box. After the <strong>Run On Save</strong> completes, the Log File protocol follows your configured start time and recurrence schedule. Selecting <strong>Run On Save</strong> clears the list of previously processed files for the Ignore Previously Processed File parameter.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.</td>
</tr>
</tbody>
</table>
Table 147. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>From the list, select gzip.</td>
</tr>
<tr>
<td></td>
<td>Processors enable event file archives to be expanded and contents are</td>
</tr>
<tr>
<td></td>
<td>processed for events. Files are processed after they are downloaded to</td>
</tr>
<tr>
<td></td>
<td>QRadar. QRadar can process files in zip, gzip, tar, or tar+gzip</td>
</tr>
<tr>
<td></td>
<td>archive format.</td>
</tr>
<tr>
<td>Ignore Previously</td>
<td>Select this check box to track and ignore files that are already</td>
</tr>
<tr>
<td>Processed File(s)</td>
<td>processed by the Log File protocol.</td>
</tr>
<tr>
<td></td>
<td>QRadar examines the log files in the remote directory to determine</td>
</tr>
<tr>
<td></td>
<td>whether a file is previously processed by the Log File protocol.</td>
</tr>
<tr>
<td></td>
<td>If a previously processed file is detected, the Log File protocol</td>
</tr>
<tr>
<td></td>
<td>does not download the file for processing. All files that are not</td>
</tr>
<tr>
<td></td>
<td>previously processed are downloaded.</td>
</tr>
<tr>
<td></td>
<td>This option applies only to FTP and SFTP service types.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>Select this check box to define a local directory on your QRadar for</td>
</tr>
<tr>
<td></td>
<td>storing downloaded files during processing.</td>
</tr>
<tr>
<td></td>
<td>It is suggested that you leave this check box clear. When this check</td>
</tr>
<tr>
<td></td>
<td>box is selected, the Local Directory field is displayed, which gives</td>
</tr>
<tr>
<td></td>
<td>you the option to configure the local directory to use for storing</td>
</tr>
<tr>
<td></td>
<td>files.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the Event Generator list, select LineByLine.</td>
</tr>
<tr>
<td></td>
<td>The Event Generator applies more processing to the retrieved event</td>
</tr>
<tr>
<td></td>
<td>files. Each line is a single event. For example, if a file has 10</td>
</tr>
<tr>
<td></td>
<td>lines of text, 10 separate events are created.</td>
</tr>
</tbody>
</table>

10. Click **Save**.

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

The DSM configuration is complete. If your DSM requires custom event properties, see the IBM Security Custom Event Properties for IBM z/OS technical note. (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf)

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:

- IBM z/OS
- IBM CICS
- IBM RACF
- IBM DB2
- CA Top Secret
- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.
The following table describes the parameters that require specific values for event collection for your DSM:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Select your DSM name from the list.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>

Integrate CA Top Secret with IBM QRadar by using audit scripts

The CA Top Secret DSM collects events and audit transactions on the IBM mainframe with the Log File protocol.

IBM QRadar records all relevant and available information from the event.

To integrate CA Top Secret events into QRadar:

1. The IBM mainframe records all security events as Service Management Framework (SMF) records in a live repository.
2. At midnight, the CA Top Secret data is extracted from the live repository by using the SMF dump utility. The SMF file contains all of the events and fields from the previous day in raw SMF format.
3. The qextopsloadlib program pulls data from the SMF formatted file. The qextopsloadlib program only pulls the relevant events and fields for QRadar and writes that information in a condensed format for compatibility. The information is saved in a location accessible by QRadar.
4. QRadar uses the Log File protocol source to retrieve the output file information on a scheduled basis. QRadar then imports and processes this file.

Configuring CA Top Secret that uses audit scripts to integrate with IBM QRadar

The CA Top Secret DSM collects events and audit transactions on the IBM mainframe by using the Log File protocol.

Procedure

1. From the IBM support website (http://www.ibm.com/support), download the following compressed file:
   qextops_bundled.tar.gz
2. On a Linux operating system, extract the file:
   tar -zxvf qextops_bundled.tar.gz
   The following files are contained in the archive:
   • qextops_jcl.txt
   • qextopsloadlib.trs
   • qextops_trsmain_JCL.txt
3. Load the files onto the IBM mainframe by using any terminal emulator file transfer method.
   Upload the sample qextops_trsmain_JCL.txt and qextops_jcl.txt files by using the TEXT protocol.
4. Upload the qextopsloadlib.trs file by using a BINARY mode transfer. The qextopsloadlib.trs file is a tersed file that contains the executable (the mainframe program qextops). When you upload the .trs file from a workstation, preallocate 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.
**Note:** Qextops is a small C mainframe program that reads the output of the TSSUTIL (EARLOUT data) line by line. Qextops adds a header to each record that contains event information, for example, record descriptor, the date, and time. The program places each field into the output record, suppresses trailing blank characters, and delimits each field with the pipe character. This output file is formatted for QRadar and the blank suppression reduces network traffic to QRadar. This program does not consume CPU or I/O disk resources.

5. Customize the `qextops_trsmain_JCL.txt` file according to your installation-specific requirements.

The `qextops_trsmain_JCL.txt` file uses the IBM utility TRSMAIN to extract the program that is stored in the `qextopsloadlib.trs` file.

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

```
//TRSMAIN JOB (yourvalidjobcard),Q1labs,
// MSGCLASS=V
//DEL EXEC PGM=IEFBR14
//D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXTOPS.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>.QEXTOPS.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 qextops program as a member.

6. 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.

7. Following the upload, copy the program to an existing link listed library or add a STEPLIB DD statement with the correct data set name of the library that contains the program.

8. The `qextops_jcl.txt` file is a text file that contains a sample JCL. You must configure the job card to meet your configuration.

The `qextops_jcl.txt` sample file includes:

```
//QEXTOPS JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXTOPS JCL version 1.0 September, 2010
 //*
*******************************************************************************/
// Change below dataset names to sites specific datasets names*
*******************************************************************************/
//SET1 SET TSSOUT='Q1JACK.EARLOUT.ALL',
// EARLOUT='Q1JACK.QEXTOPS.PROGRAM.OUTPUT'
*******************************************************************************/
// Delete old datasets *
*******************************************************************************/
DEL EXEC PGM=IEFBR14
//D1 DD DISP=(MOD,DELETE),DSN=STSSOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//D2 DD DISP=(MOD,DELETE),DSN=EARLOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
*******************************************************************************/
//Allocate new dataset *
*******************************************************************************/
```
9. After the output file is created, schedule a job to transfer the output file to an interim FTP server. The output file is forwarded to an interim FTP server.

You must configure the following parameters in the sample JCL to successfully forward the output to an interim FTP server:

**Example:**

```
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
USER>
<PASSWORD>
PUT 'EARLOUT/EARL_<THEIPOFTHEMAINFRAMEDEVICE>/QUIT
//OUTPUT DD SYSOUT=* SYSPRINT DD SYSOUT=* 
```

Where:

- `<IPADDR>` is the IP address or host name of the interim FTP server to receive the output file.
- `<USER>` is the user name that is needed to access the interim FTP server.
- `<PASSWORD>` is the password that is needed to access the interim FTP server.
- `<THEIPOFTHEMAINFRAMEDEVICE>` is the destination of the mainframe or interim FTP server that receives the output.

**Example:**

```
PUT 'xxxxxx.xxxxxx.OUTPUT.C320' /<IP_address>/CA/QEXTOPS.OUTPUT.C320 
```

<QEXOUTDSN> is the name of the output file that is saved to the interim FTP server.
You are now ready to configure the Log File protocol.

10. Schedule QRadar to collect the output file from CA Top Secret.

If the zOS platform is configured to serve files through FTP, SFTP, or allow SCP, then no interim FTP server is needed and QRadar can pull the output file directly from the mainframe. The following text must be commented out using //* or deleted from the qextops_jcl.txt file:

```plaintext
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<User>
<PASSWORD>
PUT '{EARLOUT}' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<EARLOUT>
QUIT
//OUTPUT DD SYSOUT=*  //SYSPRINT DD SYSOUT=*  
```

**What to do next**

You are now ready to configure the log source in QRadar.
Chapter 38. Carbon Black

Several Carbon Black DSMs can be integrated with IBM QRadar

Carbon Black

The IBM QRadar DSM for Carbon Black collects endpoint protection events from a Carbon Black server.

The following table describes the specifications for the Carbon Black DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Carbon Black</td>
</tr>
<tr>
<td>DSM name</td>
<td>Carbon Black</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CarbonBlackCarbonBlack-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>5.1 and later</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Watchlist hits</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate Carbon Black 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:
   - Carbon Black DSM RPM
   - DSMCommon RPM
2. Configure your Carbon Black device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Carbon Black log source on the QRadar Console. The following table describes the parameters that require specific values for Carbon Black event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Carbon Black</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Carbon Black to communicate with QRadar**

To collect events from Carbon Black, you must install and configure cb-event-forwarder to send Carbon Black events to IBM QRadar.

**Before you begin**

Install the Carbon Black Enterprise RPM and ensure that it is running. You can install the cb-event-forwarder on any 64-bit Linux computer that is running CentOS 6.x. It can be installed on the same computer as the Carbon Black server, or on another computer. If you are forwarding many events, for example, all file modifications, registry modifications, or both, to QRadar, install cb-event-forwarder on a separate server. If you are not forwarding many events to QRadar, you can install the cb-event-forwarder on the Carbon Black server.

If you are installing the cb-event-forwarder on a computer other than the Carbon Black server, you must configure the Carbon Black server:

1. Ensure that TCP port 5004 is open through the iptables firewall on the Carbon Black server. The event-forwarder connects to TCP port 5004 on the Carbon Black server to connect to the Cb message bus.
2. Get the RabbitMQ user name and password from the /etc/cb/cb.conf file on the Carbon Black server. Search for the RabbitMQUser and RabbitMQPassword variables and note their values.

**About this task**

You can find the following instructions, source code, and quick start guide on the GitHub website (https://github.com/carbonblack/cb-event-forwarder/).

**Procedure**

1. If it is not already installed, install the CbOpenSource repository:

   ```bash
cd /etc/yum.repos.d
curl -O https://opensource.carbonblack.com/release/x86_64/CbOpenSource.repo
   ```

2. Install the RPM for cb-event-forwarder:

   ```bash
   yum install cb-event-forwarder
   ```

3. Modify the /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf file to include udpout=<QRadar_IP_address>:514, and then specify LEEF as the output format:

   ```plaintext
   output_format=leef
   ```

4. If you are installing on a computer other than the Carbon Black server, copy the RabbitMQ user name and password into the rabbit_mq_username and rabbit_mq_password variables in the /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf file. In the cb_server_hostname variable, enter the host name or IP address of the Carbon Black server.

5. Ensure that the configuration is valid by running the cb-event-forwarder in check mode:

   ```bash
   /usr/share/cb/integrations/event-forwarder/cb-event-forwarder -check
   ```

   If valid, the message Initialized output displays. If there are errors, the errors are printed to your screen.

6. Choose the type of event that you want to capture.

   By default, Carbon Black publishes the all feed and watchlist events over the bus. If you want to capture raw sensor events or all binaryinfo notifications, you must enable those features in the /etc/cb/cb.conf file.

   • To capture raw sensor events, edit the DatastoreBroadcastEventTypes option in the /etc/cb/cb.conf file to enable broadcast of the raw sensor events that you want to export.
To capture binary observed events, edit the `EnableSolrBinaryInfoNotifications` option in the `/etc/cb/cb.conf` file and set it to `True`.

7. If any variables were changed in `/etc/cb/cb.conf`, restart the Carbon Black server: "service cb-enterprise restart".

8. Start the `cb-event-forwarder` service by using the `initctl` command: `initctl start cb-event-forwarder`.
   
   **Note:** You can stop the `cb-event-forwarder` service by using the `initctl` command: `initctl stop cb-event-forwarder`.

---

**Carbon Black Protection**

The IBM QRadar DSM for Carbon Black Protection receives logs from a Carbon Black Protection device. The following table identifies the specifications for the Carbon Black Protection DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Carbon Black</td>
</tr>
<tr>
<td>DSM name</td>
<td>Carbon Black Protection</td>
</tr>
<tr>
<td>RPM filename</td>
<td>DSM-CarbonBlackProtection-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>8.0.0, 8.1.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Computer Management, Server Management, Session Management, Policy Management, Policy Enforcement, Internal Events, General Management, Discovery</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

1. If automatic updates are not configured, download the most recent version of the following RPMs on your QRadar Console
   - DSMCommon RPM
   - Carbon Black Protection DSM RPM

2. Enable the Carbon Black Protection console to communicate with QRadar.

3. If QRadar does not automatically detect the log source, add a Carbon Black Protection log source on the QRadar Console. The following table describes the parameters that require specific values for Carbon Black Protection event collection:
Table 152. Carbon Black Protection log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log source type</td>
<td>Carbon Black Protection</td>
</tr>
<tr>
<td>Log source identifier</td>
<td>IP address or host name for the log source</td>
</tr>
<tr>
<td>Protocol configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

4. Verify that Carbon Black Protection is configured correctly.

The following table provides a sample event message for the Carbon Black Protection DSM:

Table 153. Carbon Black Protection sample message supported by the Carbon Black Protection device

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console user login</td>
<td>User login success</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 Carbon Black Protection to communicate with QRadar

Enable the Carbon Black Protection console to communicate with QRadar.

Procedure

1. Access the Carbon Black Protection console by entering the Carbon Black Protection server URL in your browser.
2. On the login screen, enter your username and password. You must use a Carbon Black Protection account with Administrator or Power User privileges.
3. From the top console menu, select System Configuration in the Administration section.
5. On the External Events Logging section, click Edit. Enter the QRadar Event Collector IP address in the Syslog address field and enter 514 for the Syslog port field.
6. Change the Syslog format to LEEF (Q1Labs).
7. Check Syslog Enabled for Syslog output.
8. Click Update to confirm the changes.
To collect events, you must configure your Carbon Black Bit9 Parity device to forward syslog events in Log Event Extended Format (LEEF).

**Procedure**

1. Log in to the Carbon Black Bit9 Parity console with Administrator or PowerUser privileges.
2. From the navigation menu on the left side of the console, select **Administration > System Configuration**.
   - The **System Configuration** window is displayed.
3. Click **Server Status**.
   - The **Server Status** window is displayed.
4. Click **Edit**.
5. In the **Syslog address** field, type the IP address of your QRadar Console or Event Collector.
6. From the **Syslog format** list, select **LEEF (Q1Labs)**.
7. Select the **Syslog enabled** check box.
8. Click **Update**.

The configuration is complete. The log source is added to IBM QRadar as Carbon Black Bit9 Parity events are automatically discovered. Events that are forwarded to QRadar by Carbon Black Bit9 Parity are displayed on the **Log Activity** tab of QRadar.

**Configuring a log source for Carbon Black Bit 9 Parity**

IBM QRadar automatically discovers and creates a log source for syslog events from Carbon Black Bit9 Parity.

**About this task**

The following configuration steps are optional.

**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 **Bit9 Security Platform**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Carbon Black Bit9 Parity device.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Bit9 Security Platform

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

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Carbon Black</td>
</tr>
<tr>
<td>DSM name</td>
<td>Bit9 Security Platform</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-Bit9Parity-&lt;build_number&gt;.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V6.0.2 and up</td>
</tr>
<tr>
<td>Event format</td>
<td>Syslog</td>
</tr>
<tr>
<td>Supported event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Included identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td>Bit9 website (<a href="http://www.bit9.com">http://www.bit9.com</a>)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Log Source Identifier</th>
<th>The IP address or host name of the Bit9 Security Platform device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Bit9 Security Platform</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Carbon Black Bit9 Security Platform to communicate with QRadar**

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

**Procedure**

1. Log in to the Carbon Black 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 39. Centrify

IBM QRadar supports a range of Centrify devices.

Centrify Identity Platform

The IBM QRadar DSM for Centrify Identity Platform collects logs from a Centrify Identity Platform.

To integrate Centrify Identity Platform 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:
   - Protocol Common RPM
   - Centrify Redrock REST API Protocol RPM
   - DSMCommon RPM
   - Centrify Identity Platform DSM RPM

2. Configure your Centrify Identity Platform to communicate with QRadar.

3. Add a Centrify Identity Platform log source on the QRadar Console. The following table describes the Centrify Redrock REST API protocol parameters that require specific values to collect events from Centrify Identity Platform:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Centrify Identity Platform</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Centrify Redrock REST API</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique name for the log source. The Log Source Identifier can be any valid value and does not need to reference a specific server. The Log Source Identifier can be the same value as the Log Source Name. If you have more than one Centrify Identity Platform log source that is configured, you might want to identify the first log source as centrify1, the second log source as centrify2, and the third log source as centrify3.</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>The Centrify assigned unique customer or tenant ID.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name that is associated with the Cloud service for Centrify Identity Platform.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is associated with the Centrify Identity Platform user name.</td>
</tr>
<tr>
<td>Event Logging Filter</td>
<td>Select the logging level of the events that you want to retrieve. Info, Warning and Error are selectable. At least one filter must be selected.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>When a proxy is configured, all traffic from the Centrify Redrock REST API travels through the proxy. 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.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second. The default is 5000.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The time interval can be in hours (H), minutes (M) or days (D). The default is 5 minutes (5M).</td>
</tr>
</tbody>
</table>

**Related concepts**

“Centrify Identity Platform DSM specifications” on page 290
The following table describes the specifications for the Centrify Identity Platform DSM.

“Sample event message” on page 292
Use this sample event message as a way of verifying a successful integration with QRadar.

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Centrify Identity Platform to communicate with QRadar” on page 291

**Centrify Identity Platform DSM specifications**

The following table describes the specifications for the Centrify Identity Platform DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Centrify</td>
</tr>
<tr>
<td>DSM name</td>
<td>Centrify Identity Platform</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CentrifyIdentityPlatform-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Centrify Redrock REST API</td>
</tr>
<tr>
<td>Event format</td>
<td>JSON</td>
</tr>
</tbody>
</table>
### Table 157. Centrify Identity Platform DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recorded event types</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td>Core</td>
</tr>
<tr>
<td></td>
<td>Internal</td>
</tr>
<tr>
<td></td>
<td>Mobile</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

### Configuring Centrify Identity Platform to communicate with QRadar

To send events to QRadar from your Centrify Identity Platform, create a user role and configure a user policy on your Centrify Identity Platform. The QRadar user can then create a log source in QRadar.

**Before you begin**

Ensure that you have the Tenant ID and admin login details that are supplied by Centrify. Ensure that you have the correct user permissions for the Centrify admin portal to complete the following steps:

**Procedure**

1. Log in to your Centrify Identity Platform admin portal.
2. Create a Centrify Identity Platform user role:
   a) From the navigation pane, click **Roles > Add Role**.
   b) In the **Name** field, type the name for the role.
   c) Select **Members**, and then click **Add**.
   d) In the **Add Members** window, search for the user name to assign to the role, and then select the member.
   e) Click **Add**.
   f) Select **Administrative Rights**, and then click **Add**.
   g) From the **Description** list, select **Read Only System Administrator**.
   h) Click **Save**.
3. Create an authentication profile:
   a) From the navigation pane, click **Settings > Authentication**.
   b) From the **Platform** menu, click **Authentication Profiles**.
   c) Click **Add Profile**, and then type a name for the profile in the **Profile Name** field.
   d) From the **Challenge 1** pane in the **Authentication Mechanisms** window, select **Password**.
   e) From the **Challenge Pass-Through Duration** list, select **30 minutes**, and then click **OK**. The default is 30 minutes.

   **Important**: Do not select any options from the **Challenge 2** pane in the **Authentication Mechanisms** window. Select options only from the **Challenge 1** pane.
4. Configure a user policy:
   a) From the navigation pane, click **Policies > Add Policy Set**.
   b) From the **Policy Setting** pane, type a name for the policy in the **Name** field.
c) From the Policy Assignment pane, click Specified Roles.
d) Click Add.
e) From the Select Role window, select the role that you created in Step 2 from the Role list, and then click Add.
f) From the Policy Settings menu, select Login Policies > Centrify Portal.
g) From the Enable authentication policy controls window, select Yes.
h) From the Default Profile pane, select the authentication profile that you created in Step 3 from the Default Profile list.
i) Click Save.

**Note:** If you have difficulty when configuring your Centrify Identity Platform to communicate with QRadar, contact your Centrify administrator or your Centrify contact.

### Sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when using the Centrify Identity Platform REST API protocol for the Centrify Identity Platform DSM:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud.Core&gt;Login. MultiFactorChallenge</td>
<td>User Login Attempt</td>
<td>{&quot;RequestIsMobileDevice&quot;: false,&quot;AuthMethod&quot;: &quot;MultiAuth&quot;,&quot;Level&quot;: &quot;Error&quot;,&quot;UserGuid&quot;: &quot;c2c7bcc6-9560-44e0-8dff-5be221cd37ee&quot;,&quot;Mechanism&quot;: &quot;EMail&quot;,&quot;Tenant&quot;: &quot;AAM0428&quot;,&quot;FromIPAddress&quot;: &quot;&lt;IP_address&gt;&quot;,&quot;ID&quot;: &quot;772c2e1908a4f11b.W03.c5ab.a936852233d2232d&quot;,&quot;RequestDeviceOS&quot;: &quot;Windows&quot;,&quot;EventType&quot;: &quot;Cloud.Core.Login.MultiFactorChallenge&quot;,&quot;HostName&quot;: &quot;192.0.2.1&quot;,&quot;ThreadType&quot;: &quot;RestCall&quot;,&quot;Username&quot;: &quot;<a href="mailto:username@example.com">username@example.com</a>&quot;,&quot;NormalizedUser&quot;: &quot;<a href="mailto:username@example.com">username@example.com</a>&quot;,&quot;WhenLogged&quot;: &quot;/Date(1472679431199)/&quot;,&quot;WhenOccurred&quot;: &quot;/Date(1472679431199)/&quot;,&quot;Target&quot;: &quot;<a href="mailto:username@example.com">username@example.com</a>&quot;}</td>
</tr>
</tbody>
</table>

### Centrify Infrastructure Services

The IBM QRadar DSM for Centrify Infrastructure Services collects events from Centrify Infrastructure Services standard logs.

The following table describes the specifications for the Centrify Infrastructure Services DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Centrify</td>
</tr>
<tr>
<td>DSM name</td>
<td>Centrify Infrastructure Services</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CentrifyInfrastructureServices-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>Centrify Infrastructure Services 2017</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog, TLS Syslog and WinCollect</td>
</tr>
</tbody>
</table>
To integrate Centrify Infrastructure Services with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of Centrify Infrastructure Services DSM RPM on your QRadar Console.

   **Note:** If you use the WinCollect protocol configuration option, install the latest WinCollect agent bundle (.sfs file) on your QRadar Console.

2. To send syslog or Windows events to QRadar, configure your UNIX, Linux, or Windows device where the Centrify Infrastructure Services standard logs are available.

3. If QRadar does not automatically detect the log source, add a Centrify Infrastructure Services log source on the QRadar Console.

   The following table describes the parameters that require specific values to collect events from Centrify Infrastructure Services:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Centrify Infrastructure Services</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the UNIX, Linux, or Windows device that sends Centrify Infrastructure Services events to QRadar.</td>
</tr>
</tbody>
</table>

4. Optional: To add a Centrify Infrastructure Services log source to receive Syslog events from network devices that support TLS Syslog event forwarding, configure the log source on the QRadar Console to use the TLS Syslog protocol.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Centrify Infrastructure Services</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>TLS Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
<tr>
<td>TLS Protocols</td>
<td>Select the version of TLS that is installed on the client.</td>
</tr>
</tbody>
</table>

**Related concepts**

“TLS syslog protocol configuration options” on page 93
Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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 WinCollect agent to collect event logs from Centrify Infrastructure Services**

You can forward Windows events to IBM QRadar by using WinCollect.

To forward Windows events by using WinCollect, install WinCollect agent on a Windows host. Download the WinCollect agent setup file from the IBM Support website (https://www.ibm.com/support). Add a Centrify Infrastructure Services log source and assign it to the WinCollect agent.

The following table describes the values that are required for the WinCollect log source parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Centrify Infrastructure Services</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>WinCollect</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the Windows machine from which you want to collect Windows events. The log source identifier must be unique for the log source type.</td>
</tr>
</tbody>
</table>
| Local System               | Select the **Local System** check box to disable the remote collection of events for the log source. The log source uses local system credentials to collect and forward logs to QRadar.  
You need to configure the **Domain**, **Username**, and **Password** parameters if remote collection is required. |
| Event Rate Tuning Profile  | For the default polling interval of 3000 ms, the approximate Events per second (EPS) rates attainable are as follows:  
* Default (Endpoint): 33-50 EPS  
* Typical Server: 166-250 EPS  
* High Event Rate Server: 416-625 EPS  
For a polling interval of 1000 ms, the approximate EPS rates are as follows:  
* Default (Endpoint): 100-150 EPS  
* Typical Server: 500-750 EPS  
* High Event Rate Server: 1250-1875 EPS  
For more information about tuning WinCollect, go to the IBM Support website (http://www.ibm.com/support/docview.wss?uid=swg21672193). |
| Polling Interval (ms)      | The interval, in milliseconds, between times when WinCollect polls for new events. |
### Table 162. WinCollect log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application or Service Log Type</strong></td>
<td>Select <strong>None</strong> for the <strong>Application or Service Log Type</strong>.</td>
</tr>
<tr>
<td><strong>Standard Log Types</strong></td>
<td>Do not enable the check box for any of the log types.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>No Filtering</strong> as the log filter type for the following log types: <strong>Security</strong>, <strong>System</strong>, <strong>Application</strong>, <strong>DNS Server</strong>, <strong>File Replication Service</strong>, and <strong>Directory Service</strong>.</td>
</tr>
<tr>
<td><strong>Event Types</strong></td>
<td>You must select at least one event type.</td>
</tr>
<tr>
<td><strong>XPath Query</strong></td>
<td>To forward only Centrify Audit events, you must specify the XPath filter. The query is in XML format and can be created by using Custom View Properties of Microsoft Event Viewer. For more information about creating an XPath query, go to the Creating a custom view documentation on the IBM Support website (<a href="https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.wincollect.doc/t_ug_wincollect_creating_customview.html">https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.wincollect.doc/t_ug_wincollect_creating_customview.html</a>). <strong>Important:</strong> When you create the custom view, ensure that the <strong>By Source</strong> option is selected. From the <strong>Event sources</strong> list, select the application name of the Centrify Audit Events. Example XPath query:  &lt;QueryList&gt;  &lt;Query Id=&quot;0&quot; Path=&quot;Application&quot;&gt;  &lt;SelectPath=&quot;Application&quot;&gt;*[System [Provider[@Name='Centrify AuditTrail V2']]]&lt;/Select&gt;  &lt;/Query&gt;  &lt;/QueryList&gt;</td>
</tr>
<tr>
<td><strong>Enable Active Directory Lookups</strong></td>
<td>Do not select the check box.</td>
</tr>
<tr>
<td><strong>WinCollect Agent</strong></td>
<td>Select your WinCollect agent from the list.</td>
</tr>
<tr>
<td><strong>Target Internal Destination</strong></td>
<td>Use any managed host with an event processor component as an internal destination.</td>
</tr>
</tbody>
</table>

Configuring Centrify Infrastructure Services on a UNIX or Linux device to communicate with QRadar

You can configure your UNIX or Linux device to send audit events to IBM QRadar. The audit events are available locally in the syslog event logs where the Centrify Infrastructure Services is installed and configured.

Procedure

1. Log in to your Centrify Infrastructure Services device.
2. Ensure that syslog or rsyslog is installed:
   • To verify that syslog is installed, type `service syslog status`.
   • To verify that rsyslog is installed, type `service rsyslog status`.
3. If syslog or rsyslog is not installed, install them by using your preferred method based on your UNIX or Linux device. For example, you can type the following command to install rsyslog on a Linux device:
   
   ```sh
   yum install rsyslog
   ```
4. To forward events to your QRadar Event Collector, open the `rsyslog.conf` file or the `syslog.conf` file that is located in `/etc/` directory, and then add the following line:

   ```conf
   :msg, contains, "AUDIT_TRAIL" @@QRadar Event Collector IP>:514
   ```

   **Example:**
   ```conf
   :msg, contains, "AUDIT_TRAIL" @@127.0.0.1:514
   ```
5. Restart the syslog or rsyslog service:
   • If you are using syslog, type `service syslog restart`.
   • If you are using rsyslog, type `service rsyslog restart`.

   **Note:** The Centrify Linux agent might forward some Linux system messages with the Audit Trail logs. If no specific category is found, the Linux OS log source type in QRadar discovers the Linux messages and normalizes them as stored.

Sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table shows sample event messages from Centrify Infrastructure Services:
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote login success</td>
<td>Remote Access Login Succeeded</td>
<td>`&lt;13&gt;May 09 20:58:48 127.1.1.1 AgentDevice=WindowsLog AgentLogFile=Application Plugin Version=7.2.6.39 Source=Centrify AuditTrail V2 Computer=Centrify WindowsAgent.Centrify.lab OriginatingComputer=127.1.1.1 User=user Domain =CENTRIFY EventID=1234 EventID Code=1234 EventType=4 Event Category=4 RecordNumber=1565 TimeGenerated=1494374321 TimeWritten=1494374321 Level=Informational Keywords= ClassicTask=None Opcode=Info Message=Product: Centrify Suite Category: Direct Authorize - Windows Event name: User successfully logged on remotely using role 'Windows Login/CentrifyTest'. May 09 16:58:41 centrifywindowsagent.centrify.lab dzagent[2008]: INFO AUDIT_TRAIL</td>
</tr>
<tr>
<td>The user logged in to the system successfully</td>
<td>User Login Success</td>
<td>`&lt;38&gt;May 4 23:45:19 hostname adclient[1472]: INFO AUDIT_TRAIL</td>
</tr>
</tbody>
</table>
Chapter 40. Check Point

Several Check Point products can be integrated with IBM QRadar. The following products are supported:

- Firewall
- SmartDefense
- IPS
- Anti Malware
- Anti-Bot
- Antivirus
- Mobile Access
- DDoS Protector
- Security Gateway/Management
- Threat Emulation
- URL Filtering
- DLP
- Application Control
- Identity Logging
- VPN
- Endpoint Security

Check Point

You can configure IBM QRadar to integrate with a Check Point device by employing one of several methods. Employ one of the following methods:

- “Integration of Check Point by using OPSEC” on page 299
- “Integrate Check Point by using syslog” on page 306
- “Integration of Check Point Firewall events from external syslog forwarders” on page 308

Note: Depending on your Operating System, the procedures for the Check Point device might vary. The following procedures are based on the Check Point SecurePlatform Operating system.

Integration of Check Point by using OPSEC

This section describes how to ensure that IBM QRadar accepts Check Point events using Open Platform for Security (OPSEC/LEA).

To integrate Check Point OPSEC/LEA with QRadar, you must create two Secure Internal Communication (SIC) files and enter the information in to QRadar as a Check Point log source.

Check Point configuration overview

To integrate Check Point with QRadar, you must complete the following procedures in sequence:

1. Add QRadar as a host for Check Point.
2. Add an OPSEC application to Check Point.
3. Locate the Log Source Secure Internal Communications DN.
4. In QRadar, configure the OPSEC LEA protocol.
5. Verify the OPSEC/LEA communications configuration.

**Adding a Check Point Host**
You can add IBM QRadar as a host in Check Point SmartCenter:

**Procedure**
1. Log in to the Check Point SmartCenter user interface.
2. Select **Objects > New Host**.
3. Enter the information for your Check Point host:
   - **Object Name**: QRadar
   - **IP address**: IP address of QRadar
4. Click **OK**.

**What to do next**
You are now ready to create an OPSEC Application Object for Check Point.

**Creating an OPSEC Application Object**
After you add IBM QRadar as a host in Check Point SmartCenter, you can create the OPSEC Application Object.

**Procedure**
1. Open the Check Point SmartConsole user interface.
2. Select **Objects > More Object Types > Server > OPSEC Application > New Application**.
3. Configure your OPSEC Application:
   a) Configure the following **OPSEC Application Properties** parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>QRadar-OPSEC</td>
</tr>
<tr>
<td>Host</td>
<td>QRadar</td>
</tr>
<tr>
<td>Client Entities</td>
<td>LEA</td>
</tr>
</tbody>
</table>

   b) Click **Communication**.
   c) In the **One-time password** field, type the password that you want to use.
   d) In the **Confirm one-time password** field, type the password that you used for **One-time password**.
   e) Click **Initialize**.
   f) Click **Close**.
4. Select **Menu > Install Policy**
5. Click **Publish & Install**.
6. Click **Install**.
7. Select **Menu > Install Database**.
8. Click **Install**.

**Note**: The SIC value is required for the OPSEC Application Object SIC attribute parameter when you configure the Check Point log source in QRadar. The value can be found by viewing the OPSEC Application Object after it is created.

The OPSEC Application Object resembles the following example:
Results
If you have issues after you install the database policy, contact your system administrator to restart Check Point services on the central SmartCenter server that hosts the policy files. After services restart, the updated policies are pushed to all Check Point appliances.

Locating the log source SIC
After you create the OPSEC Application Object, you can locate the Log Source SIC from the Check Point SmartConsole.

Procedure
1. Select Objects > Object Explorer.
2. In the Categories tree, select Gateways and Servers under Networks Objects.
3. Select your Check Point Log Host object.
4. Copy the Secure Internal Communication (SIC).

Important: Depending on your Check Point version, the Communication button displays the SIC attribute. You can locate the SIC attribute from the Check Point Management Server command-line interface. You must use the `cpca_client lscert` command from the command-line interface of the Management Server to display all certificates.

Important: The Log Source SIC Attribute resembles the following example: `cn=cp_mgmt,o=cpmodule...tdfaaz`. For more information, see your Check Point Command Line Interface Guide.

You must now install the Security Policy from the Check Point SmartConsole user interface.

What to do next
You are now ready to configure the OPSEC LEA protocol.

Configuring an OPSEC/LEA log source in IBM QRadar
After you locate the Log Source SIC, you configure the OPSEC LEA protocol:

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.
5. In the Log Source Name field, type a name for your log source.
6. In the Log Source Description field, type a description for the log source.
7. From the Log Source Type list, select Check Point.
8. Using the Protocol Configuration list, select OPSEC/LEA.
9. Configure the following values:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address for the log source. This value must match the value that is configured in the Server IP parameter. The log source identifier must be unique for the log source type.</td>
</tr>
<tr>
<td>Server IP</td>
<td>Type the IP address of the Check Point host or Check Point Management Server IP.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Type the port number that is used for OPSEC communication. Administrators must ensure that the existing firewall policy allows the LEA/OPSEC connection from your QRadar.</td>
</tr>
<tr>
<td>Use Server IP for Log Source</td>
<td>Select the check box to use the LEA server's IP address instead of the managed device's IP address for a log source. All events that are received by QRadar are funneled into a single log source. Clear the check box to have all events that are forwarded by Check Point Management Server to go into their individual log sources. By default, this parameter is enabled.</td>
</tr>
<tr>
<td>Statistics Report Interval</td>
<td>Type the interval, in seconds, during which the number of syslog events are recorded in the QRadar.log file. The valid range is 4 - 2,147,483,648 and the default is 600.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>From the list, select the Authentication Type that you want for this LEA configuration. The options are as follows: • sslca (default) • sslca_clear • clear This value must match the authentication method that is configured on the Check Point Firewall or Check Point custom log management server.</td>
</tr>
<tr>
<td>OPSEC Application Object SIC Attribute (SIC Name)</td>
<td>Type the Secure Internal Communications (SIC) name of the OPSEC Application Object. The SIC name is the distinguished name (DN) of the application, for example: CN=LEA, o=fwconsole..7psasx.</td>
</tr>
</tbody>
</table>
Table 165. OPSEC/LEA protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Log Source SIC Attribute (Entity SIC Name) | Type the SIC name for the server that generates log sources.  
**Example:** cn=cp_mgmt,o=fwconsole..7psasx.                                                                                                         |
| Specify Certificate             | Select the **Specify Certificate** check box to define a certificate for this LEA configuration.                                                                                                           |
| Certificate Filename            | Type the file name of the certificate that you want to use for this configuration. The certificate file must be located in the /opt/qradar/conf/trusted_certificates/lea directory.                        |
| Certificate Authority IP        | Type the IP address of the SmartCenter server from which you want to pull your certificate.                                                                                                                   |
| Pull Certificate Password       | Type the password that you want to use when you request a certificate.                                                                                                                                 |
| OPSEC Application               | Type the name of the application you want to use when you request a certificate. This value can be up to 255 characters in length.                                                                           |

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

**What to do next**
You are now ready to verify your OPSEC/LEA communications for Check Point.

**Edit your OPSEC communications configuration**
This section describes how to modify your Check Point configuration to allow OPSEC communications on non-standard ports.
It also explains how to configure communications in a clear text, unauthenticated stream, and verify the configuration in IBM QRadar.

**Change your Check Point Custom Log Manager (CLM) IP address**
If your Check Point configuration includes a Check Point Custom Log Manager (CLM), you might eventually need to change the IP address for the CLM, which impacts any of the automatically discovered Check Point log sources from that CLM in QRadar. When you manually add the log source for the CLM by using the OPSEC/LEA protocol, all Check Point firewalls that forward logs to the CLM are automatically discovered by QRadar. These automatically discovered log sources cannot be edited. If the CLM IP address changes, you must edit the original Check Point CLM log source that contains the OPSEC/LEA protocol configuration and update the server IP address and log source identifier.

After you update the log source for the new Check Point CLM IP address, then any new events reported from the automatically discovered Check Point log sources are updated.

**Important:** Do not delete and re-create your Check Point CLM or automatically discovered log sources in QRadar. Deleting a log source does not delete event data, but can make finding previously recorded events more difficult.
Updating your Check Point OPSEC log source
You can update your Check Point OPSEC log source.

Procedure
1. Log in to IBM QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
4. Click the Log Sources icon.
5. Select the original Check Point CLM log source that contains the OPSEC/LEA protocol configuration and click Edit.
6. In the Log Source Identifier field, type a new identifying name of your Check Point CLM.
7. In the Server IP field, type the new IP address of your Check Point CLM.
8. Click Save.

The IP address update for your Check Point CLM in IBM QRadar is complete.

Changing the default port for OPSEC LEA communication
Change the default port (18184) on which OPSEC LEA communicates.

Procedure
1. At the command-line prompt of your Check Point SmartCenter Server, type the following command to stop the firewall services:

cpstop

2. Depending on your Check Point SmartCenter Server operating system, open the following file:
   • Linux - $FWDIR\conf\fwopsec.conf
   • Windows - %FWDIR%\conf\fwopsec.conf

   The default contents of this file are as follows:

   ```conf
   # The VPN-1 default settings are:
   # # sam_server auth_port 0 # sam_server port 18183
   # # lea_server auth_port 18184 # lea_server port 0
   # # ela_server auth_port 18187 # ela_server port 0
   # # cpmi_server auth_port 18190
   # # uaa_server auth_port 19191 # uaa_server port 0 #
   ```

3. Change the default lea_server auth_port from 18184 to another port number.
4. Remove the hash (#) mark from that line.

   Example:

   ```conf
   lea_server auth_port 18888 # lea_server port 0
   ```

5. Save and close the file.
6. Type the following command to start the firewall services:

cpstart

Configuring OPSEC LEA for unencrypted communications
You can configure the OPSEC LEA protocol for unencrypted communications:

Procedure
1. At the command-line prompt of your Check Point SmartCenter Server, stop the firewall services by typing the following command:

cpstop
2. Depending on your Check Point SmartCenter Server operating system, open the following file:
   - Linux - $FWDIR\conf\fwopsec.conf
   - Windows - %FWDIR%\conf\fwopsec.conf
3. Change the default `lea_server auth_port` from 18184 to 0.
4. Change the default `lea_server port` from 0 to 18184.
5. Remove the hash (#) marks from both lines.
   
   **Example:**
   
   `lea_server auth_port 0 lea_server port 18184`

6. Save and close the file.
7. Type the following command to start the firewall services:
   
   `cpstart`

### Configuring IBM QRadar to receive events from a Check Point device

Configure IBM QRadar to receive events from a Check Point device.

#### Procedure

1. Login 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 **Check Point**.
7. Using the **Protocol Configuration** list, select **OPSEC/LEA**.
8. Configure the following parameters:

<table>
<thead>
<tr>
<th>Table 166. OPSEC/LEA protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Server IP</td>
</tr>
<tr>
<td>Server Port</td>
</tr>
<tr>
<td>Use Server IP for Log Source</td>
</tr>
<tr>
<td>Statistics Report Interval</td>
</tr>
</tbody>
</table>
Table 166. OPSEC/LEA protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Type</strong></td>
<td>From the list, select the <strong>Authentication Type</strong> that you want to use for this LEA configuration. The options are sslca (default), sslca_clear, or clear. This value must match the authentication method that is used by the server. The following parameters appear if sslca or sslca_clear is selected as the authentication type:</td>
</tr>
<tr>
<td><strong>OPSEC Application Object SIC Attribute (SIC Name)</strong></td>
<td>Type the Secure Internal Communications (SIC) name of the OPSEC Application Object. The SIC name is the distinguished name (DN) of the application, for example: CN=LEA, o=fwconsole..7psasx. The name can be up to 255 characters in length and is case-sensitive.</td>
</tr>
<tr>
<td><strong>Log Source SIC Attribute (Entity SIC Name)</strong></td>
<td>Type the SIC name of the server, for example: cn=cp_mgmt,o=fwconsole..7psasx. The name can be up to 255 characters in length and is case-sensitive.</td>
</tr>
<tr>
<td><strong>Specify Certificate</strong></td>
<td>Select this check box if you want to define a certificate for this LEA configuration. QRadar attempts to retrieve the certificate by using these parameters when the certificate is needed.</td>
</tr>
<tr>
<td><strong>Certificate Filename</strong></td>
<td>This option appears only if Specify Certificate is selected. Type the file name of the certificate that you want to use for this configuration. The certificate file must be located in the /opt/qradar/conf/trusted_certificates/lea directory.</td>
</tr>
<tr>
<td><strong>Certificate Authority IP</strong></td>
<td>Type the IP address of the SmartCenter server from which you want to pull your certificate.</td>
</tr>
<tr>
<td><strong>Pull Certificate Password</strong></td>
<td>Type the password that you want to use when you request a certificate. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td><strong>OPSEC Application</strong></td>
<td>Type the name of the application you want to use when you request a certificate. This value can be up to 255 characters in length.</td>
</tr>
<tr>
<td><strong>Important:</strong></td>
<td>Access to port 18210 is required for certificate pulls.</td>
</tr>
</tbody>
</table>

9. Click **Save**.

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

**Integrate Check Point by using syslog**

This section describes how to ensure that the IBM QRadar Check Point DSMs accept Check Point events with syslog.

Before you configure IBM QRadar to integrate with a Check Point device, you must take the following steps:

**Important:** If Check Point SmartCenter is installed on Microsoft Windows, you must integrate Check Point with QRadar by using OPSEC.

1. Type the following command to access the Check Point console as an expert user:
A password prompt appears.

2. Type your expert console password. Press the Enter key.

3. Open the following file:
   /etc/rc.d/rc3.d/S99local

4. Add the following lines:
   ```
   $FWDIR/bin/fw log -ftn | /usr/bin/logger -p <facility>.<priority> /dev/null 2>&1 &
   ```

   Where:
   - `<facility>` is a syslog facility, for example, local3.
   - `<priority>` is a syslog priority, for example, info.

   For example:
   ```
   $FWDIR/bin/fw log -ftn | /usr/bin/logger -p local3.info > /dev/null 2>&1 &
   ```

5. Save and close the file.

6. Open the syslog.conf file.

7. Add the following line:
   ```
   <facility>.<priority> <TAB><TAB>@<host>
   ```

   Where:
   - `<facility>` is the syslog facility, for example, local3. This value must match the value that you typed in Step 4.
   - `<priority>` is the syslog priority, for example, info or notice. This value must match the value that you typed in Step 4.
   - `<TAB>` indicates you must press the Tab key.
   - `<host>` indicates the QRadar Console or managed host.

8. Save and close the file.

9. Enter the following command to restart syslog:
   - In Linux: `service syslog restart`
   - In Solaris: `/etc/init.d/syslog start`

10. Enter the following command:
    ```
    nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p <facility>.<priority> > /dev/null 2>&1 &
    ```

    Where:
    - `<facility>` is a Syslog facility, for example, local3. This value must match the value that you typed in Step 4.
    - `<priority>` is a Syslog priority, for example, info. This value must match the value that you typed in Step 4.

The configuration is complete. The log source is added to QRadar as Check Point syslog events are automatically discovered. Events that are forwarded to QRadar are displayed on the **Log Activity** tab.
Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Check Point. The following configuration steps are optional.

**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 **Check Point**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name for the log source, which is used as an identifier for the events that are forwarded from your Check Point appliance.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

**Integration of Check Point Firewall events from external syslog forwarders**
Check Point Firewall events can be forwarded from external sources, such as Splunk Forwarders, or other third-party syslog forwarders that send events to IBM QRadar.

When Check Point Firewall events are provided from external sources in syslog format, the events identify with the IP address in the syslog header. This identification causes events to identify incorrectly when they are processed with the standard syslog protocol. The syslog redirect protocol provides administrators a method to substitute an IP address from the event payload into the syslog header to correctly identify the event source.

To substitute an IP address, administrators must identify a common field from their Check Point Firewall event payload that contains the proper IP address. For example, events from Splunk Forwarders use `orig=` in the event payload to identify the original IP address for the Check Point firewall. The protocol substitutes in the proper IP address to ensure that the device is properly identified in the log source. As Check Point Firewall events are forwarded, QRadar automatically discovers and create new log sources for each unique IP address.

Substitutions are that are performed with regular expressions and can support either TCP or UDP syslog events. The protocol automatically configures iptables for the initial log source and port configuration. If an administrator decides to change the port assignment a Deploy Full Configuration is required to update the iptables configuration and use the new port assignment.

**Configuring a log source for Check Point forwarded events**
To collect raw events that are forwarded from an external source, you must configure a log source before events are forwarded to IBM QRadar.

**Procedure**
1. Log in to QRadar.
2. Click the **Admin** tab.
3. From 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 your log source.
8. From the **Log Source Type** list, select **Check Point**.
9. From the **Protocol Configuration** list, select **Syslog Redirect**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 168. Syslog redirect protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>
| Log Source Identifier Regex | Type the regular expression (regex) needed to identify the Check Point Firewall IP address from the event payload. **Example:** Administrators can use the following regular expression to parse Check Point Firewall events that are provided by Splunk Forwarders. 
```
orig=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
```

| Perform DNS Lookup On Regex Match | Select the **Perform DNS Lookup On Regex Match** check box to enable DNS functionality, which is based on the **Log Source Identifier** parameter value. By default, the check box is not selected. |
| Listen Port | Type the port number that is used by QRadar to accept incoming syslog redirect events. The default listen port is 517. The port number that you configure must match the port that you configured on the appliance that forwards the syslog events. Administrators cannot specify port 514 in this field. |
| Protocol | From the list, select either **UDP** or **TCP**. The syslog redirect protocol supports any number of UDP syslog connections, but restricts TCP connections to 2500. If the syslog stream has more than 2500 log sources, you must enter a second Check Point log source and listen port number. |
| Enabled | Select this check box to enable the log source. By default, the check box is selected. |
**Table 168. Syslog redirect protocol parameters (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credibility</strong></td>
<td>From the list, select the <strong>Credibility</strong> of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
<td>From the list, select the <strong>Target Event Collector</strong> to use as the target for the log source.</td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
<td>Select the <strong>Coalescing Events</strong> check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the <strong>Coalescing Events</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td><strong>Incoming Event Payload</strong></td>
<td>From the <strong>Incoming Event Payload</strong> list, select the incoming payload encoder for parsing and storing the logs.</td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
<td>Select the <strong>Store Event Payload</strong> check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the <strong>Store Event Payload</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

**Configuring Check Point to forward LEEF events to QRadar**

To forward LEEF events to IBM QRadar, use the Check Point Log Exporter and configure a new target for the logs.

**Before you begin**

Log Exporter can be installed on several versions of Check Point. Before you send events in LEEF format to QRadar, ensure that you have the correct version of Check Point and Log Exporter installed in your environment.

The following table describes where LEEF events are supported.
Table 169. Check Point versions that support LEEF

<table>
<thead>
<tr>
<th>Check Point version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>80.20</td>
<td>Log Exporter is included in this version.</td>
</tr>
<tr>
<td>80.10</td>
<td>Install Log Exporter and then install the hotfix after.</td>
</tr>
<tr>
<td>77.30</td>
<td>Install Log Exporter and then install the hotfix after.</td>
</tr>
</tbody>
</table>

Check Point 80.20
If you want to preserve the Log Exporter configuration before you upgrade to Check Point R80.20, follow the backup and restore Log Exporter instructions on the Check Point website. (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk127653).

Check Point R80.10
Ensure that Check Point version R80.10 is installed on the following servers:

- R80.10 Multi-Domain Log Server
- Security Management Server
- Log Server
- SmartEvent Server

You can install Log Exporter on version R80.10 Jumbo Hotfix Take 56 or later. The hotfix must be installed after Jumbo is installed. If you want to upgrade Jumbo, uninstall the hotfix, upgrade Jumbo, and then reinstall the hotfix. For more information, see the installation topic on the Check Point website (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323#Installation).

Check Point R77.30
Ensure that Check Point version R77.30 is installed on the following servers:

- Multi-Domain server
- Multi-Domain Log Server
- Log Server
- SmartEvent Server

You can install Log Exporter on version R77.30 Jumbo Hotfix Take 292 or later. The hotfix must be installed after Jumbo is installed. If you want to upgrade Jumbo, uninstall the hotfix, upgrade Jumbo, and then reinstall the hotfix. For more information, see the installation topic on the Check Point website (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323#Installation).

Procedure
1. To access the expert mode on the Check Point Log Exporter console, type `expert`.
2. Click *Enter* and then follow the prompts.

   The Event Hub Connection String contains the Namespace Name, the path to the Event Hub within the namespace, and the shared access signature (SAS) authentication information.

3. On the Check Point Log Exporter console, type the following command:

   ```
   cp_log_export add name <name> [domain-server <domain-server>] target-server <target-server IP address> target-port <target-port> protocol <(udp|tcp)> format <(syslog)|(cef)|(leef)> [optional arguments]
   ```

   A new target directory and default files are created in the $EXPORTERDIR/targets/<deployment_name> directory.

   The following table shows sample parameters and their values.
Table 170. Sample target configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td><code>&lt;service_name&gt;</code></td>
</tr>
<tr>
<td>Enabled</td>
<td>True</td>
</tr>
<tr>
<td>Target-server</td>
<td><code>&lt;QRadar_IP_address&gt;</code></td>
</tr>
<tr>
<td>Target-port</td>
<td>514</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Read-mode</td>
<td>Semi-unified</td>
</tr>
</tbody>
</table>

The default value for the Read-mode parameter is Semi-unified to ensure that complete data is collected.

For more information about other commands, go to the Check Point website (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323#Deployment Script Additional Commands).

4. To change a configuration, type `cp_log_export set`.
5. To verify a configuration in an existing deployment, type `cp_log_export show`.
6. To start Log Exporter automatically, type the following command: `cp_log_export restart`.

By default, Log Exporter doesn't start automatically.

Results
If QRadar isn't receiving events from Check Point, try these troubleshooting tips:

- Check the `$EXPORTERDIR/targets/<deployment_name>/conf/LeefFieldsMapping.xml` file for attributes-mapping issues.
- Check the `$EXPORTERDIR/targets/<deployment_name>/conf/LeefFormatDefinition.xml` file for LEEF header-mapping issues.
- Check the file paths. File paths might change with Check Point updates. If a configuration file can't be found, contact your Check Point administrator.

For more troubleshooting information, see the Troubleshooting Check Point Syslog LEEF Events from the Log Exporter (cp_log_export) Utility technote (https://www.ibm.com/support/docview.wss?uid=ibm10876650).

Check Point Multi-Domain Management (Provider-1)

You can configure IBM QRadar to integrate with a Check Point Multi-Domain Management (Provider-1) device.

All events from Check Point Multi-Domain Management (Provider-1) are parsed by using the Check Point Multi-Domain Management (Provider-1) DSM. You can integrate Check Point Multi-Domain Management (Provider-1) using one of the following methods:

- “Integrating syslog for Check Point Multi-Domain Management (Provider-1)” on page 313
- “Configuring OPSEC for Check Point Multi-Domain Management (Provider-1)” on page 314

Note: Depending on your Operating System, the procedures for using the Check Point Multi-Domain Management (Provider-1) device can vary. The following procedures are based on the Check Point SecurePlatform operating system.
Integrating syslog for Check Point Multi-Domain Management (Provider-1)
This method ensures that the Check Point Multi-Domain Management (Provider-1) DSM for IBM QRadar accepts Check Point Multi-Domain Management (Provider-1) events by using syslog.

About this task
QRadar records all relevant Check Point Multi-Domain Management (Provider-1) events.
Configure syslog on your Check Point Multi-Domain Management (Provider-1) device:

Procedure
1. Type the following command to access the console as an expert user:
   ```
   expert
   ```
   A password prompt is displayed.
2. Type your expert console password. Press the Enter key.
3. Type the following command:
   ```
   csh
   ```
4. Select the wanted customer logs:
   ```
   mdsenv <customer name>
   ```
5. Input the following command:
   ```
   # nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p <facility>.<priority> 2>&1 &
   ```
   Where:
   - `<facility>` is a syslog facility, for example, local3.
   - `<priority>` is a syslog priority, for example, info.
You are now ready to configure the log source in QRadar.

The configuration is complete. The log source is added to QRadar as the Check Point Multi-Domain Management Provider-1 syslog events are automatically discovered. Events that are forwarded to QRadar are displayed on the Log Activity tab.

Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Check Point Multi-Domain Management (Provider-1) as Check Point FireWall-1 events.

About this task
The following configuration steps are optional. To manually configure a log source for Check Point Multi-Domain Management (Provider-1) syslog events:

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 **Check Point Firewall-1**.
9. Using the **Protocol Configuration** list, select **Syslog**.

   The syslog protocol configuration is displayed.
10. Configure the following values:

    | Parameter               | Description                                                                 |
    |-------------------------|-----------------------------------------------------------------------------|
    | Log Source Identifier   | Type the IP address or host name for the log source as an identifier for events from your Check Point Multi-Domain Management (Provider-1) appliance. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

### Configuring OPSEC for Check Point Multi-Domain Management (Provider-1)

This method ensures that the IBM QRadar Check Point FireWall-1 DSM accepts Check Point Multi-Domain Management (Provider-1) events by using OPSEC.

### About this task

In the Check Point Multi-Domain Management (Provider-1) Management Domain GUI (MDG), create a host object that represents the QRadar. The **leapipe** is the connection between the Check Point Multi-Domain Management (Provider-1) and QRadar.

To reconfigure the Check Point Multi-Domain Management (Provider-1) SmartCenter (MDG):

### Procedure

1. To create a host object, open the Check Point SmartDashboard user interface and select **Manage > Network Objects > New > Node > Host**.
2. Type the Name, IP address, and write comments if needed.
3. Click **OK**.
4. Select **Close**.
5. To create the OPSEC connection, select **Manage > Servers and OPSEC Applications > New > OPSEC Application Properties**.
6. Type a Name, and write comments if needed.
    
   The Name that you enter must be different than the name used in Step 2.
7. From the **Host** drop-down menu, select the QRadar **host object** that you created.
8. From **Application Properties**, select **User Defined** as the Vendor type.
9. From **Client Entries**, select **LEA**.
10. To configure the Secure Internal Communication (SIC) certificate, click **Communication** and enter an activation key.
11. Select **OK** and then **Close**.
12. To install the Policy on your firewall, select **Policy > Install > OK**.
Configuring an OPSEC log source
You can configure the log source in IBM QRadar:

Procedure
1. Login to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
6. From the Log Source Type list, select Check Point FireWall-1.
7. Using the Protocol Configuration list, select OPSEC/LEA.
   The OPSEC/LEA protocol parameters are displayed
8. Log Source Name - Type a name for the log source.
9. Log Source Identifier - Type the IP address for the log source. This value must match the value that you typed in the Server IP parameter.
10. Server IP - Type the IP address of the Check Point Multi-Domain Management (Provider-1).
11. Server Port - Type the Port number that is used for OPSEC/LEA. The default is 18184.
   You must ensure that the existing firewall policy allows the LEA/OPSEC connection from your QRadar.
12. OPSEC Application Object SIC Attribute - Type the SIC DN of the OPSEC Application Object.
13. Log Source SIC Attribute - Type the SIC Name for the server that generates the log source.
   SIC attribute names can be up to 255 characters in length and are case-sensitive.
14. Specify Certificate - Ensure that the Specify Certificate check box is clear.
15. Pull Certificate Password - Type the activation key password.
16. Certificate Authority IP - Type the Check Point Manager Server IP address.
17. OPSEC Application - Type the name of the OPSEC Application that requests a certificate.
   Example: If the value is CN=QRadar-OPSEC,O=cpmodule...tdfaz, the OPSEC Application value is QRadar-OPSEC
18. Click Save.
19. On the Admin tab, click Deploy Changes.

Related concepts
“OPSEC/LEA protocol configuration options” on page 76
To receive events on port 18184, configure a log source to use the OPSEC/LEA protocol.

Configuring Check Point to forward LEEF events to QRadar
To forward LEEF events to IBM QRadar, use the Check Point Log Exporter and configure a new target for the logs.

Before you begin
Log Exporter can be installed on several versions of Check Point. Before you send events in LEEF format to QRadar, ensure that you have the correct version of Check Point and Log Exporter installed in your environment.

The following table describes where LEEF events are supported.
Table 172. Check Point versions that support LEEF

<table>
<thead>
<tr>
<th>Check Point version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>80.20</td>
<td>Log Exporter is included in this version.</td>
</tr>
<tr>
<td>80.10</td>
<td>Install Log Exporter and then install the hotfix after.</td>
</tr>
<tr>
<td>77.30</td>
<td>Install Log Exporter and then install the hotfix after.</td>
</tr>
</tbody>
</table>

**Check Point 80.20**
If you want to preserve the Log Exporter configuration before you upgrade to Check Point R80.20, follow the backup and restore Log Exporter instructions on the Check Point website. (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk127653).

**Check Point R80.10**
Ensure that Check Point version R80.10 is installed on the following servers:
- R80.10 Multi-Domain Log Server
- Security Management Server
- Log Server
- SmartEvent Server

You can install Log Exporter on version R80.10 Jumbo Hotfix Take 56 or later. The hotfix must be installed after Jumbo is installed. If you want to upgrade Jumbo, uninstall the hotfix, upgrade Jumbo, and then reinstall the hotfix. For more information, see the installation topic on the Check Point website (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323#Installation).

**Check Point R77.30**
Ensure that Check Point version R77.30 is installed on the following servers:
- Multi-Domain server
- Multi-Domain Log Server
- Log Server
- SmartEvent Server

You can install Log Exporter on version R77.30 Jumbo Hotfix Take 292 or later. The hotfix must be installed after Jumbo is installed. If you want to upgrade Jumbo, uninstall the hotfix, upgrade Jumbo, and then reinstall the hotfix. For more information, see the installation topic on the Check Point website (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323#Installation).

**Procedure**
1. To access the expert mode on the Check Point Log Exporter console, type `expert`.
2. Click `Enter` and then follow the prompts.

   The Event Hub Connection String contains the **Namespace Name**, the path to the Event Hub within the namespace, and the shared access signature (SAS) authentication information.

3. On the Check Point Log Exporter console, type the following command:

   ```bash
cp_log_export add name <name> [domain-server <domain-server>] target-server <target-server IP address> target-port <target-port> protocol <(udp|tcp)> format <(syslog)|(cef)|(leef)> [optional arguments]
   ``

   A new target directory and default files are created in the `$EXPORTERDIR/targets/<deployment_name>` directory.

   The following table shows sample parameters and their values.
Table 173. Sample target configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>&lt;service_name&gt;</td>
</tr>
<tr>
<td>Enabled</td>
<td>True</td>
</tr>
<tr>
<td>Target-server</td>
<td>&lt;QRadar_IP_address&gt;</td>
</tr>
<tr>
<td>Target-port</td>
<td>514</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Read-mode</td>
<td>Semi-unified</td>
</tr>
<tr>
<td></td>
<td>The default value for the Read-mode parameter is Semi-unified to ensure that complete data is collected.</td>
</tr>
</tbody>
</table>

For more information about other commands, go to the Check Point website (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_dGoGviewsolutiondetails=&solutionid=sk122323#Deployment Script Additional Commands).

4. To change a configuration, type `cp_log_export set`.
5. To verify a configuration in an existing deployment, type `cp_log_export show`.
6. To start Log Exporter automatically, type the following command: `cp_log_export restart`.
   By default, Log Exporter doesn't start automatically.

Results
If QRadar isn't receiving events from Check Point, try these troubleshooting tips:

- Check the $EXPORTERDIR/targets/<deployment_name>/conf/LeefFieldsMapping.xml file for attributes-mapping issues.
- Check the $EXPORTERDIR/targets/<deployment_name>/conf/LeefFormatDefinition.xml file for LEEF header-mapping issues.
- Check the file paths. File paths might change with Check Point updates. If a configuration file can't be found, contact your Check Point administrator.

For more troubleshooting information, see the Troubleshooting Check Point Syslog LEEF Events from the Log Exporter (cp_log_export) Utility technote (https://www.ibm.com/support/docview.wss?uid=ibm10876650).
IBM QRadar collects detailed audit events from Cilasoft QJRN/400 software for IBM i.

To collect events, administrators can configure Cilasoft QJRN/400 to forward events with syslog, or optionally configure the integrated file system (IFS) to write events to a file. Syslog provides real-time events to QRadar and provides automatic log source discovery for administrators, which is the easiest configuration method for event collection. The IFS option provides an optional configuration to write events to a log file, which can be read remotely by using the log file protocol. QRadar supports syslog events from Cilasoft QJRN/400 V5.14.K and later.

To configure Cilasoft QJRN/400, complete the following tasks:

1. On your Cilasoft QJRN/400 installation, configure the Cilasoft Security Suite to forward syslog events to QRadar or write events to a file.
2. For syslog configurations, administrators can verify that the events forwarded by Cilasoft QJRN/400 are automatically discovered on the Log Activity tab.

Cilasoft QJRN/400 configurations that use IFS to write event files to disk are considered an alternative configuration for administrators that cannot use syslog. IFS configurations require the administrator to locate the IFS file and configure the host system to allow FTP, SFTP, or SCP communications. A log source can then be configured to use the log file protocol with the location of the event log file.

### Configuring Cilasoft QJRN/400

To collect events, you must configure queries on your Cilasoft QJRN/400 to forward syslog events to IBM QRadar.

**Procedure**

1. To start the Cilasoft Security Suite, type the following command:
   ```
   IJRN/QJRN
   ```
   
   The account that is used to make configuration changes must have ADM privileges or USR privileges with access to specific queries through an Extended Access parameter.
2. To configure the output type, select one of the following options:
   
   To edit several selected queries, type 2EV to access the Execution Environment and change the Output Type field and type SEM.
3. To edit large numbers of queries, type the command CHGQJQRYA and change the Output Type field and type SEM.
4. On the Additional Parameters screen, configure the following parameters:

<table>
<thead>
<tr>
<th>Table 174. Cilasoft QJRN/400 output parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td><strong>Format</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>-----------</td>
</tr>
</tbody>
</table>
| **Output** | To configure an output type, use one of the following parameters to select an output type:  
  *SYSLOG* - Type this parameter to forward events with the syslog protocol. This option provides real-time events.  
  *IFS* - Type this parameter to write events to a file with the integrated file system. This option requires the administrator to configure a log source with the log file protocol. This option writes events to a file, which can be read in only 15-minute intervals. |
| **IP Address** | Enter the IP address of your IBM QRadar system.  
  If an IP address for IBM QRadar is defined as a special value in the WRKQJVAL command, you can type *CFG.  
  Events can be forwarded to either the QRadar Console, an Event Collector, an Event Processor, or your IBM QRadar all-in-one appliance. |
| **Port** | Type 514 or *CFG as the port for syslog events.  
  By default, *CFG automatically selects port 514. |
| **Tag** | This field is not used by IBM QRadar. |
| **Facility** | This field is not used by IBM QRadar. |
| **Severity** | Select a value for the event severity.  
  For more information about severity that is assigned to *QRY destinations, look up the command WRKQJFVAL in your Cilasoft documentation. |

For more information on Cilasoft configuration parameters, see the Cilasoft QJRN/400 User's Guide.

Syslog events that are forwarded to IBM QRadar are viewable on the Log Activity tab.

**Configuring a Cilasoft QJRN/400 log source**

IBM QRadar automatically discovers and creates a log source for syslog events that are forwarded from Cilasoft QJRN/400.

**About this task**
These configuration steps are optional.

**Procedure**
1. Log in to IBM QRadar.
2. Click the Admin tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. In the **Log Source Name** field, type a name for your log source.
6. From the **Log Source Type** list, select **Cilasoft QJRN/400**.
7. From the **Protocol Configuration** list, select **Syslog**.

**Note:** If Cilasoft QJRN/400 is configured to write events to the integrated file system with the *IFS option, the administrator must select **Log File**, and then configure the log file protocol.

8. Configure the protocol values.

**Learn more about syslog protocol parameters:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Enter the IP address as an identifier for events from your Cilasoft QJRN/400 installation. The <strong>Log Source Identifier</strong> must be unique value.</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>Select the <strong>Enabled</strong> check box to enable the log source. By default, the check box is selected.</td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
<td>Select the <strong>Credibility</strong> of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
<td>Select the <strong>Target Event Collector</strong> to use as the target for the log source.</td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
<td>Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the <strong>Coalescing Events</strong> list from the System Settings in IBM QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td><strong>Incoming Event Payload</strong></td>
<td>From the list, select the <strong>Incoming Event Payload</strong> encoder for parsing and storing the logs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>Select the <strong>Store Event Payload</strong> check box to enable the log source to store event payload information.</td>
</tr>
<tr>
<td></td>
<td>By default, automatically discovered log sources inherit the value of the <strong>Store Event Payload</strong> list from the System Settings in IBM QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

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

**Related concepts**

“**Log File protocol configuration options**” on page 62

To receive events from remote hosts, configure a log source to use the Log File protocol.
Chapter 42. Cisco

Several Cisco DSMs can be integrated with IBM QRadar.

Cisco ACE Firewall

The Cisco ACE firewall can be integrated with IBM QRadar.

QRadar can accept events that are forwarded from Cisco ACE Firewalls by using syslog. QRadar records all relevant events. Before you configure QRadar to integrate with an ACE firewall, you must configure your Cisco ACE Firewall to forward all device logs to QRadar.

Configuring Cisco ACE Firewall

To forward Cisco ACE device logs to IBM QRadar:

Procedure

1. Log in to your Cisco ACE device.
2. From the Shell Interface, select Main Menu > Advanced Options > Syslog Configuration.
3. The Syslog Configuration menu varies depending on whether there are any syslog destination hosts configured yet. If no syslog destinations are configured, create one by selecting the Add First Server option. Click OK.
4. Type the host name or IP address of the destination host and port in the First Syslog Server field. Click OK.
   The system restarts with new settings. When finished, the Syslog server window displays the host that is configured.
5. Click OK.
   The Syslog Configuration menu is displayed. Notice that options for editing the server configuration, removing the server, or adding a second server are now available.
6. If you want to add another server, click Add Second Server.
   At any time, click the View Syslog options to view existing server configurations.
7. To return to the Advanced menu, click Return.
   The configuration is complete. The log source is added to QRadar as Cisco ACE Firewall events are automatically discovered. Events that are forwarded to QRadar by Cisco ACE Firewall appliances are displayed on the Log Activity tab of QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Cisco ACE Firewalls.

About this task

The following configuration steps are optional. You can manually create a log source for QRadar to receive syslog events.

To manually configure a log source for Cisco ACE Firewall:

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
The Data Sources pane is displayed.
4. Click the Log Sources icon.
The Log Sources window is displayed.
5. Click Add.
The Add a log source window is displayed.
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 Cisco ACE Firewall.
9. From the Protocol Configuration list, select Syslog.
The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 176. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
The configuration is complete.

Cisco ACS

The Cisco ACS DSM for IBM QRadar accepts syslog ACS events by using syslog and UDP multiline. QRadar records all relevant and available information from the event. You can integrate Cisco ACS with QRadar by using one of the following methods:

- Configure your Cisco ACS device to directly send syslog to QRadar for Cisco ACS v5.x. See “Configuring Syslog for Cisco ACS v5.x” on page 324.
- Configure your Cisco ACS device to directly send syslog to QRadar for Cisco ACS v4.x. See “Configuring Syslog for Cisco ACS v4.x” on page 326.
- Configure your Cisco ACS device to directly send UDP multiline syslog to QRadar. See “Configuring UDP multiline syslog for Cisco ACS appliances” on page 99

Note: QRadar supports only Cisco ACS versions earlier than v3.x using a Universal DSM.

Configuring Syslog for Cisco ACS v5.x

The configuration of syslog forwarding from a Cisco ACS appliance with software version 5.x involves several steps.

About this task
You must complete the following tasks:

Procedure
1. Create a Remote Log Target
2. Configure global logging categories
3. Configure a log source
Creating a Remote Log Target
Creating a remote log target for your Cisco ACS appliance.
Log in to your Cisco ACS appliance.
On the navigation menu, click System Administration > Configuration > Log Configuration > Remote Log Targets.
The Remote Log Targets page is displayed.
Click Create.
Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the remote syslog target.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description for the remote syslog target.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Syslog.</td>
</tr>
<tr>
<td>IP address</td>
<td>Type the IP address of QRadar or your Event Collector.</td>
</tr>
</tbody>
</table>

Click Submit.
You are now ready to configure global policies for event logging on your Cisco ACS appliance.

Configuring global logging categories
To configure Cisco ACS to forward log failed attempts to IBM QRadar:

Procedure
1. On the navigation menu, click System Administration > Configuration > Log Configuration > Global.
   The Logging Categories window is displayed.
2. Select the Failed Attempts logging category and click Edit.
3. Click Remote Syslog Target.
4. From the Available targets window, use the arrow key to move the syslog target for QRadar to the Selected targets window.
5. Click Submit.
   You are now ready to configure the log source in QRadar.

Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Cisco ACS v5.x.

About this task
However, you can manually create a log source for QRadar to receive Cisco ACS events.
To manually configure a log source for Cisco ACS:

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
   The **Log Sources** window is displayed.
5. Click **Add**.
   The **Add a log source** window is displayed.
6. From the **Log Source Type** list, select **Cisco ACS**.
7. Using the **Protocol Configuration** list, select **Syslog**.
   The syslog protocol configuration is displayed.
8. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for Cisco ACS events.</td>
</tr>
</tbody>
</table>

9. Click **Save**.
10. On the **Admin** tab, click **Deploy Changes**.
    The configuration is complete.

### Configuring Syslog for Cisco ACS v4.x

The configuration of syslog forwarding from a Cisco ACS appliance with software version 4.x involves a few steps.

**About this task**
Complete the following steps:

**Procedure**
1. Configure syslog forwarding
2. Configure a log source

### Configuring syslog forwarding for Cisco ACS v4.x

Configuration of an ACS device to forward syslog events to IBM QRadar.

**About this task**
Take the following steps to configure the ACS device to forward syslog events to QRadar

**Procedure**
1. Log in to your Cisco ACS device.
2. On the navigation menu, click **System Configuration**.
   The **System Configuration** page opens.
3. Click **Logging**.
   The logging configuration is displayed.
4. In the Syslog column for **Failed Attempts**, click **Configure**.
   The **Enable Logging** window is displayed.
5. Select the **Log to Syslog Failed Attempts report** check box.
6. Add the following Logged Attributes:
7. Configure the following syslog parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Type the IP address of QRadar.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the syslog port number of IBM QRadar. The default is port 514.</td>
</tr>
<tr>
<td>Max message length (Bytes) - Type</td>
<td>Type 1024 as the maximum syslog message length.</td>
</tr>
</tbody>
</table>

**Note:** Cisco ACS provides syslog report information for a maximum of two syslog servers.

8. Click **Submit**.

You are now ready to configure the log source in QRadar.

**Configuring a log source for Cisco ACS v4.x**

IBM QRadar automatically discovers and creates a log source for syslog events from Cisco ACS v4.x.

**About this task**

The following configuration steps are optional.

To manually create a log source for Cisco ACS v4.x, take the following steps:

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   - The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
   - The **Log Sources** window is displayed.
5. Click **Add**.
   - The **Add a log source** window is displayed.
6. From the **Log Source Type** list, select **Cisco ACS**.
7. Using the **Protocol Configuration** list, select **Syslog**.
   - The syslog protocol configuration is displayed.
8. Configure the following values:
Table 180. Syslog parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for Cisco ACS events.</td>
</tr>
</tbody>
</table>

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

The configuration is complete.

**Configuring UDP multiline syslog for Cisco ACS appliances**

The Cisco ACS DSM for IBM Security QRadar accepts syslog events from Cisco ACS appliances with log sources that are configured to use the UDP Multiline Syslog protocol.

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the Data Sources section, click the **Log Sources** icon, and then click **Add**.
4. In the **Log Source Name** field, type a name for your log source.
5. From the **Log Source Type** list, select **Cisco ACS**.
6. From the **Protocol Configuration** list, select **UDP Multiline Syslog**.
7. Configure the parameters:

   The following parameters require specific values to collect events from Cisco ACS appliances:

   **Table 181. Cisco ACS log source parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address, host name, or name to identify your Cisco ACS appliance.</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The default port number that is used by QRadar to accept incoming UDP Multiline Syslog events is 517. You can use a different port. The valid port range is 1 - 65535.</td>
</tr>
<tr>
<td></td>
<td>To edit a saved configuration to use a new port number, complete the following steps.</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Listen Port</strong> field, type the new port number for receiving UDP Multiline Syslog events.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>The port update is complete and event collection starts on the new port number.</td>
</tr>
<tr>
<td>Message ID Pattern</td>
<td>\s(\d{10})\s</td>
</tr>
<tr>
<td>Event Formatter</td>
<td>Select <strong>Cisco ACS Multiline</strong> from the list.</td>
</tr>
</tbody>
</table>

**Related concepts**

“UDP multiline syslog protocol configuration options” on page 96
To create a single-line syslog event from a multiline event, configure a log source to use the UDP multiline protocol. The UDP multiline syslog protocol uses a regular expression to identify and reassemble the multiline syslog messages into single event payload.

**Cisco Aironet**

You can integrate Cisco Aironet devices with IBM QRadar.

**About this task**

A Cisco Aironet DSM accepts Cisco Emblem Format events by using syslog. Before you configure QRadar to integrate with a Cisco Aironet device, you must configure your Cisco Aironet appliance to forward syslog events.

To configure Cisco Aironet to forward events:

**Procedure**

1. Establish a connection to the Cisco Aironet device by using one of the following methods:
   - Telnet to the wireless access point
   - Access the console
2. Type the following command to access privileged EXEC mode:
   ```
   enable
   ```
3. Type the following command to access global configuration mode:
   ```
   config terminal
   ```
4. Type the following command to enable message logging:
   ```
   logging on
   ```
5. Configure the syslog facility. The default is local7.
   ```
   logging <facility>
   ```
   where `<facility>` is, for example, local7.
6. Type the following command to log messages to your QRadar:
   ```
   logging <IP address>
   ```
   where `<IP address>` is IP address of your QRadar.
7. Enable **timestamp** on log messages:
   ```
   service timestamp log datatime
   ```
8. Return to privileged EXEC mode:
   ```
   end
   ```
9. View your entries:
   ```
   show running-config
   ```
10. Save your entries in the configuration file:
    ```
    copy running-config startup-config
    ```

The configuration is complete. The log source is added to QRadar as Cisco Aironet events are automatically discovered. Events that are forwarded to QRadar by Cisco Aironet appliances are displayed on the **Log Activity** tab of QRadar.
Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Cisco Aironet.

About this task
The following configuration steps are optional. To manually configure a log source for Cisco Aironet:

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 Cisco Aironet.
9. From the Protocol Configuration list, select Syslog.
   The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 182. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.

Cisco ASA
You can integrate a Cisco Adaptive Security Appliance (ASA) with IBM QRadar.

A Cisco ASA DSM accepts events through syslog or NetFlow by using NetFlow Security Event Logging (NSEL). QRadar records all relevant events. Before you configure QRadar, you must configure your Cisco ASA device to forward syslog or NetFlow NSEL events.

Choose one of the following options:
- Forward events to QRadar by using syslog. See “Integrate Cisco ASA Using Syslog” on page 330
- Forward events to QRadar by using NetFlow (NSEL). See “Integrate Cisco ASA for NetFlow by using NSEL” on page 332

Integrate Cisco ASA Using Syslog
Integrating Cisco ASA by using syslog involves the configuration of a log source, and syslog forwarding.

Complete the following tasks to integrate Cisco ASA by using syslog:
Configuring syslog forwarding

To configure Cisco ASA to forward syslog events, some manual configuration is required.

Procedure

1. Log in to the Cisco ASA device.
2. Type the following command to access privileged EXEC mode:
   ```
   enable
   ```
3. Type the following command to access global configuration mode:
   ```
   conf t
   ```
4. Enable logging:
   ```
   logging enable
   ```
5. Configure the logging details:
   ```
   logging console warning
   logging trap warning
   logging asdm warning
   ```
   Note: The Cisco ASA device can also be configured with logging trap informational to send additional events. However, this may increase the event rate (Events Per Second) of your device.
6. Type the following command to configure logging to IBM QRadar:
   ```
   logging host <interface> <IP address>
   ```
   Where:
   - `<interface>` is the name of the Cisco Adaptive Security Appliance interface.
   - `<IP address>` is the IP address of QRadar.
   Note: Using the command `show interfaces` displays all available interfaces for your Cisco device.
7. Disable the output object name option:
   ```
   no names
   ```
   Disable the output object name option to ensure that the logs use IP addresses and not the object names.
8. Exit the configuration:
   ```
   exit
   ```
9. Save the changes:
   ```
   write mem
   ```

Results

The configuration is complete. The log source is added to QRadar as Cisco ASA syslog events are automatically discovered. Events that are forwarded to QRadar by Cisco ASA are displayed on the Log Activity tab of QRadar.
**Configuring a log source**

IBM QRadar automatically discovers and creates a log source for syslog events from Cisco ASA. The following configuration steps are optional.

**About this task**

To manually configure a log source for Cisco ASA syslog events:

**Procedure**

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 Cisco Adaptive Security Appliance (ASA).
9. From the Protocol Configuration list, select Syslog.
   The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your OSSEC installations.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.

**Integrate Cisco ASA for NetFlow by using NSEL**

Integrating Cisco ASA for Netflow by using NSEL involves two steps.

This section includes the following topics:

- “Configuring NetFlow Using NSEL” on page 332
- “Configuring a log source” on page 334

**Configuring NetFlow Using NSEL**

You can configure Cisco ASA to forward NetFlow events by using NSEL.

**Procedure**

1. Log in to the Cisco ASA device command-line interface (CLI).
2. Type the following command to access privileged EXEC mode:
   ```enable```
3. Type the following command to access global configuration mode:
   ```conf t```
4. Disable the output object name option:
   ```no names```
5. Type the following command to enable NetFlow export:
   ```flow-export destination <interface-name> <ipv4-address or hostname> <udp-port>```
   Where:
   - `<interface-name>` is the name of the Cisco Adaptive Security Appliance interface for the NetFlow collector.
   - `<ipv4-address or hostname>` is the IP address or host name of the Cisco ASA device with the NetFlow collector application.
   - `<udp-port>` is the UDP port number to which NetFlow packets are sent.
   **Note:** IBM QRadar typically uses port 2055 for NetFlow event data on QRadar QFlow Collectors. You must configure a different UDP port on your Cisco Adaptive Security Appliance for NetFlow by using NSEL.
6. Type the following command to configure the NSEL class-map:
   ```class-map flow_export_class```
7. Choose one of the following traffic options:
   To configure a NetFlow access list to match specific traffic, type the command:
   ```match access-list flow_export_acl```
8. To configure NetFlow to match any traffic, type the command:
   ```match any```
   **Note:** The Access Control List (ACL) must exist on the Cisco ASA device before you define the traffic match option in “Configuring NetFlow Using NSEL” on page 332.
9. Type the following command to configure the NSEL policy-map:
   ```policy-map flow_export_policy```
10. Type the following command to define a class for the flow-export action:
    ```class flow_export_class```
11. Type the following command to configure the flow-export action:
    ```flow-export event-type all destination <IP address>```
    Where `<IP address>` is the IP address of QRadar.
    **Note:** If you are using a Cisco ASA version before v8.3 you can skip “Configuring NetFlow Using NSEL” on page 332 as the device defaults to the flow-export destination. For more information, see your Cisco ASA documentation.
12. Type the following command to add the service policy globally:
    ```service-policy flow_export_policy global```
13. Exit the configuration:
    ```exit```
14. Save the changes:
    ```write mem```
You must verify that your collector applications use the Event Time field to correlate events.
Configuring a log source

To integrate Cisco ASA that uses NetFlow with IBM QRadar, you must manually create a log source to receive NetFlow events.

About this task

QRadar does not automatically discover or create log sources for syslog events from Cisco ASA devices that use NetFlow and NSEL.

Note: Your system must be running the current version of the NSEL protocol to integrate with a Cisco ASA device that uses NetFlow and NSEL. The NSEL protocol is available on IBM Support, http://www.ibm.com/support, or through auto updates in QRadar.

To configure a log source:

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   - The Data Sources pane is displayed.
4. Click the Log Sources icon.
   - The Log Sources window is displayed.
5. Click Add.
   - The Add a log source window is displayed.
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 Cisco Adaptive Security Appliance (ASA).
9. Using the Protocol Configuration list, select Cisco NSEL.
   - The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source.</td>
</tr>
<tr>
<td>Collector Port</td>
<td>Type the UDP port number that is used by Cisco ASA to forward NSEL events. The valid range of the Collector Port parameter is 1-65535.</td>
</tr>
<tr>
<td></td>
<td>QRadar typically uses port 2055 for NetFlow event data on the QRadar QFlow Collector. You must define a different UDP port on your Cisco</td>
</tr>
<tr>
<td></td>
<td>Adaptive Security Appliance for NetFlow that uses NSEL.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

   The log source is added to QRadar. Events that are forwarded to QRadar by Cisco ASA are displayed on the Log Activity tab. For more information on configuring NetFlow with your Cisco ASA device, see your vendor documentation.
The IBM QRadar DSM for Cisco advanced malware protection (Cisco AMP) collects event logs from your Cisco AMP for Endpoints platform. The Cisco AMP DSM uses the RabbitMQ protocol.

To integrate Cisco AMP with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the following RPMs on your QRadar Console.
   **Important:** You need QRadar V7.2.8 Patch 9 (V7.2.8.20170726184122) or later to install the RabbitMQ Protocol RPM.
   - Protocol Common RPM
   - DSMCommon RPM
   - RabbitMQ Protocol RPM
   - Cisco AMP DSM RPM

2. Create a Cisco AMP Client ID and API key. Alternatively, you can request access to an already created event stream from your administrator. For more information about creating these values, go to the Creating a Cisco AMP Client ID and API key procedure.

3. Create a Cisco AMP event stream. For more information about creating the event stream, go to the “Creating a Cisco AMP event stream” on page 337 procedure.

4. Add a Cisco AMP log source on the QRadar Console for a user to manage the Cisco AMP event stream.

**Related concepts**

“Configure a log source for a user to manage the Cisco AMP event stream” on page 338
Configure a log source in QRadar to manage a specific event stream that you want QRadar to collect events from.

**Related tasks**

“Adding a DSM” on page 4

**Cisco AMP DSM specifications**

The following table describes the specifications for the Cisco AMP DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Cisco</td>
</tr>
<tr>
<td>DSM</td>
<td>Cisco AMP</td>
</tr>
<tr>
<td>RPM name</td>
<td>DSM-CiscoAMP-QRadar_version-Build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>RabbitMQ</td>
</tr>
<tr>
<td>Event format</td>
<td>Cisco AMP</td>
</tr>
</tbody>
</table>
Creating a Cisco AMP Client ID and API key for event queues

A Cisco AMP administrator must create a Client ID and an API key in the Cisco AMP for Endpoints Portal. These keys are used to manage queues.

Before you begin
If you do not have Administrator privileges, request the Client ID and API key values from your Administrator. If you want QRadar to automatically manage the event stream, you need these values when you configure a log source in QRadar.

Procedure
1. Log in to the Cisco AMP for Endpoints Portal as an administrator.
2. Click Accounts > API Credentials.
3. In the API Credentials pane, click New API Credential.
4. In the Application name field, type a name, and then select Read & Write.
   Note: You must have Read & Write access to manage event streams on your Cisco AMP for Endpoints platform.
5. Click Create.
6. From the API Key Details section, make note of the values for the 3rd Party API Client ID and the API Key. You need these values to manage queues.

What to do next
Create a Cisco AMP event stream.

Related concepts
“Configure a log source for a user to manage the Cisco AMP event stream” on page 338
Configure a log source in QRadar to manage a specific event stream that you want QRadar to collect events from.

Related tasks
“Creating a Cisco AMP event stream” on page 337
The Cisco AMP for Endpoints API returns the Advanced Message Queuing Protocol (AMQP) credentials in several Cisco AMP for Endpoints API query responses.

“Adding a log source” on page 4

### Table 185. Cisco AMP DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recorded event types</td>
<td>All security events</td>
</tr>
<tr>
<td></td>
<td>For a detailed list of supported events, go to the Cisco AMP for Endpoints API documentation. (<a href="https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fevent_types&amp;amp;api_host=api.amp.cisco.com&amp;amp;api_resource=Event+Type&amp;amp;api_version=v1">https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fevent_types&amp;amp;api_host=api.amp.cisco.com&amp;amp;api_resource=Event+Type&amp;amp;api_version=v1</a>) Note: Network traffic is supported only for Data Flow Control (DCF) events.</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Cisco website (<a href="https://api-docs.amp.cisco.com/">https://api-docs.amp.cisco.com/</a>)</td>
</tr>
</tbody>
</table>
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 Cisco AMP event stream**

The Cisco AMP for Endpoints API returns the Advanced Message Queuing Protocol (AMQP) credentials in several Cisco AMP for Endpoints API query responses.

**Procedure**

1. Download the curl command line tool from the [curl download website](https://curl.haxx.se/download.html).

2. To create a Cisco AMP event stream, type the following command. You will need the parameter values when you configure a log source in QRadar.

   ```bash
curl -X POST -H 'accept: application/json' 
-H 'content-type: application/json' --compressed 
-H 'Accept-Encoding: gzip, deflate' 
-d '{"name": "<STREAMNAME>", "event_type": [553648130, 554696714, 554696715, 1091567628, 2165309453, 1090519054, 553648143, 2164260880, 570425394, 553648151, 553648155, 2164260892, 2164260893, 553648158, 2164260903, 570425397, 570425398, 570425399, 1090524040, 1090524041, 1090519084, 1107296257], 
"group_guid": ["0a00a0aa-0000-0000-0000-000000000000"], 
"event_types": [553648130, 554696714], 
"amqp_credentials": { 
"user_name": "1116-aa00a000-0000-0000-0000-000000000000", 
"password": "1116-aa00a000-0000-0000-0000-000000000000"}, 
"group_guid": ["0a00a0aa-0000-0000-0000-000000000000"], 
"event_types": [553648130, 554696714]
}' 
-u '<CLIENTID:APIKEY'> 
'https://api.amp.cisco.com/v1/event_streams'
```

Where:

- `<STREAMNAME>` is a name of your choosing for the event stream.
- `<group_guid>` is the group GUID that you want to use to link to the `<0a00a0aa-0000-0000-0000-000000000000>` event stream.
- `<CLIENTID:APIKEY>` is the **Client ID** and the **API key** that you created.

If you are in the Asia Pacific Japan and China (APJC) region, change `'https://api.amp.cisco.com/v1/event_streams'` to `'https://api.apjc.amp.cisco.com/v1/event_streams'`.

If you are in the European region, change `'https://api.amp.cisco.com/v1/event_streams'` to `'https://api.eu.amp.cisco.com/v1/event_streams'`.

**Sample Query Response:**

```json
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": "https://api.amp.cisco.com/v1/event_streams"
    }
  },
  "data": {
    "id": 2216,
    "name": "STREAMNAME",
    "group_guids": ["0a00a0aa-0000-0000-0000-000000000000"],
    "event_types": [553648130, 554696714],
    "amqp_credentials": {
      "user_name": "1116-aa00a00000000000000", 
      "password": "1116-aa00a00000000000000"
    }
  }
}
```
What to do next
Configure a log source in QRadar for a user to manage the Cisco AMP event stream.

Related concepts
“Configure a log source for a user to manage the Cisco AMP event stream” on page 338

Configure a log source in QRadar to manage a specific event stream that you want QRadar to collect events from.

Related tasks
“Adding a log source” on page 4

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

Configure a log source for a user to manage the Cisco AMP event stream

Configure a log source in QRadar to manage a specific event stream that you want QRadar to collect events from.

To connect to a specific Cisco AMP event stream, you also need to have access to the Advanced Message Queuing Protocol (AMQP) credentials that are provided by the Cisco AMP for Endpoints API.

The Cisco AMP for Endpoints API is used to manage event streams. For more information about supported queries to manage the Cisco AMP for Enpoint API, see Cisco AMP for Endpoints API (https://api-docs.amp.cisco.com/).

Important: If an issue occurs while you use the Cisco AMP for Endpoints API, contact your Cisco administrator for assistance. For Cisco contact information, see Cisco Support (https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html).

The following table describes the parameters that require specific values to collect events from the Cisco AMP for Endpoints API by using the RabbitMQ protocol:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Cisco AMP</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>RabbitMQ</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique name for the log source. The Log Source Identifier can be any valid value and does not need to reference a specific server. The Log Source Identifier can be the same value as the Log Source Name. If more than one Cisco AMP log source is configured, you might identify the first log source as CiscoAMP1, the second log source as CiscoAMP2, and so on.</td>
</tr>
<tr>
<td>Event Format</td>
<td>You must select Cisco AMP.</td>
</tr>
</tbody>
</table>
Table 186. RabbitMQ protocol log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name that is used for the Cisco AMP for Endpoints API event stream. You can find the IP or host name in the AMQP credentials field. For more information about AMQP credentials, see Creating a Cisco AMP event stream.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that is used for the Cisco AMP for Endpoints API event stream. You can find the port number in the AMQP credentials field. For more information about AMQP credentials, see Creating a Cisco AMP event stream.</td>
</tr>
<tr>
<td>Queue</td>
<td>The queue name that is used for the Cisco AMP for Endpoints API event stream. You can find the queue name value in the AMQP credentials field. For more information about the AMQP credentials, see “Creating a Cisco AMP event stream” on page 337.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name that is used for the Cisco AMP for Endpoints API event stream. You can find the user name value in the AMQP credentials field. For more information about AMQP credentials, see “Creating a Cisco AMP event stream” on page 337.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is used for the Cisco AMP for Endpoints API event stream. You can find the password value in the AMQP credentials field. For more information about AMQP credentials, see “Creating a Cisco AMP event stream” on page 337.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The upper limit for the maximum number of events per second (EPS). The default is 5000.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>Select Yes for QRadar to automatically download the server certificate and begin trusting the target server. If you select No, server certificates are not retrieved.</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Sample event message

Use this sample event messages as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when you use the RabbitMQ protocol for the Cisco AMP DSM:
Cisco CallManager

The Cisco CallManager DSM for IBM QRadar collects application events that are forwarded from Cisco CallManager devices that are using Syslog.

Before events can be received in QRadar, you must configure your Cisco Call Manager device to forward events. After you forward Syslog events from Cisco CallManager, QRadar automatically detects and adds Cisco CallManager as a log source.

Configuring syslog forwarding

You can configure syslog on your Cisco CallManager:

**Procedure**

1. Log in to your Cisco CallManager interface.
2. Select **System Enterprise > Parameters**.
3. In the **Remote Syslog Server Name** field, type the IP address of the QRadar Console.
4. From the **Syslog Severity For Remote Syslog messages** list, select **Informational**.

The informational severity selection allows the collection of all events at the information level and later.
5. Click **Save**.
6. Click **Apply Config**.

The syslog configuration is complete. You are now ready to configure a syslog log source for Cisco CallManager.
Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Cisco CallManager devices.

About this task
The following configuration steps are optional. To manually configure a syslog log source for Cisco CallManager take the following steps:

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 Cisco Call Manager.
   The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 188. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.

Cisco CatOS for Catalyst Switches
The Cisco CatOS for Catalyst Switches DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant device events. Before you configure a Cisco CatOS device in QRadar, you must configure your device to forward syslog events.

Configuring syslog
Configuring your Cisco CatOS device to forward syslog events.

About this task
Take the following steps to configure your Cisco CatOS device to forward syslog events:
**Procedure**

1. Log in to your Cisco CatOS user interface.
2. Type the following command to access privileged EXEC mode:
   ```
   enable
   ```
3. Configure the system to **timestamp** messages:
   ```
   set logging timestamp enable
   ```
4. Type the following command with the IP address of IBM QRadar:
   ```
   set logging server <IP address>
   ```
5. Limit messages that are logged by selecting a severity level:
   ```
   set logging server severity <server severity level>
   ```
6. Configure the facility level to be used in the message. The default is local7.
   ```
   set logging server facility <server facility parameter>
   ```
7. Enable the switch to send syslog messages to the QRadar.
   ```
   set logging server enable
   ```
You are now ready to configure the log source in QRadar.

**Configuring a log source**

IBM QRadar automatically discovers and creates a log source for syslog events from Cisco CatOS appliances.

**About this task**

The following configuration steps are optional.

To manually configure a syslog log source for Cisco CatOS:

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
   The **Log Sources** window is displayed.
5. Click **Add**.
   The **Add a log source** window is displayed.
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 **Cisco CatOS for Catalyst Switches**.
9. Using the **Protocol Configuration** list, select **Syslog**.
   The syslog protocol configuration is displayed.
10. Configure the following values:
### Table 189. Syslog parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Cisco CatOS for Catalyst Switch appliance.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

---

**Cisco Cloud Web Security**

The IBM QRadar DSM for Cisco Cloud Web Security (CWS) collects web usage logs from a Cisco Cloud Web Security (CWS) storage by using an Amazon S3 - compatible API.

The following table describes the specifications for the Cisco Cloud Web Security DSM:

### Table 190. Cisco Cloud Web Security DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Cisco</td>
</tr>
<tr>
<td>DSM name</td>
<td>Cisco Cloud Web Security</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CiscoCloudWebSecurity-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Amazon AWS S3 REST API</td>
</tr>
<tr>
<td>Event format</td>
<td>W3C</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All web usage logs</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate Cisco Cloud Web Security with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs, in the order that they are listed, on your QRadar Console:
   - Protocol Common RPM
   - Amazon AWS REST API Protocol RPM
   - DSMCommon RPM
   - Cisco Cloud Web Security DSM RPM
2. Enable Log Extraction in your Cisco ScanCenter (administration portal).
3. Add a Cisco Cloud Web Security log source on the QRadar Console. The following table describes the parameters that require specific values for Cisco Cloud Web Security event collection:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Cisco Cloud Web Security</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Amazon AWS S3 REST API</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The Log Source Identifier can be any valid value and does not need</td>
</tr>
<tr>
<td></td>
<td>to reference a specific server. The Log Source Identifier can be</td>
</tr>
<tr>
<td></td>
<td>the same value as the Log Source Name. If you configured more than</td>
</tr>
<tr>
<td></td>
<td>one Cisco CWS log source, you might want to identify the first log</td>
</tr>
<tr>
<td></td>
<td>source as ciscocws1, the second log source as ciscocws2, and the</td>
</tr>
<tr>
<td></td>
<td>third log source as ciscocws13.</td>
</tr>
<tr>
<td>Signature Version</td>
<td>Select Signature Version 2.</td>
</tr>
<tr>
<td></td>
<td>If your Cisco CWS API is using Signature Version 4, contact your</td>
</tr>
<tr>
<td></td>
<td>system administrator.</td>
</tr>
<tr>
<td>Region Name (Signature V4 only)</td>
<td>The region that is associated with the Amazon S3 bucket.</td>
</tr>
<tr>
<td>Service Name (Signature V4 only)</td>
<td>Type s3. The name of the Amazon Web Service.</td>
</tr>
<tr>
<td>Bucket Name</td>
<td>The name of the Cisco CWS bucket where the log files are stored.</td>
</tr>
<tr>
<td>Endpoint URL</td>
<td><a href="https://vault.scansafe.com/">https://vault.scansafe.com/</a></td>
</tr>
<tr>
<td>Public Key</td>
<td>The access key to enable log extraction from the Cisco CWS bucket.</td>
</tr>
<tr>
<td>Access Key</td>
<td>The secret key to enable log extraction from the Cisco CWS bucket.</td>
</tr>
<tr>
<td>Directory Prefix</td>
<td>The location of the root directory on the Cisco CWS storage bucket</td>
</tr>
<tr>
<td></td>
<td>from where the Cisco CWS logs are retrieved. For example, the root</td>
</tr>
<tr>
<td></td>
<td>directory location might be cws-logs/.</td>
</tr>
<tr>
<td>File Pattern</td>
<td>.*?.txt.gz</td>
</tr>
<tr>
<td>Event Format</td>
<td>W3C. The log source retrieves W3C text formatted events.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>When a proxy is configured, all traffic for the log source travels</td>
</tr>
<tr>
<td></td>
<td>through the proxy so that QRadar can access the Amazon AWS S3</td>
</tr>
<tr>
<td></td>
<td>buckets. Configure the Proxy Server, Proxy Port, Proxy Username,</td>
</tr>
<tr>
<td></td>
<td>and Proxy Password fields. If the proxy does not require</td>
</tr>
<tr>
<td></td>
<td>authentication, leave the Proxy Username and Proxy Password fields</td>
</tr>
<tr>
<td></td>
<td>blank.</td>
</tr>
<tr>
<td>Automatically Acquire Server</td>
<td>If you select Yes, QRadar downloads the certificate and begins</td>
</tr>
<tr>
<td>Certificate(s)</td>
<td>trusting the target server.</td>
</tr>
</tbody>
</table>
Table 191. Cisco Cloud Web Security log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurrence</td>
<td>Specifies how often the Amazon AWS S3 REST API Protocol connects to the Cisco CWS API to check for new files, and retrieves them if they exist. The format is M/H/D for Months/Hours/Days. The default is 5 M. Every access to an AWS S3 bucket incurs a monetary cost to the account that owns the bucket. Therefore, a smaller recurrence value increases the cost.</td>
</tr>
</tbody>
</table>

The following table shows a sample event message from Cisco Cloud Web Security:

Table 192. Cisco Cloud Web Security sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>c:comp - block</td>
<td>Access Denied</td>
<td>2016-08-22 18:22:34 GMT &lt;IP_address1&gt; &lt;IP_address1&gt; GET http <a href="http://www.example.com">www.example.com</a> 88 / Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0 0 0 0 &lt;IP_address2&gt; c:comp Block all block category Computers and Internet &lt;IP_address1&gt; 0 Unknown</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Cloud Web Security to communicate with QRadar

To send events from Cloud Web Security to IBM QRadar, you must enable log extraction in Cisco CWS ScanCenter.

Before you begin
The log extraction service must be enabled and provisioned for your company. You must have super user administrator privileges to access the Log Extraction page.

Procedure
1. Log in to your Cisco ScanCenter account.
2. Click the Admin tab to view the administration menus.
3. From the Your Account menu, click Log Extraction.
4. In the Actions column in the Credentials area, click Issue Key.
5. In the Warning dialog box, click Issue & Download.

A key pair is issued and the keypair.csv file is downloaded.

The Access Key and Last issued column values are updated. The secret key does not display in the user interface (UI).
6. Open the keypair.csv file and make a copy of the `accessKey` and `secretKey`. The keypair.csv file contains a 20 character string access key and a 40 character string secret key. The key pair values that you copied are used when you configure the log source in QRadar.

7. From the **Connection Details** pane, copy and record the values in the **Endpoint** and **Bucket** columns. The connection details values that you copied are used when you configure the log source in QRadar.

**What to do next**

Configure the log source in QRadar.

For more information about Cisco CWS log extraction, see the [*Cisco ScanCenter Administrator Guide*, Release 5.2](https://search.cisco.com/search?query=cisco%20scancenter%20administrator%20guide&locale=enUS&tab=Cisco).

**Related tasks**

- “Adding a log source” on page 4
- If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

---

**Cisco CSA**

You can integrate a Cisco Security Agent (CSA) server with IBM QRadar.

The Cisco CSA DSM accepts events by using syslog, SNMPv1, and SNMPv2. QRadar records all configured Cisco CSA alerts.

**Configuring syslog for Cisco CSA**

Configuration of your Cisco CSA server to forward events.

**About this task**

Take the following steps to configure your Cisco CSA server to forward events:

**Procedure**

1. Open the **Cisco CSA** user interface.
2. Select **Events > Alerts**.
3. Click **New**.
   - The **Configuration View** window is displayed.
4. Type in values for the following parameters:
   - **Name** - Type a name that you want to assign to your configuration.
   - **Description** - Type a description for the configuration. This step is not a requirement.
5. From the **Send Alerts**, select the event set from the list to generate alerts.
6. Select the **SNMP** check box.
7. Type a Community name.
   - The Community name that is entered in the CSA user interface must match the Community name that is configured on IBM QRadar. This option is only available for the SNMPv2 protocol.
8. For the **Manager IP address** parameter, type the IP address of QRadar.
9. Click **Save**.
   - You are now ready to configure the log source in QRadar.
Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Cisco CSA appliances.

About this task
To manually configure a syslog log source for Cisco CSA, take the following configuration steps, which are optional:

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 Cisco CSA.
   The syslog protocol configuration is displayed.
10. Configure the following values:
    
    | Table 193. Syslog parameters |
    |-----------------------------|
    | Parameter | Description |
    | Log Source Identifier | Type the IP address or host name for the log source as an identifier for events from your Cisco CSA appliance. |

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.

Cisco Firepower Management Center
The IBM QRadar DSM for Cisco Firepower Management Center collects Cisco Firepower Management Center events by using the eStreamer API service.

Cisco Firepower Management Center is formerly known as Cisco FireSIGHT Management Center.

QRadar supports Cisco Firepower Management Center V 5.2 to V 6.4.

Configuration overview
To integrate QRadar with Cisco Firepower Management Center, you must create certificates in the Firepower Management Center interface, and then add the certificates to the QRadar appliances that receive eStreamer event data.

If your deployment includes multiple Cisco Firepower Management Center appliances, you must copy the certificate for each appliance that sends eStreamer events to any temporary location on the QRadar Event
Collector. The certificate allows the Cisco Firepower Management Center appliance and the QRadar Console or QRadar Event Collectors to communicate by using the eStreamer API to collect events.

To integrate QRadar with Cisco Firepower Management Center, complete the following steps:
1. Create the eStreamer certificate on your Firepower Management Center appliance.
2. Import a Cisco Firepower Management Center certificate in QRadar.
3. Configure a log source in QRadar for your Firepower Management Center appliances.

**Supported event types**

QRadar supports the following event types from Cisco Firepower Management Center:

- Discovery Events
- Correlation and White List Events
- Impact Flag Alerts
- User Activity
- Malware Events
- File Events
- Connection Events
- Intrusion Events
- Intrusion Event Packet Data
- Intrusion Event Extra Data

Intrusion events that are categorized by the Cisco Firepower Management 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 Cisco Firepower Management 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 Cisco Firepower Management Center.

The following table provides sample event messages for the Cisco Firepower Management Center DSM:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login Change Event</td>
<td>Computer Account Changed</td>
<td>DeviceType=Estreamer    DeviceAddress ==&lt;IP_address&gt;    CurrentTime=150774    0597988    netmapId=0    recordTyp e=USER_LOGIN_CHANGE_EVENT    record Length=142    timestamp=01 May 201 5 12:13:50    detectionEngineRef= 0    ipAddress=&lt;IP_address&gt;    MACAddress s=&lt;MAC_address&gt;    hasIPv6=true    eventSecond=1430491035    eventMicroSecond=0    eventType=USER LOGIN_INFORMATION    fileNumber=00    ipAddress=&lt;IP_address&gt;    userLoginInformation.timestamp=1430491035    userLoginInformation.userName=username    userLoginInformation.userRef=0    userLoginInformation.protocolRef=710    userLoginInformation.ipv6Ad dress=&lt;IP_address&gt;    userLoginIn formation.loginType=0    userLoginIn formation.reportedBy=IPAddress&quot;</td>
</tr>
</tbody>
</table>
Table 194. Cisco Firepower Management Center sample messages supported by the Cisco Firepower Management Center device. (continued)

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Removed Change Event</td>
<td>User Account Removed</td>
<td>DeviceType=Estreamer DeviceAddress=&lt;IP_address&gt; 43344985 netmapId=0 recordType=USER_REMOVED_CHANGE_EVENT recordLength=191 timestamp=21 Sep 2017 14:53:14 detectionEngineRef=0 ipAddress=&lt;IP_address&gt; MACAddress=&lt;MAC_address&gt; hasIPv6=true eventSecond=1506016392 eventMicroSecond=450775 eventType=DELETE_USER_IDENTITY fileNumber=00000000 filePosition=00000000 ipAddress=&lt;IPv6_address&gt; userInformation.userName=username userInformation.lastName=lastname userInformation.email=EmailAddress userInformation.department=Research userInformation.phone=000-000-0000</td>
</tr>
<tr>
<td>INTRUSION EVENT EXTRA DATA RECORD</td>
<td>Information</td>
<td>DeviceType=Estreamer DeviceAddress=&lt;IP_address&gt; 06690263 netmapId=0 recordType=INTRUSION_EVENT_EXTRA_DATA_RECORD recordLength=49 timestamp=01 May 2015 15:32:53 eventExtraData.eventId=393275 eventExtraData.eventSecond=1430505172 eventExtraData.managedDeviceId=6 eventExtraData.managedDevice.name=manageddevice.&lt;Server&gt;.example.com eventExtraData.eventExtraDataType.eventExtraDataType.name=HTTP Hostname eventExtraData.eventExtraDataType.encoding=String eventExtraData.eventExtraDataType.eventExtraData=www.example.com</td>
</tr>
<tr>
<td>RUA User record</td>
<td>Information</td>
<td>DeviceType=Estreamer DeviceAddress=&lt;IP_address&gt; 40603372 netmapId=0 recordType=RUA_USER_RECORD recordLength=21 timestamp=11 Oct 2017 13:50:02 userRef=2883 protocolRef=710 userName=UserName</td>
</tr>
</tbody>
</table>

Related tasks

“Creating Cisco Firepower Management Center 5.x and 6.x certificates” on page 350
IBM QRadar requires a certificate for every Cisco Firepower Management Center appliance in your deployment. Certificates are generated in pkcs12 format and must be converted to a keystore and a truststore file, which are usable by QRadar appliances.

“Importing a Cisco Firepower Management Center certificate in QRadar” on page 351
The estreamer-cert-import.pl script for QRadar converts your pkcs12 certificate file to a keystore and truststore file and copies the certificates to your QRadar appliance. Repeat this procedure for each Firepower Management Center pkcs12 certificate that you need to import to your QRadar Console or Event Collector.

“Configuring a log source for Cisco Firepower Management Center events” on page 352
QRadar does not automatically discover Cisco Firepower Management Center events. You must configure a log source in QRadar.

“Adding a DSM” on page 4

Creating Cisco Firepower Management Center 5.x and 6.x certificates
IBM QRadar requires a certificate for every Cisco Firepower Management Center appliance in your deployment. Certificates are generated in pkcs12 format and must be converted to a keystore and a truststore file, which are usable by QRadar appliances.

Procedure
1. Log in to your Cisco Firepower Management Center interface.
   • If you are using version 5.x, select System > Local > Registration.
   • If you are using version 6.x, select System > Integration.
2. Click the eStreamer tab.
3. Select the types of events that you want Cisco Firepower Management Center to send to QRadar, and then click Save.
   The following image lists the types of events that Cisco Firepower Management Center sends to QRadar.

![eStreamer Event Configuration](image)

*Figure 7. Cisco Firepower Management Center eStreamer Event Configuration*

4. Click Create Client in the upper right side of the window.
5. In the Hostname field, type the IP address or host name, depending on which of the following conditions applies to your environments.
   • If you use a QRadar Console or you use a QRadar All-in-One appliance to collect eStreamer events, type the IP address or host name of your QRadar Console.
   • If you use a QRadar Event Collector to collect eStreamer events, type the IP address or host name for the Event Collector.
   • If you use QRadar High Availability (HA), type the virtual IP address.
6. In the **Password** field, type a password for your certificate. If you choose to provide a password, the password is required to import the certificate.

7. Click **Save**.

   The new client is added to the eStreamer Client list and the host can communicate with the eStreamer API on port 8302.

8. Click **Download Certificate** 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 Cisco Firepower Management Center certificate to your QRadar appliance.

**Related tasks**

“Importing a Cisco Firepower Management Center certificate in QRadar” on page 351

The estreamer-cert-import.pl script for QRadar converts your pkcs12 certificate file to a keystore and truststore file and copies the certificates to your QRadar appliance. Repeat this procedure for each Firepower Management Center pkcs12 certificate that you need to import to your QRadar Console or Event Collector.

**Importing a Cisco Firepower Management Center certificate in QRadar**

The estreamer-cert-import.pl script for QRadar converts your pkcs12 certificate file to a keystore and truststore file and copies the certificates to your QRadar appliance. Repeat this procedure for each Firepower Management Center pkcs12 certificate that 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 import script is stored on your QRadar Event Collector when you install the Cisco Firepower eStreamer protocol.

The script converts and imports only 1 pkcs12 file at a time. You are required to import a certificate only for the QRadar appliance that receives the Firepower Management Center events. For example, after the Firepower Management Center 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 Firepower Management Center certificates on the QRadar appliance are renamed to estreamer.keystore.old and estreamer.truststore.old.

**Procedure**

1. Log in as the root user by using SSH on the QRadar appliance that will receive the events.

2. Copy the downloaded certificate from your Firepower Management Center appliance to a temporary directory on the QRadar Event Collector.

3. Type the following command to import your pkcs12 file.

   ```bash
   /opt/qradar/bin/estreamer-cert-import.pl -f <pkcs12_absolute_filepath> options
   ```

   The `-f` parameter is required. All other parameters that are described in the following table are optional.
Table 195. Import script command parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f</td>
<td>Identifies the file name of the pkcs12 files to import.</td>
</tr>
<tr>
<td>-o</td>
<td>Overrides the default eStreamer name for the keystore and truststore files. Use the -o parameter when you integrate multiple Firepower Management Center devices. For example, /opt/qradar/bin/estreamer-cert-import.pl -f &lt;file name&gt; -o &lt;IP_address&gt;</td>
</tr>
<tr>
<td>-d</td>
<td>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.</td>
</tr>
<tr>
<td>-p</td>
<td>Specifies a password if a password was provided when you generated the pkcs12 file.</td>
</tr>
<tr>
<td>-v</td>
<td>Displays the version information for the import script.</td>
</tr>
<tr>
<td>-h</td>
<td>Displays a help message about using the import script.</td>
</tr>
</tbody>
</table>

Results
The import script displays the location where the import files were copied.

Example:
```
[root@FM199-22 ~]# /opt/qradar/bin/estreamer-cert-import.pl -f yourCertificate.pkcs12 -o 61estreamer
Successfully generated truststore file [/opt/qradar/conf/61estreamer.truststore].
Successfully generated keystore file [/opt/qradar/conf/61estreamer.keystore].
```

Figure 8. Sample import script output

Configuring a log source for Cisco Firepower Management Center events
QRadar does not automatically discover Cisco Firepower Management Center events. You must configure a log source in QRadar.

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, and then click Add.
5. From the Log Source Type list, select Cisco Firepower Management Center.
6. From the Protocol Configuration list, select Cisco Firepower eStream.
7. Configure the following parameters:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>The IP address or host name of the Cisco Firepower Management Center device.</td>
</tr>
<tr>
<td>Server Port</td>
<td>The port number that the Cisco Firepower Management Center device is configured to accept connection requests on. The default port that QRadar uses for the Cisco Firepower Management Center device is 8302.</td>
</tr>
<tr>
<td>Keystore Filename</td>
<td>The directory path and file name for the keystore private key and associated certificate. By default, the import script creates the keystore file in the following directory: /opt/qradar/conf/estreamer.keystore</td>
</tr>
<tr>
<td>Truststore Filename</td>
<td>The directory path and file name for the truststore files. The truststore file contains the certificates that are trusted by the client. By default, the import script creates the truststore file in the following directory: /opt/qradar/conf/estreamer.truststore</td>
</tr>
<tr>
<td>Request Extra Data</td>
<td>Select this option to request intrusion event extra data from Cisco Firepower Management Center. For example, extra data includes the original IP address of an event.</td>
</tr>
</tbody>
</table>
| Domain                       | **Note:** Domain Streaming Requests are only supported for eStreamer version 6.x. Leave the Domain field blank for eStreamer version 5.x.  

The domain where the events are streamed from.  
The value in the Domain field must be a fully qualified domain. This means that all ancestors of the desired domain must be listed starting with the top-level domain and ending with the leaf domain that you want to request events from.  
Example:  
Global is the top level domain, B is a second level domain that is a subdomain of Global, and C is a third-level domain and a leaf domain that is a subdomain of B. To request events from C, type the following value for the Domain parameter:  
Global \ B \ C |

8. Click **Save**.

**Cisco FWSM**

You can integrate Cisco Firewall Service Module (FWSM) with IBM QRadar.

The Cisco FWSM DSM for QRadar accepts FWSM events by using syslog. QRadar records all relevant Cisco FWSM events.
Configuring Cisco FWSM to forward syslog events

To integrate Cisco FWSM with IBM QRadar, you must configure your Cisco FWSM appliances to forward syslog events to QRadar.

About this task
To configure Cisco FWSM:

Procedure
1. Using a console connection, telnet, or SSH, log in to the Cisco FWSM.
2. Enable logging:
   ```
   logging on
   ```
3. Change the logging level:
   ```
   logging trap <level>
   ```
   Where `<level>` is set from levels 1-7. By default, the logging trap level is set to 3 (error).
4. Designate QRadar as a host to receive the messages:
   ```
   logging host [interface] ip_address [tcp[/port] | udp[/port]] [format emblem]
   ```
   For example:
   ```
   logging host dmz1 192.0.2.1
   ```
   Where 192.0.2.1 is the IP address of your QRadar system.
   You are now ready to configure the log source in QRadar.

Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Cisco FWSM appliances.

About this task
The following configuration steps are optional. To manually configure a syslog log source for Cisco FWSM, take the following steps:

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 Cisco Firewall Services Module (FWSM).
   The syslog protocol configuration is displayed.
10. Configure the following values:
Cisco Identity Services Engine

The IBM QRadar DSM for Cisco Identity Services Engine (ISE) collects device events from Cisco ISE appliances by using the UDP Multiline Syslog protocol.

The following table describes the specifications for the Cisco Identity Services Engine DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Cisco</td>
</tr>
<tr>
<td>DSM name</td>
<td>Cisco Identity Services Engine</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CiscoISE-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>1.1 to 2.2</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP Multiline Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Device events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate Cisco ISE 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. RPMs are available for download from the IBM support website ([http://www.ibm.com/support](http://www.ibm.com/support)):
   - DSMCommon RPM
   - Cisco Identity Services Engine DSM RPM
2. Configure your Cisco ISE appliance to send UDP Multiline Syslog events to QRadar.
3. Add a Cisco Identity Services Engine log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from Cisco ISE:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Cisco FWSM appliance.</td>
</tr>
</tbody>
</table>
Table 198. Cisco Identity Services Engine log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Cisco Identity Service Engine</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>UDP Multiline Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the Cisco Identity Service Engine device that sends UDP Multiline Syslog events to QRadar.</td>
</tr>
</tbody>
</table>
| Listen Port                | Type 517 as the port number used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65535. **Note:** UDP Multiline Syslog events can be assigned to any port that is not in use, except for port 514. The default port that is assigned to the UDP Multiline protocol is UDP port 517. For a list of ports that are used by QRadar, see *Common ports and servers used by QRadar* in the *IBM QRadar Administration Guide* or in the IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_adm_ports_and_servers.html). To edit a saved configuration to use a new port number, complete the following steps:  
  a. In the **Listen Port** field, type the new port number for receiving UDP Multiline Syslog events.  
  b. Click **Save**.  
   The port update is complete and event collection starts on the new port number. |
| Message ID Pattern         | Type the following regular expression (regex) to filter the event payload messages:  
  CISE_\S+ (\d{10})                                                                 |

4. Configure a remote logging target on your Cisco ISE appliance.
5. Configure the event logging categories on your Cisco ISE appliance.
6. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Cisco Identity Services Engine:
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTHEN_PASSED</td>
<td>Admin Login Successful</td>
<td><code>&lt;181&gt;Jan 26 15:00:15 cisco.ise.test.com CISE_Administrative_and_Operational_Audit 0000003812 1 0 2015-01-26 15:00:15.510 +00:00 000008620 51001 NOTICE Administrator -Login: Administrator authentication succeeded, ConfigVersionId=84, AdminInterface=GUI, AdminIPAddress=x.x.x.x, AdminSession=0DE370E5527018DA537F60AAAAA, AdminName=adminUser, OperationMessage Text=Administrator authentication successful,</code></td>
</tr>
<tr>
<td>FAILED_ATTEMPT</td>
<td>General Authentication Failed</td>
<td><code>&lt;181&gt;Oct 31 16:35:39 isi CISE_Failed_Attempts 0000199854 2017-10-31 16:35:39.919 +01:00 0021309086 5400 NOTICE Failed-Attempt: Authentication failed, ConfigVersionId=4, Device IP Address=x.x.x.x, Device Port=33987, DestinationIPAddress=x.x.x.x, DestinationPort=1812, RadiusPacketType=AccessRequest, UserName=admin, Protocol=Radius, RequestLatency=8, NetworkDeviceName=device1, UserName=admin, NAS-Identifier=12782c2b-747a-4894-9689-0000000000, NetworkDeviceProfileName=Cisco, NetworkDeviceProfileId=efb762c5-9082-4c79-a101-000000000000, IsThirdPartyDeviceFlow=false, AcsSessionID=isi/298605301/000000, AuthenticationMethod=PAP_ASCII, SelectedAccessService=Default Network Access, FailureReason=22056 Subject not found in the applicable identity store(s), Step=11001, Step=11017, Step=11117, Step=15049, Step=15008, Step=15048, Step=15048, Step=15048, Step=15006, Step=15013, Step=24210, Step=24216, Step=22056, Step=22058, Step=22061, Step=11003</code></td>
</tr>
</tbody>
</table>

**Related concepts**

“UDP multiline syslog protocol configuration options” on page 96

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

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4
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 a remote logging target in Cisco ISE” on page 358
To forward syslog events to IBM QRadar, you must configure your Cisco ISE appliance with a remote logging target.

“Configuring logging categories in Cisco ISE” on page 358
The Cisco Identity Services Engine DSM for IBM QRadar collects syslog events from multiple event logging categories. To define which events are forwarded to QRadar, you must configure each event logging category on your Cisco ISE appliance.

Configuring a remote logging target in Cisco ISE
To forward syslog events to IBM QRadar, you must configure your Cisco ISE appliance with a remote logging target.

Procedure
1. Log in to your Cisco ISE Administration Interface.
2. From the navigation menu, select Administration > System > Logging > Remote Logging Targets.
3. Click Add, and then configure the following parameters:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for the remote target system.</td>
</tr>
<tr>
<td>Description</td>
<td>You can uniquely identify the target system for users.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Type the IP address of the QRadar Console or Event Collector.</td>
</tr>
<tr>
<td>Port</td>
<td>Type 517 or use the port value that you specified in your Cisco ISE log source for QRadar</td>
</tr>
<tr>
<td>Facility Code</td>
<td>From the Facility Code list, select the syslog facility to use for logging events.</td>
</tr>
<tr>
<td>Maximum Length</td>
<td>Type 1024 as the maximum packet length allowed for the UDP syslog message.</td>
</tr>
</tbody>
</table>
4. Click Submit.

What to do next
Configure the logging categories that are forwarded by Cisco ISE to QRadar.

Configuring logging categories in Cisco ISE
The Cisco Identity Services Engine DSM for IBM QRadar collects syslog events from multiple event logging categories. To define which events are forwarded to QRadar, you must configure each event logging category on your Cisco ISE appliance.

Procedure
1. Log in to your Cisco ISE Administration Interface.
2. From the navigation menu, select Administration > System > Logging > Logging Categories.
   The following list shows the supported event logging categories for the IBM QRadar DSM for Cisco Identity Services Engine:
   - AAA audit
   - Failed attempts
   - Passed authentication
   - AAA diagnostics
   - Administrator authentication and authorization
• Authentication flow diagnostics
• Identity store diagnostics
• Policy diagnostics
• Radius diagnostics
• Guest
• Accounting
• Radius accounting
• Administrative and operational audit
• Posture and client provisioning audit
• Posture and client provisioning diagnostics
• Profiler
• System diagnostics
• Distributed management
• Internal operations diagnostics
• System statistics

3. Select an event logging category, and then click Edit.
4. From the Log Severity list, select a severity for the logging category.
5. In the Target field, add your remote logging target for QRadar to the Select box.
6. Click Save.
7. Repeat this process for each logging category that you want to forward to QRadar.

Events that are forwarded by Cisco ISE are displayed on the Log Activity tab in QRadar.

Cisco IDS/IPS

The Cisco IDS/IPS DSM for IBM QRadar polls Cisco IDS/IPS for events by using the Security Device Event Exchange (SDEE) protocol.

About this task

The SDEE specification defines the message format and the protocol that is used to communicate the events that are generated by your Cisco IDS/IPS security device. QRadar supports SDEE connections by polling directly to the IDS/IPS device and not the management software, which controls the device.

Note: You must have security access or web authentication on the device before you connect to QRadar.

After you configure your Cisco IDS/IPS device, you must configure the SDEE protocol in QRadar. When you configure the SDEE protocol, you must define the URL required to access the device.

For example, https://www.example.com/cgi-bin/sdee-server.

You must use an http or https in the URL, which is specific to your Cisco IDS version:

• If you are using RDEP (for Cisco IDS v4.0), check that /cgi-bin/event-server is at the end of the URL.

  For example, https://www.example.com/cgi-bin/event-server

• If you are using SDEE/CIDEE (for Cisco IDS v5.x and later), check that /cgi-bin/sdee-server is at the end of the URL.

  For example, https://www.example/cgi-bin/sdee-server

QRadar does not automatically discover or create log sources for syslog events from Cisco IDS/IPS devices. To integrate Cisco IDS/IPS device events with QRadar, you must manually create a log source for each Cisco IDS/IPS in your network.
To configure a Cisco IDS/IPS log source by using SDEE polling:

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   - The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
   - The **Log Sources** window is displayed.
5. Click **Add**.
   - The **Add a log source** window is displayed.
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 **Cisco Intrusion Prevention System (IPS)**.
9. Using the **Protocol Configuration** list, select SDEE.
   - The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th><strong>Table 200. SDEE parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>URL</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Events / Query</td>
</tr>
</tbody>
</table>
Table 200. SDEE parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Subscription</td>
<td>Select this check box if you want to force a new SDEE subscription. By default, the check box is selected. The check box forces the server to drop the least active connection and accept a new SDEE subscription connection for this log source. Clearing the check box continues with any existing SDEE subscription.</td>
</tr>
<tr>
<td>Severity Filter Low</td>
<td>Select this check box if you want to configure the severity level as low. Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.</td>
</tr>
<tr>
<td>Severity Filter Medium</td>
<td>Select this check box if you want to configure the severity level as medium. Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.</td>
</tr>
<tr>
<td>Severity Filter High</td>
<td>Select this check box if you want to configure the severity level as high. Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The log source is added to QRadar. Events that are polled from your Cisco IDS/IPS appliances are displayed on the Log Activity tab of QRadar.

Cisco IOS

You can integrate Cisco IOS series devices with IBM QRadar.

The Cisco IOS DSM for QRadar accepts Cisco IOS events by using syslog. QRadar records all relevant events. The following Cisco Switches and Routers are automatically discovered as Cisco IOS series devices, and their events are parsed by the Cisco IOS DSM:

- Cisco 12000 Series Routers
- Cisco 6500 Series Switches
- Cisco 7600 Series Routers
- Cisco Carrier Routing System
- Cisco Integrated Services Router.

Note: Make sure all Access Control Lists (ACLs) are set to LOG.

Configuring Cisco IOS to forward events

You can configure a Cisco IOS-based device to forward events.

About this task
Take the following steps to configure your Cisco device:
**Procedure**

1. Log in to your Cisco IOS Server, switch, or router.
2. Type the following command to log in to the router in privileged-exec:
   ```
   enable
   ```
3. Type the following command to switch to configuration mode:
   ```
   conf t
   ```
4. Type the following commands:
   ```
   logging <IP address>
   logging source-interface <interface>
   ```
   Where:
   - `<IP address>` is the IP address of the IBM QRadar host and the SIM components.
   - `<interface>` is the name of the interface, for example, dmz, lan, ethernet0, or ethernet1.
5. Type the following to configure the priority level:
   ```
   logging trap warning
   logging console warning
   ```
   Where `warning` is the priority setting for the logs.
6. Configure the syslog facility:
   ```
   logging facility syslog
   ```
7. Save and exit the file.
8. Copy the `running-config` to `startup-config` by typing the following command:
   ```
   copy running-config startup-config
   ```
   You are now ready to configure the log source in QRadar.

The configuration is complete. The log source is added to QRadar as Cisco IOS events are automatically discovered. Events that are forwarded to QRadar by Cisco IOS-based devices are displayed on the **Log Activity** tab of QRadar.

**Configuring a log source**

IBM QRadar automatically discovers and creates a log source for syslog events from Cisco IOS.

**About this task**

The following configuration steps are optional. To manually configure a log source for Cisco IOS-based devices, take the following steps:

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   - The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
   - The **Log Sources** window is displayed.
5. Click **Add**.
   - The **Add a log source** window is displayed.
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 one of the following devices:

- Cisco IOS
- Cisco 12000 Series Routers
- Cisco 6500 Series Switches
- Cisco 7600 Series Routers
- Cisco Carrier Routing System
- Cisco Integrated Services Router

9. Using the **Protocol Configuration** list, select **Syslog**.

The syslog protocol configuration is displayed.

10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Cisco IOS-based device.</td>
</tr>
</tbody>
</table>

11. Click **Save**.

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

The configuration is complete.

---

**Cisco IronPort**

IBM QRadar DSM for Cisco IronPort retrieves logs from the following Cisco products: Cisco IronPort, Cisco Email Security Appliance (ESA), and Cisco Web Security Appliance (WSA). The Cisco IronPort DSM retrieves web content filtering events (W3C format), Text Mail Logs, and System Logs.

To integrate Cisco IronPort with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the [IBM Support Website](https://www.ibm.com/support/fixcentral/) onto your QRadar Console:
   - Log File Protocol RPM
   - Cisco IronPort DSM RPM
2. Configure Cisco IronPort to communicate with QRadar.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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

**Cisco IronPort DSM specifications**

The following table describes the specifications for the Cisco IronPort DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Cisco</td>
</tr>
</tbody>
</table>
### Table 202. Cisco IronPort DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSM name</td>
<td>Cisco IronPort</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CiscoIronPort-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>• Cisco IronPort: V5.5, V6.5, V7.1, V7.5</td>
</tr>
<tr>
<td></td>
<td>• Cisco ESA: V10.0</td>
</tr>
<tr>
<td></td>
<td>• Cisco WSA: V10.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog: Cisco IronPort, Cisco WSA</td>
</tr>
<tr>
<td></td>
<td>Log File Protocol: Cisco IronPort, Cisco ESA</td>
</tr>
<tr>
<td>Event format</td>
<td>W3C</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Text Mail Logs, System Logs, Web Content, Filtering Events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

### Configuring Cisco IronPort appliances to communicate with QRadar

Complete the configuration on Cisco IronPort appliances so that they can send events to QRadar.

**Procedure**

1. To configure your Cisco IronPort Appliance to push Web Content Filter events, you must configure a log subscription for the Web Content Filter that uses the W3C format. For more information, see your Cisco IronPort documentation.


**Note:** When you add a log subscription on your Cisco Web Security Appliance (WSA), the Log Style parameter value must be **Squid**.
Configuring a Cisco IronPort and Cisco ESA log source by using the log file protocol

You can configure a log source on the QRadar Console so that Cisco IronPort and Cisco Email Security Appliance (ESA) can communicate with QRadar by using the log file protocol.

Procedure

Configure a Cisco IronPort log source on the QRadar Console by using the log file protocol. The following tables describe the Log File log source parameters that require specific values for retrieving logs from Cisco IronPort and Cisco ESA.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Cisco IronPort</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Log File Protocol</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The <strong>Log Source Identifier</strong> can be any valid value, including the same value as the <strong>Log Source Name</strong> parameter, and doesn't need to reference a specific server.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the <strong>Remote IP or Hostname</strong> field has the SFTP subsystem enabled.</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>Type the IP address or host name of the device that contains the event log files.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Type the port that is used to communicate with the remote host. The valid range is 1 - 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.</td>
</tr>
<tr>
<td>Remote User</td>
<td>Type the user name necessary to log in to the host that contains the event files.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Type the password necessary to log in to the host.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password necessary to log in to the host.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>If the system is configured to use key authentication, type the path to the SSH key. When an SSH key file is used, the <strong>Remote Password</strong> field is ignored.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>Type the directory location on the remote host from which the files are retrieved. The directory path is relative to the user account that is used to log in.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>For FTP only. If the log files are in the remote user’s home directory, you can leave the remote directory blank. A blank remote directory field supports systems where a change in the working directory (CWD) command is restricted.</td>
</tr>
<tr>
<td>Recursive</td>
<td>Select this check box to enable the file pattern to search sub folders. By default, the check box is clear.</td>
</tr>
<tr>
<td></td>
<td>This option is ignored for SCP file transfers.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>Must use a regular expression that matches the log files that are generated.</td>
</tr>
<tr>
<td></td>
<td>The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that end with .log, type the following command:  .*.log.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the Oracle Java documentation (<a href="http://docs.oracle.com/javase/tutorial/essential/regex/">http://docs.oracle.com/javase/tutorial/essential/regex/</a>).</td>
</tr>
<tr>
<td>Start Time</td>
<td>Type the time of day for the log source to start the file import.</td>
</tr>
<tr>
<td></td>
<td>This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>Type a time interval to determine how frequently the remote directory is scanned for new event log files. The minimum value is 15 minutes.</td>
</tr>
<tr>
<td></td>
<td>The time interval can include values in hours (H), minutes (M), or days (D). For example, a recurrence of 2H scans the remote directory every 2 hours.</td>
</tr>
<tr>
<td>Run On Save</td>
<td>Select this check box to start the log file import immediately after the administrator saves the log source.</td>
</tr>
<tr>
<td></td>
<td>After the first file import, the log file protocol follows the start time and recurrence schedule that is defined by the administrator.</td>
</tr>
<tr>
<td></td>
<td>When selected, this check box clears the list of previously downloaded and processed files.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that the protocol cannot exceed. The valid range is 100 - 5000.</td>
</tr>
<tr>
<td>Processor</td>
<td>From the list, select gzip.</td>
</tr>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>Select this check box to track files that were processed by the log file protocol. QRadar examines the log files in the remote directory to determine if a file was 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 weren’t previously processed are downloaded. This option only applies to FTP and SFTP Service Types.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>Select this check box to define the local directory on the QRadar Console for storing downloaded files during processing. Administrators can leave this check box clear for more configurations. When this check box is selected, the Local Directory field is displayed so that you can configure the local directory to use for storing files.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>W3C. The Event Generator uses W3C to process the web content filter log files.</td>
</tr>
<tr>
<td>File Encoding</td>
<td>From the list box, select the character encoding that is used by the events in your log file.</td>
</tr>
</tbody>
</table>
| Folder Separator                  | Type the character that is used to separate folders for your operating system. The default value is /.
Most configurations can use the default value in Folder Separator field.
This field is intended for operating systems that use a different character to define separate folders. For example, periods that separate folders on mainframe systems. |

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 a Cisco IronPort and Cisco WSA log source by using the Syslog protocol**

You can configure a log source on the QRadar Console so that the Cisco IronPort Appliance and Cisco Web Security Appliance (WSA) can communicate with QRadar by using the Syslog protocol.

**Procedure**

Configure a Cisco IronPort log source on the QRadar Console by using Syslog. The following tables describe the Syslog log source parameters that require specific values for retrieving logs from Cisco IronPort and Cisco WSA.

<table>
<thead>
<tr>
<th>Table 204. Cisco IronPort log source parameters for Syslog</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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

**Sample event messages**

Use these sample event messages as a way of verifying a successful integration with QRadar. Replace the sample IP addresses, etc. with your own content.

The following table shows a sample event message from Cisco IronPort:

<table>
<thead>
<tr>
<th>Table 205. Cisco IronPort sample message supported by the Cisco IronPort device</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Event name</strong></td>
</tr>
<tr>
<td>Mailserver_info</td>
</tr>
</tbody>
</table>
Cisco Meraki

The IBM QRadar DSM for Cisco Meraki collects Syslog events from a Cisco Meraki device.

To integrate Cisco Meraki with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the Cisco Meraki DSM RPM on your QRadar Console.

2. Configure your Cisco Meraki device to send Syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a Cisco Meraki log source on the QRadar Console. The following table describes the parameters that require specific values to collect Syslog events from Cisco Meraki:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Cisco Meraki</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>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, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.</td>
</tr>
</tbody>
</table>

Related concepts
Configure Cisco Meraki to communicate with IBM QRadar
To collect Cisco Meraki events, configure your Cisco Meraki device to send Syslog events to QRadar.

Sample event messages
Use these sample event messages as a way of verifying a successful integration with QRadar.

Related tasks
“Adding a DSM” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Related reference**

Cisco Meraki DSM specifications

The following table describes the specifications for the Cisco Meraki DSM.

### Cisco Meraki DSM specifications

The following table describes the specifications for the Cisco Meraki DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Cisco</td>
</tr>
<tr>
<td>DSM name</td>
<td>Cisco Meraki</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CiscoMeraki-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Events</td>
</tr>
<tr>
<td></td>
<td>Flows</td>
</tr>
<tr>
<td></td>
<td>security_event ids_alerted</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Cisco Meraki product information (<a href="https://Meraki.cisco.com">https://Meraki.cisco.com</a>)</td>
</tr>
</tbody>
</table>

**Related concepts**

Cisco Meraki

The IBM QRadar DSM for Cisco Meraki collects Syslog events from a Cisco Meraki device.

**Configure Cisco Meraki to communicate with IBM QRadar**

To collect Cisco Meraki events, configure your Cisco Meraki device to send Syslog events to QRadar.

Configure Cisco Meraki to communicate with QRadar by following the Syslog Server Overview and Configuration steps on the Cisco Meraki website (https://documentation.meraki.com/zGeneral_Administration/Monitoring_and_Reporting/Syslog_Server_Overview_and_Configuration).

**Related concepts**

Cisco Meraki

The IBM QRadar DSM for Cisco Meraki collects Syslog events from a Cisco Meraki device.

**Sample event messages**

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides sample event messages when using the Syslog protocol for the Cisco Meraki DSM:
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound Flow</td>
<td>Information</td>
<td><code>&lt;134&gt;1 1515988859.051369334 QRADAR flows src=&lt;Source_IP_address&gt; dst=&lt;Destination_IP_address&gt; protocol=tcp sport=&lt;Port&gt; dport=&lt;Port&gt; pattern: 1 all</code></td>
</tr>
<tr>
<td>Outbound Flow</td>
<td>Information</td>
<td><code>&lt;134&gt;1 1515988859.626061236 QRADAR_appliance flows src=&lt;Source_IP_address&gt; dst=&lt;Destination_IP_address&gt; mac=&lt;MAC_address&gt; protocol=tcp sport=&lt;Port&gt; dport=&lt;Port&gt; pattern: allow all</code></td>
</tr>
<tr>
<td>URL-UNKNOWN</td>
<td>Notice</td>
<td><code>&lt;134&gt;1 1516057359.742046722 QRADAR_appliance urls src=&lt;Source_IP_address&gt;:&lt;Port&gt; dst=&lt;Destination_IP_address&gt;:&lt;Port&gt; mac=&lt;MAC_address&gt; request: UNKNOWN https://www.example.com/cgibin/sdee-server/...</code></td>
</tr>
<tr>
<td>URL-GET</td>
<td>Information</td>
<td><code>&lt;134&gt;1 1516057357.668297541 QRADAR_appliance urls src=&lt;Source_IP_address&gt;:&lt;Port&gt; dst=&lt;Destination_IP_address&gt;:&lt;Port&gt; mac=&lt;MAC_address&gt; agent='Test' request: GET https://www.example.com/cgibin/sdee-server</code></td>
</tr>
<tr>
<td>URL-POST</td>
<td>Information</td>
<td><code>&lt;134&gt;1 1515990652.718750836 QRADAR_appliance urls src=&lt;Source_IP_address&gt;:&lt;Port&gt; dst=&lt;Destination_IP_address&gt;:&lt;Port&gt; mac=&lt;MAC_address&gt; agent='Windows-Update-Agent/&lt;IP_address&gt; Client-Protocol/1.40' request: POST https://www.example.com/cgibin/sdee-server</code></td>
</tr>
<tr>
<td>DHCP Lease</td>
<td>Information</td>
<td><code>&lt;134&gt;1 1516153561.629079842 QRADAR events dhcp lease of ip &lt;IP_address1&gt; from server mac &lt;MAC_address&gt; for client mac &lt;MAC_address&gt; from router &lt;IP_address2&gt; on subnet &lt;IP_address3&gt; with dns &lt;IP_address4&gt;, &lt;IP_address5&gt;</code></td>
</tr>
</tbody>
</table>
### Table 208. Cisco Meraki DSM sample messages supported by Cisco Meraki. (continued)

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn_registry_change</td>
<td>Notice</td>
<td><code>&lt;134&gt;1 1516085616.402689713 QRADAR events type=vpn_registry_change vpn_type='site-to-site' connectivity='false'</code></td>
</tr>
<tr>
<td>Content Filtering Block</td>
<td>Notice</td>
<td><code>&lt;134&gt;1 1516149081.972680893 QRADAR appliance events content_filtering_block url='https://www.example.com/cgi-bin/sdee-server/...' category0='Malware Sites' server='&lt;IP_address&gt;:&lt;Port&gt;'</code></td>
</tr>
<tr>
<td>MAC Address - IP Conflict</td>
<td>Warning</td>
<td><code>&lt;134&gt;1 1516057331.654660510 QRADAR events MAC &lt;MAC_address&gt; and MAC &lt;MAC_address&gt; both claim IP: &lt;IP_address&gt;</code></td>
</tr>
<tr>
<td>1:45148</td>
<td>Trojan Detected</td>
<td><code>&lt;134&gt;1 1516050030.553653046 QRADAR security_event ids_alerted signature=1:45148:1 priority=1 timestamp=1516050030.236281 dhost=&lt;MAC_address&gt; direction=ingress protocol=tcp/ip src=&lt;Source_IP_address&gt;:&lt;Port&gt; dst=&lt;Destination_IP_address&gt;:&lt;Port&gt; message: BROWSER-IE Microsoft Internet Explorer Array out of bounds write attempt</code></td>
</tr>
</tbody>
</table>

### Related concepts
**Cisco Meraki**
The IBM QRadar DSM for Cisco Meraki collects Syslog events from a Cisco Meraki device.

### Cisco NAC
The Cisco NAC DSM for IBM QRadar accepts events by using syslog.

QRadar records all relevant audit, error, failure events, quarantine, and infected system events. Before you configure a Cisco NAC device in QRadar, you must configure your device to forward syslog events.

### Configuring Cisco NAC to forward events
You can configure Cisco NAC to forward syslog events:

#### Procedure
1. Log in to the Cisco NAC user interface.
2. In the Monitoring section, select **Event Logs**.
3. Click the **Syslog Settings** tab.
4. In the **Syslog Server Address** field, type the IP address of your IBM QRadar.
5. In the **Syslog Server Port** field, type the syslog port number. The default is 514.
6. In the **System Health Log Interval** field, type the frequency, in minutes, for system statistic log events.
7. Click **Update**.

You are now ready to configure the log source in QRadar.

**Configuring a log source**
To integrate Cisco NAC events with IBM QRadar, you must manually create a log source to receive Cisco NAC events

**About this task**
QRadar does not automatically discover or create log sources for syslog events from Cisco NAC appliances.

**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 **Cisco NAC Appliance**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type the IP address or host name for the log source as an identifier for events from your Cisco NAC appliance.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The log source is added to QRadar. Events that are forwarded to QRadar by Cisco NAC are displayed on the **Log Activity** tab.

**Cisco Nexus**
The Cisco Nexus DSM for IBM QRadar supports alerts from Cisco NX-OS devices.

Syslog is used to forward events from Cisco Nexus to QRadar. Before you can integrate events with QRadar, you must configure your Cisco Nexus device to forward syslog events.

**Configuring Cisco Nexus to forward events**
You can configure syslog on your Cisco Nexus server to forward events:

**Procedure**
1. Type the following command to switch to configuration mode:
config t

2. Type the following commands:
   ```
   logging server <IP address> <severity>
   ```
   Where:
   - `<IP address>` is the IP address of your QRadar Console.
   - `<severity>` is the severity level of the event messages, that range 0 - 7 in value.
   For example, `logging server 192.0.2.1 6` forwards information level (6) syslog messages to 192.0.2.1.

3. Type the following command to configure the interface for sending syslog events:
   ```
   logging source-interface loopback
   ```

4. Type the following command to save your current configuration as the startup configuration:
   ```
   copy running-config startup-config
   ```

   The configuration is complete. The log source is added to IBM QRadar as Cisco Nexus events are automatically discovered. Events that are forwarded to QRadar by Cisco Nexus are displayed on the Log Activity tab of QRadar.

### Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Cisco Nexus.

#### About this task

The following configuration steps are optional. To manually configure a log source for Cisco Nexus, take the following steps:

#### Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   - The Data Sources pane is displayed.
4. Click the Log Sources icon.
   - The Log Sources window is displayed.
5. Click Add.
   - The Add a log source window is displayed.
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 Cisco Nexus.
   - The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 210. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete. For more information on configuring a Virtual Device Context (VDC) on your Cisco Nexus device, see your vendor documentation.

---

**Cisco Pix**

You can integrate Cisco Pix security appliances with IBM QRadar.

The Cisco Pix DSM for QRadar accepts Cisco Pix events by using syslog. QRadar records all relevant Cisco Pix events.

**Configuring Cisco Pix to forward events**

You can configure Cisco Pix to forward events.

**Procedure**

1. Log in to your Cisco PIX appliance by using a console connection, telnet, or SSH.
2. Type the following command to access Privileged mode:
   ```
   enable
   ```
3. Type the following command to access Configuration mode:
   ```
   conf t
   ```
4. Enable logging and time stamp the logs:
   ```
   logging on
   logging timestamp
   ```
5. Set the log level:
   ```
   logging trap warning
   ```
6. Configure logging to IBM QRadar:
   ```
   logging host <interface> <IP address>
   ```
   Where:
   - `<interface>` is the name of the interface, for example, DMZ, LAN, ethernet0, or ethernet1.
   - `<IP address>` is the IP address of the QRadar host.

The configuration is complete. The log source is added to QRadar as Cisco Pix Firewall events are automatically discovered. Events that are forwarded to QRadar by Cisco Pix Firewalls are displayed on the **Log Activity** tab of QRadar.

**Configuring a log source**

IBM QRadar automatically discovers and creates a log source for syslog events from Cisco Pix Firewalls.

**About this task**

The following configuration steps are optional.

To manually configure a log source for Cisco Pix, take the following steps:

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   - The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
   The **Log Sources** window is displayed.
5. Click **Add**.
   The **Add a log source** window is displayed.
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 **Cisco PIX Firewall**.
9. Using the **Protocol Configuration** list, select **Syslog**.
   The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 211. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
   The configuration is complete.

---

**Cisco Stealthwatch**

The IBM QRadar DSM for Cisco Stealthwatch receives events from a Cisco Stealthwatch device. The following table identifies the specifications for the Cisco Stealthwatch DSM:

<table>
<thead>
<tr>
<th>Table 212. Cisco Stealthwatch DSM specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Specification</strong></td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>DSM name</td>
</tr>
<tr>
<td>RPM file name</td>
</tr>
<tr>
<td>Supported versions</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>Event format</td>
</tr>
<tr>
<td>Recorded event types</td>
</tr>
<tr>
<td>Automatically discovered?</td>
</tr>
<tr>
<td>Includes identity?</td>
</tr>
<tr>
<td>Includes Custom properties?</td>
</tr>
<tr>
<td>More information</td>
</tr>
</tbody>
</table>
To integrate Cisco Stealthwatch with QRadar, complete the following steps:

1. If automatic updates are not configured, download the most recent version of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - Cisco Stealthwatch DSM RPM

2. Configure your Cisco Stealthwatch device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a Cisco Stealthwatch log source on the QRadar Console. The following table describes the parameters that require specific values for Cisco Stealthwatch event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Cisco Stealthwatch</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source</td>
<td>A unique identifier for the log source.</td>
</tr>
</tbody>
</table>

The following table shows a sample syslog message that is supported by the Cisco Stealthwatch device:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| 16         | Network Threshold Policy Violation | May 5 18:11:01 127.0.0.1 May 05 18:11:01 <Server> StealthWatch[3706]: LEEF:2.8|Lancope|Stealthwatch|6.8|16|0x7C|src=<Source_IP_address>|dst=<Destination_IP_address>|dstPort=|proto=|msg=The total traffic inbound + outbound exceeds the acceptable total traffic values.|fullmessage=Observed 3.956 bytes. Expected 2.22M bytes, tolerance of 50 all owns up to 1.92G bytes.|start=2017-05-05T18:10:00Z|end=|cat=High Total Traffic|alarmId=3L-1CR1-JJ38-Q0GNE-2|sourceHG=<Country>|targetHG=Unknown|source eHostSnapshot=https://<Server>/smc/getHostSnapshot?domainid=123&hostip=<Server_IP>&date=2017-05-05T18:10:00Z|targetHostSnapshot=https://<Server>/smc/getHostSnapshot?domainid=123&hostip=<Server_IP>&date=2017-05-05T18:10:00Z|flowCollectorName=<Server2>|flowCollectorIP=<IP_address2>|domain=example.com|exporterName=|exporterIPAddress=<IP_address2>|targetUser=|targetHostname=|sourceUser=|alarmStatus=ACTIV|alarmSev=Major    

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Cisco Stealthwatch to communicate with QRadar

About this task
Cisco Stealthwatch can forward events of different message types, including customized syslog messages, to third parties.

Procedure
1. Log in to the Stealthwatch Management Console (SMC) as an administrator.
2. In the menu bar, click Configuration > Response Management.
3. From the Actions section in the Response Management menu, click Add > Syslog Message.
4. In the Add Syslog Message Action window, configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name for the syslog message action.</td>
</tr>
<tr>
<td>Enabled</td>
<td>This check box is enabled by default.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the QRadar Event Collector.</td>
</tr>
<tr>
<td>Port</td>
<td>The default port is port 514.</td>
</tr>
<tr>
<td>Format</td>
<td>Select Syslog Formats.</td>
</tr>
</tbody>
</table>

5. Enter the following custom format:

```
LEEF:2.0|Lancope|Stealthwatch|6.8|{alarm_type_id}|{source_ip}|{target_ip}|{port}|{protocol}|{alarm_type_description}|{details}|{start_active_time}|{end_active_time}|{alarm_category_name}|{alarmID}|{alarm_id}|{source_host_group_names}|{target_host_group_names}|{sourceHostSnapshot}|{targetHostSnapshot}|{target_hostname}|{flowCollectorName}|{flowCollectorIP}|{device_name}|{device_ip}|{domain_name}|{exporter_name}|{exporter_hostname}|{exporter_label}|{exporter_ip}|{exporterInfo}|{exporter_label}|{targetUser}|{sourceUser}|{alarmStatus}|{alarm_status}|{alarmSev}|{alarm_severity_name}|
```

6. Select the custom format from the list and click OK.

Note: Use the Test button to send test message to QRadar

7. Click Response Management > Rules.
8. Click Add and select Host Alarm.
9. Provide a rule name in the Name field.
10. Create rules by selecting values from the Type and Options menus. To add more rules, click the ellipsis icon. For a Host Alarm, combine as many possible types in a statement as possible.
11. In the Action dialog, select IBM QRadar syslog action for both Active and Inactive conditions. The event is forwarded to QRadar when any predefined condition is satisfied.

Cisco Umbrella

The IBM QRadar DSM for Cisco Umbrella collects DNS logs from Cisco Umbrella storage by using an Amazon S3 compatible API.

To integrate Cisco Umbrella with QRadar, complete the following steps:
1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console in the order that they are listed.
   - Protocol Common RPM
   - Amazon AWS REST API Protocol RPM
   - Cisco Cloud Web Security DSM RPM
   - Cisco Umbrella DSM RPM

2. Configure your Cisco Umbrella to communicate with QRadar.

3. Add a Cisco Umbrella log source on the QRadar Console. The following table describes the parameters that require specific values for Cisco Umbrella event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Cisco Umbrella</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Amazon AWS S3 REST API</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique name for the log source. The Log Source Identifier can be any valid value and does not need to reference a specific server. The Log Source Identifier can be the same value as the Log Source Name. If you configured more than one Cisco Umbrella log source, you might want to identify the first log source as ciscoumbrella1, the second log source as ciscoumbrella2, and the third log source as ciscoumbrella3.</td>
</tr>
<tr>
<td>Signature Version</td>
<td>Select AWSSIGNATUREV2 or AWSSIGNATUREV4. AWSSIGNATUREV2 does not support all Amazon AWS regions. If you are using a region that supports only AWSSIGNATUREV4, you must choose AWSSIGNATUREV4 from the list. Note: If you need to create a log source to retrieve events from multiple regions, you must choose AWSSIGNATUREV4.</td>
</tr>
<tr>
<td>Region Name (Signature V4 only)</td>
<td>The region that is associated with the Amazon S3 bucket.</td>
</tr>
<tr>
<td>Bucket Name</td>
<td>The name of the AWS S3 bucket where the log files are stored.</td>
</tr>
<tr>
<td>Endpoint URL</td>
<td><a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
</tr>
</tbody>
</table>

The Endpoint URL can be different depending on the device configurations.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td><strong>Access Key ID / Secret Key</strong></td>
</tr>
<tr>
<td></td>
<td>Standard authentication that can be used from anywhere.</td>
</tr>
<tr>
<td></td>
<td><strong>EC2 Instance IAM Role</strong></td>
</tr>
<tr>
<td></td>
<td>If your QRadar managed host is running in an AWS EC2 instance, choosing this option will use the IAM Role from the instance metadata assigned to the instance for authentication and no keys are required. This method will only work for managed hosts that are running within an AWS EC2 container.</td>
</tr>
<tr>
<td>Access Key ID</td>
<td>The public access key that is required to access the AWS S3 bucket.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>The private access key that is required to access the AWS S3 bucket.</td>
</tr>
<tr>
<td>Directory Prefix</td>
<td>The location of the root directory on the Cisco Umbrella storage bucket from where the Cisco Umbrella logs are retrieved. For example, the root directory location might be <code>dnslogs/</code>.</td>
</tr>
<tr>
<td>File Pattern</td>
<td><code>.*\.csv\.gz</code></td>
</tr>
<tr>
<td>Event Format</td>
<td>Select <strong>Cisco Umbrella CSV</strong> from the list. The log source retrieves CSV formatted events.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses the Amazon Web Service by using a proxy, enable the check box.</td>
</tr>
<tr>
<td></td>
<td>If the proxy requires authentication, configure the <strong>Proxy Server</strong>, <strong>Proxy Port</strong>, <strong>Proxy Username</strong>, and <strong>Proxy Password</strong> fields. If the proxy does not require authentication, configure the <strong>Proxy Username</strong> and <strong>Proxy Password</strong> fields.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>If you select <strong>Yes</strong>, QRadar automatically downloads the server certificate and begin trusting the target server. This option can be used to initialize a newly created log source, obtain certificates, and replace expired certificates.</td>
</tr>
</tbody>
</table>
Table 215. Amazon AWS S3 REST API log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurrence</td>
<td>How often the Amazon AWS S3 REST API 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. Type a time interval to determine how frequently the remote directory is scanned for new event log files. The minimum value is 1 minute. The time interval can include values in hours (H), minutes (M), or days (D). For example: 2H = 2 hours, 15M = 15 minutes.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second. The default is 5000.</td>
</tr>
</tbody>
</table>

Related concepts
“Configure Cisco Umbrella to communicate with QRadar” on page 381
QRadar collects Cisco Umbrella events from an Amazon S3 bucket. You need to configure your Cisco Umbrella to forward events to QRadar.

“Cisco Umbrella DSM specifications” on page 381
The following table describes the specifications for the Cisco Umbrella DSM.

“Sample event messages” on page 382
Use these sample event messages as a way of verifying a successful integration with QRadar.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configure Cisco Umbrella to communicate with QRadar
QRadar collects Cisco Umbrella events from an Amazon S3 bucket. You need to configure your Cisco Umbrella to forward events to QRadar.

Follow the procedures that are mentioned in Cisco online documentation to configure your Cisco Umbrella:

Cisco Umbrella DSM specifications
The following table describes the specifications for the Cisco Umbrella DSM.

Table 216. Cisco Umbrella DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Cisco</td>
</tr>
<tr>
<td>DSM name</td>
<td>Cisco Umbrella</td>
</tr>
<tr>
<td>Specification</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CiscoUmbrella-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Amazon AWS S3 REST API</td>
</tr>
<tr>
<td>Event format</td>
<td>Cisco Umbrella CSV</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Cisco Umbrella product information page (<a href="https://umbrella.cisco.com">https://umbrella.cisco.com</a>)</td>
</tr>
</tbody>
</table>

**Sample event messages**

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following tables provide sample event messages for the Cisco Umbrella DSM:

**Table 217. Cisco Umbrella sample syslog message**

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>

**Table 218. Cisco Umbrella sample event message**

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOERROR</td>
<td>18081 (DNS In Progress)</td>
<td>&quot;2015-01-16 17:48:41&quot;,&quot;Active DirectoryUser Name&quot;,&quot;Active Directory User Name,ADSite,Network&quot;,&quot;&lt;IP_address1&gt;&quot;,&quot;&lt;IP_address2&gt;&quot;,&quot;Allowed&quot;,&quot;1 (A)&quot;, &quot;NOERROR&quot;, &quot;domain-visited.com.&quot;, &quot;Chat, Photo Sharing, Social Networking, Allow List&quot;</td>
</tr>
</tbody>
</table>
Cisco VPN 3000 Concentrator

The Cisco VPN 3000 Concentrator DSM for IBM QRadar accepts Cisco VPN Concentrator events by using syslog.

About this task

QRadar records all relevant events. Before you can integrate with a Cisco VPN concentrator, you must configure your device to forward syslog events to QRadar.

To configure your Cisco VPN 3000 Concentrator:

Procedure

1. Log in to the Cisco VPN 3000 Concentrator command-line interface (CLI).
2. Type the following command to add a syslog server to your configuration:

   set logging server <IP address>

   Where <IP address> is the IP address of QRadar or your Event Collector.
3. Type the following command to enable system messages to be logged to the configured syslog servers:

   set logging server enable
4. Set the facility and severity level for syslog server messages:

   • set logging server facility <server_facility_parameter>
   • set logging server severity <server_severity_level>

   The configuration is complete. The log source is added to QRadar as Cisco VPN Concentrator events are automatically discovered. Events that are forwarded to QRadar are displayed on the Log Activity tab of QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Cisco VPN 3000 Series Concentrators.

About this task

These configuration steps are optional.

To manually configure a log source, take the following steps:

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.

   The Data Sources pane is displayed.
4. Click the Log Sources icon.

   The Log Sources window is displayed.
5. Click Add.

   The Add a log source window is displayed.
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 Cisco VPN 3000 Series Concentrator.
9. Using the **Protocol Configuration** list, select **Syslog**.

The syslog protocol configuration is displayed.

10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Cisco VPN 3000 Series Concentrators.</td>
</tr>
</tbody>
</table>

11. Click **Save**.

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

The configuration is complete.

---

**Cisco Wireless LAN Controllers**

The Cisco Wireless LAN Controllers DSM for IBM QRadar collects events that are forwarded from Cisco Wireless LAN Controller devices by using syslog or SNMPv2.

This section includes the following topics:

- “Configuring syslog for Cisco Wireless LAN Controller” on page 384
- “Configuring SNMPv2 for Cisco Wireless LAN Controller” on page 386

**Before you begin**

If you collect events from Cisco Wireless LAN Controllers, select the best collection method for your configuration. The Cisco Wireless LAN Controller DSM for QRadar supports both syslog and SNMPv2 events. However, syslog provides all available Cisco Wireless LAN Controller events, whereas SNMPv2 sends only a limited set of security events to QRadar.

**Configuring syslog for Cisco Wireless LAN Controller**

You can configure the Cisco Wireless LAN Controller to forward syslog events to IBM QRadar.

**Procedure**

1. Log in to your Cisco Wireless LAN Controller interface.
2. Click the **Management** tab.
3. From the menu, select **Logs > Config**.
4. In the **Syslog Server IP Address** field, type the IP address of your QRadar Console.
5. Click **Add**.
6. From the **Syslog Level** list, select a logging level.

   - The **Information** logging level allows the collection of all Cisco Wireless LAN Controller events above the **Debug** logging level.
7. From the **Syslog Facility** list, select a facility level.
8. Click **Apply**.
9. Click **Save Configuration**.

**What to do next**

You are now ready to configure a syslog log source for Cisco Wireless LAN Controller.
**Configuring a syslog log source in IBM QRadar**

QRadar does not automatically discover incoming syslog events from Cisco Wireless LAN Controllers. You must create a log source for each Cisco Wireless LAN Controller that provides syslog events to QRadar.

**About this task**

To configure a log source in QRadar, take the following steps:

**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 **Cisco Wireless LAN Controllers**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 220. Syslog protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Enabled</td>
</tr>
<tr>
<td>Credibility</td>
</tr>
<tr>
<td>Target Event Collector</td>
</tr>
<tr>
<td>Coalescing Events</td>
</tr>
<tr>
<td>Incoming Event Payload</td>
</tr>
</tbody>
</table>
Table 220. Syslog protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store Event Payload</td>
<td>Select this check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the Store Event Payload drop-down list in the QRadar Settings window on the Admin tab. However, when you create a new log source or update the configuration for an automatically discovered log source that you can override the default value by configuring this check box for each log source.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the Admin tab, click **Deploy Changes**.

   The configuration is complete.

**Configuring SNMPv2 for Cisco Wireless LAN Controller**

SNMP event collection for Cisco Wireless LAN Controllers allows the capture of events for IBM QRadar.

**About this task**

The following events are collected:

- SNMP Config Event
- bsn Authentication Errors
- LWAPP Key Decryption Errors

**Procedure**

1. Log in to your Cisco Wireless LAN Controller interface.
2. Click the Management tab.
3. From the menu, select **SNMP > Communities**.

   You can use the one of the default communities that are created or create a new community.
4. Click **New**.
5. In the **Community Name** field, type the name of the community for your device.
6. In the **IP Address** field, type the IP address of QRadar.

   The IP address and IP mask that you specify is the address from which your Cisco Wireless LAN Controller accepts SNMP requests. You can treat these values as an access list for SNMP requests.
7. In the **IP Mask** field, type a subnet mask.
8. From the **Access Mode** list, select **Read Only** or **Read/Write**.
9. From the **Status** list, select **Enable**.
10. Click **Save Configuration** to save your changes.

**What to do next**

You are now ready to create a SNMPv2 trap receiver.
**Configuring a trap receiver for Cisco Wireless LAN Controller**

Trap receivers that are configured on Cisco Wireless LAN Controllers define where the device can send SNMP trap messages.

**About this task**

To configure a trap receiver on your Cisco Wireless LAN Controller, take the following steps:

**Procedure**

1. Click the Management tab.
2. From the menu, select SNMP > Trap Receivers.
3. In the Trap Receiver Name field, type a name for your trap receiver.
4. In the IP Address field, type the IP address of IBM QRadar.
   
   The IP address you specify is the address to which your Cisco Wireless LAN Controller sends SNMP messages. If you plan to configure this log source on an Event Collector, you want to specify the Event Collector appliance IP address.
5. From the Status list, select Enable.
6. Click Apply to commit your changes.
7. Click Save Configuration to save your settings.

**What to do next**

You are now ready to create a SNMPv2 log source in QRadar.

**Configuring a log source for the Cisco Wireless LAN Controller that uses SNMPv2**

IBM QRadar does not automatically discover and create log sources for SNMP event data from Cisco Wireless LAN Controllers. You must create a log source for each Cisco Wireless LAN Controller providing SNMPv2 events.

**About this task**

Take the following steps to create a log source for your Cisco Wireless LAN Controller:

**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 Cisco Wireless LAN Controllers.
10. Configure the following values:

   **Table 221. SNMPv2 protocol parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Cisco Wireless LAN Controller.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Community</td>
<td>Type the SNMP community name that is needed to access the system that contains the SNMP events. The default is Public.</td>
</tr>
<tr>
<td>Include OIDs in Event Payload</td>
<td>Select the Include OIDs in Event Payload check box. This option allows the SNMP event payload to be constructed by using name-value pairs instead of the standard event payload format. OIDs in the event payload are needed to process SNMPv2 or SNMPv3 events from certain DSMs.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the Enabled check box to enable the log source. By default, the check box is selected.</td>
</tr>
<tr>
<td>Credibility</td>
<td>From the list, select the credibility of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>From the list, select the Target Event Collector to use as the target for the log source.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value that is configured in the Coalescing Events drop-down in the QRadar Settings window on the Admin tab. However, when you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source. For more information on settings, see the IBM QRadar Administration Guide.</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>Select this check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the Store Event Payload drop-down in the QRadar Settings window on the Admin tab. However, when you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source.</td>
</tr>
</tbody>
</table>

11. Click Save.

12. On the Admin tab, click Deploy Changes.

The configuration is complete. Events that are forwarded to by Cisco Wireless LAN Controller are displayed on the Log Activity tab of QRadar.

**Cisco Wireless Services Module**

You can integrate a Cisco Wireless Services Module (WiSM) device with IBM QRadar.

A Cisco WiSM DSM for QRadar accepts events by using syslog. Before you can integrate QRadar with a Cisco WiSM device, you must configure Cisco WiSM to forward syslog events.
Configuring Cisco WiSM to forward events
You can configure Cisco WiSM to forward syslog events to IBM QRadar.

About this task
Take the following steps to configure Cisco WiSM to forward syslog events:

Procedure
1. Log in to the Cisco Wireless LAN Controller user interface.
2. Click **Management > Logs > Config.**
   
   The **Syslog Configuration** window is displayed.
3. In the **Syslog Server IP Address** field, type the IP address of the QRadar host that receives the syslog messages.
4. Click **Add**.
5. Using the **Syslog Level** list, set the severity level for filtering syslog messages to the syslog servers by using one of the following severity levels:
   - **Emergencies** - Severity level 0
   - **Alerts** - Severity level 1 (Default)
   - **Critical** - Severity level 2
   - **Errors** - Severity level 3
   - **Warnings** - Severity level 4
   - **Notifications** - Severity level 5
   - **Informational** - Severity level 6
   - **Debugging** - Severity level 7
   
   If you set a syslog level, only those messages whose severity level is equal to or less than the selected syslog level are sent to the syslog server. For example, if you set the syslog level to **Warnings** (severity level 4), only those messages whose severity is 0 - 4 are sent to the syslog servers.
6. From the **Syslog Facility** list, set the facility for outgoing syslog messages to the syslog server by using one of the following facility levels:
   - **Kernel** - Facility level 0
   - **User Process** - Facility level 1
   - **Mail** - Facility level 2
   - **System Daemons** - Facility level 3
   - **Authorization** - Facility level 4
   - **Syslog** - Facility level 5 (default value)
   - **Line Printer** - Facility level 6
   - **USENET** - Facility level 7
   - **Unix-to-Unix Copy** - Facility level 8
   - **Cron** - Facility level 9
   - **FTP Daemon** - Facility level 11
   - **System Use 1** - Facility level 12
   - **System Use 2** - Facility level 13
   - **System Use 3** - Facility level 14
   - **System Use 4** - Facility level 15
   - **Local Use 0** - Facility level 16
7. Click **Apply**.

8. From the **Buffered Log Level** and the **Console Log Level** lists, select the severity level for log messages sent to the controller buffer and console by using one of the following severity levels:
   - **Emergencies** - Severity level 0
   - **Alerts** - Severity level 1
   - **Critical** - Severity level 2
   - **Errors** - Severity level 3 (default value)
   - **Warnings** - Severity level 4
   - **Notifications** - Severity level 5
   - **Informational** - Severity level 6
   - **Debugging** - Severity level 7

   If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to **Warnings** (severity level 4), only those messages whose severity is 0 - 4 are logged.

9. Select the **File Info** check box if you want the message logs to include information about the source file. The default value is enabled.

10. Select the **Proc Info** check box if you want the message logs to include process information. The default value is disabled.

11. Select the **Trace Info** check box if you want the message logs to include trace back information. The default value is disabled.

12. Click **Apply** to commit your changes.

13. Click **Save Configuration** to save your changes.

   The configuration is complete. The log source is added to QRadar as Cisco WiSM events are automatically discovered. Events that are forwarded by Cisco WiSM are displayed on the **Log Activity** tab of QRadar.

### Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Cisco WiSM.

#### About this task

The following configuration steps are optional.

To manually configure a log source for Cisco WiSM, take the following steps:

#### Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   - The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
The Log Sources window is displayed.

5. Click Add.

The Add a log source window is displayed.

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 Cisco Wireless Services Module (WiSM).


The syslog protocol configuration is displayed.

10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Cisco WiSM appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.

12. On the Admin tab, click Deploy Changes.

The configuration is complete.
Chapter 43. Citrix

Citrix NetScaler and Citrix Access Gateway DSMs.
The Citrix NetScaler DSM for IBM QRadar accepts all relevant audit log events by using syslog.
The Citrix Access Gateway DSM accepts access, audit, and diagnostic events that are forwarded from
your Citrix Access Gateway appliance by using syslog.

Citrix NetScaler

To integrate Citrix NetScaler events with IBM QRadar, you must configure Citrix NetScaler to forward
syslog events.

Procedure
1. Using SSH, log in to your Citrix NetScaler device as a root user.
2. Type the following command to add a remote syslog server:
   
   ```
   add audit syslogAction <ActionName> <IP Address> -serverPort 514 -logLevel Info -
   dateFormat DDMMYYYY
   ```
   
   Where:
   
   `<ActionName>` is a descriptive name for the syslog server action.
   `<IP Address>` is the IP address or host name of your QRadar Console.

   Example:
   
   ```
   add audit syslogAction action-QRadar 192.0.2.1 -serverPort 514 -logLevel Info -
   dateFormat DDMMYYYY
   ```

3. Type the following command to add an audit policy:
   
   ```
   add audit syslogPolicy <PolicyName> <Rule> <ActionName>
   ```
   
   Where:
   
   `<PolicyName>` is a descriptive name for the syslog policy.
   `<Rule>` is the rule or expression the policy uses. The only supported value is `ns_true`.
   `<ActionName>` is a descriptive name for the syslog server action.

   Example:
   
   ```
   add audit syslogPolicy policy-QRadar ns_true action-QRadar
   ```

4. Type the following command to bind the policy globally:
   
   ```
   bind system global <PolicyName> -priority <Integer>
   ```
   
   Where:
   
   `<PolicyName>` is a descriptive name for the syslog policy.
   `<Integer>` is a number value that is used to rank message priority for multiple policies that are
   communicating by using syslog.

   Example:
   
   ```
   bind system global policy-QRadar -priority 30
   ```
When multiple policies have priority (represented by a number value that is assigned to them) the lower number value is evaluated before the higher number value.

5. Type the following command to save the Citrix NetScaler configuration.
   ```
   save config
   ```

6. Type the following command to verify that the policy is saved in your configuration:
   ```
   sh system global
   ```

   **Note:** For information on configuring syslog by using the Citrix NetScaler user interface, see [http://support.citrix.com/article/CTX121728](http://support.citrix.com/article/CTX121728) or your vendor documentation.

   The configuration is complete. The log source is added to QRadar as Citrix NetScaler events are automatically discovered. Events that are forwarded by Citrix NetScaler are displayed on the Log Activity tab of QRadar.

### Configuring a Citrix NetScaler log source

IBM QRadar automatically discovers and creates a log source for syslog events from Citrix NetScaler.

**About this task**

This procedure is optional.

**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 **Citrix NetScaler**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

    **Table 223. Syslog protocol parameters**

    | Parameter               | Description                                                                 |
    |-------------------------|-----------------------------------------------------------------------------|
    | Log Source Identifier   | Type the IP address or host name for the log source as an identifier for events from your Citrix NetScaler devices. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

### Citrix Access Gateway

Configuration of syslog on your Citrix Access Gateway to forward events to the QRadar Console or Event Collector.

**Procedure**

1. Log in to your Citrix Access Gateway web interface.
2. Click the **Access Gateway Cluster** tab.
3. Select **Logging/Settings**.
4. In the **Server** field, type the IP address of your QRadar Console or Event Collector.
5. From the **Facility** list, select a syslog facility level.
6. In the **Broadcast interval (mins)**, type 0 to continuously forward syslog events to QRadar.
7. Click **Submit** to save your changes.

**Results**

The configuration is complete. The log source is added to QRadar as Citrix Access Gateway events are automatically discovered. Events that are forwarded to QRadar by Citrix Access Gateway are displayed on the **Log Activity** tab in QRadar.

**Configuring a Citrix Access Gateway log source**

IBM QRadar automatically discovers and creates a log source for syslog events from Citrix Access Gateway appliances.

**About this task**

This procedure is optional.

**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 **Citrix Access Gateway**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 224. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the Admin tab, click **Deploy Changes**.
Chapter 44. Cloudera Navigator

The IBM QRadar DSM for Cloudera Navigator collects events from Cloudera Navigator. The following table identifies the specifications for the Cloudera Navigator DSM:

<table>
<thead>
<tr>
<th>Table 225. Cloudera Navigator DSM specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Specification</strong></td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>DSM name</td>
</tr>
<tr>
<td>RPM file name</td>
</tr>
<tr>
<td>Supported versions</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>Recorded event types</td>
</tr>
<tr>
<td>Automatically discovered?</td>
</tr>
<tr>
<td>Includes identity?</td>
</tr>
<tr>
<td>Includes custom properties?</td>
</tr>
<tr>
<td>More information</td>
</tr>
</tbody>
</table>

To integrate Cloudera Navigator 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:
   - Cloudera Navigator DSM RPM
2. Configure your Cloudera Navigator device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Cloudera Navigator log source on the QRadar Console. The following table describes the parameters that require specific values for Cloudera Navigator event collection:

<table>
<thead>
<tr>
<th>Table 226. Cloudera Navigator log source parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

Related tasks
   - “Adding a DSM” on page 4
   - “Adding a log source” on page 4
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 Cloudera Navigator to communicate with QRadar**

You can configure Cloudera Navigator device to send JSON format syslog events to IBM QRadar.

**Before you begin**

Ensure that Cloudera Navigator can access port 514 on the QRadar system.

**About this task**

When you install Cloudera Navigator, all audit logs are collected automatically. However, you must configure Cloudera Navigator to send audits logs to QRadar by using syslog.

**Procedure**

1. Do one of the following tasks:
   - Click Clusters > Cloudera Management Service > Cloudera Management Service.
   - On the Status tab of the Home page, click the Cloudera Management Service link in Cloudera Management Service table.
2. Click the Configuration tab.
4. Depending on the format type, enter one of the following values in the Value field:
   - log4j.logger.auditStream = TRACE,SYSLOG
   - log4j.appender.SYSLOG = org.apache.log4j.net.SyslogAppender
   - log4j.appender.SYSLOG.SyslogHost = <QRadar Hostname>
   - log4j.appender.SYSLOG.Facility = Local2
   - log4j.appender.SYSLOG.FacilityPrinting = true
   - log4j.additivity.auditStream = false
5. Click Save Changes.
Chapter 45. CloudPassage Halo

The CloudPassage Halo DSM for IBM QRadar can collect event logs from the CloudPassage Halo account. The following table identifies the specifications for the CloudPassage Halo DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>CloudPassage</td>
</tr>
<tr>
<td>DSM name</td>
<td>CloudPassage Halo</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CloudPassageHalo-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>All</td>
</tr>
<tr>
<td>Event format</td>
<td>Syslog, Log file</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Included identity?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>CloudPassage website (<a href="http://www.cloudpassage.com">www.cloudpassage.com</a>)</td>
</tr>
</tbody>
</table>

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 **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`.
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:

    ```bash
    haloEvents.py --leefsyslog=192.0.2.1
    ```

    By default, the Event Connector retrieves existing events on initial connection and then retrieves only new 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:

    ```bash
    haloEvents.py --leefsyslog=192.0.2.1 --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:

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

    Depending on what Linux 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:

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

**Notice:** 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 46. CloudLock Cloud Security Fabric

The IBM QRadar DSM for CloudLock Cloud Security Fabric collects events from the CloudLock Cloud Security Fabric service.

The following table describes the specifications for the CloudLock Cloud Security Fabric DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>CloudLock</td>
</tr>
<tr>
<td>DSM name</td>
<td>CloudLock Cloud Security Fabric</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CloudLockCloudSecurityFabric-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>NA</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Log Event Extended Format (LEEF)</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Incidents</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate CloudLock Cloud Security Fabric 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 in the order that they are listed:
   - DSMCommon RPM
   - CloudLock Cloud Security Fabric DSM RPM

2. Configure your CloudLock Cloud Security Fabric service to send Syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a CloudLock Cloud Security Fabric log source on the QRadar Console. The following table describes the parameters that require specific values for CloudLock Cloud Security Fabric event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>CloudLock Cloud Security Fabric</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

The following table provides a sample event message for the CloudLock Cloud Security Fabric DSM:
### Table 230. CloudLock Cloud Security Fabric sample message supported by the CloudLock Cloud Security Fabric service

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Incident</td>
<td>Suspicious Activity</td>
<td>LEEF: 1.0</td>
</tr>
</tbody>
</table>

**Related tasks**

* “Adding a DSM” on page 4
  * “Adding a log source” on page 4

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 CloudLock Cloud Security Fabric to communicate with QRadar**

You can configure CloudLock Cloud Security Fabric to communicate with QRadar by using a Python script.

**Before you begin**

- To collect incidents from CloudLock, a script that makes CloudLock API calls is required. This script collects incidents and converts them to Log Event Extended Format (LEEF).
- Python is required.

**Procedure**

1. Generate a CloudLock API token. To generate an API token in CloudLock, open the Settings. Go to the **Integrations** panel. Copy the Access token that appears on the page.
2. Go to the CloudLock Support website (https://www.cloudlock.com/support/). Open a support case to obtain the cl_sample_incidents.py file and then schedule the script for event collection.
Chapter 47. Correlog Agent for IBM z/OS

The CorreLog Agent for IBM z/OS DSM for IBM 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:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>CorreLog</td>
</tr>
<tr>
<td>DSM name</td>
<td>CorreLog Agent for IBM z/OS</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CorreLogzOSAgent_qradar-version_build-number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>7.1, 7.2</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog LEEF</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom event properties</td>
<td>No</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>CorreLog Agent for IBM zOS</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 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 48. CrowdStrike Falcon Host

The IBM QRadar DSM for CrowdStrike Falcon Host collects LEEF events that are forwarded by a Falcon SIEM Connector.

The following table describes the specifications for the CrowdStrike Falcon Host DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>CrowdStrike</td>
</tr>
<tr>
<td>DSM name</td>
<td>CrowdStrike Falcon Host</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CrowdStrikeFalconHost-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
</tbody>
</table>
| Recorded event types       | Falcon Host Detection Summary  
Falcon Host Authentication Log  
Falcon Host Detect Status Update Logs  
Customer IOC Detect Event  
Hash Spreading Event                                                  |
| Automatically discovered?  | Yes                                                                                                                                      |
| Includes identity?         | No                                                                                                                                       |
| Includes custom properties?| No                                                                                                                                       |
| More information           | CrowdStrike website (https://www.crowdstrike.com/products/falcon-host/)                                                               |

To integrate CrowdStrike Falcon Host with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs in the order that they are listed, on your QRadar Console:
   - DSMCommon RPM
   - CrowdStrike Falcon Host DSM RPM
2. Install and configure your Falcon SIEM connector to send events to QRadar.
3. If QRadar does not automatically detect the log source, add a CrowdStrike Falcon Host log source on the QRadar Console. The following table describes the parameters that require specific values for CrowdStrike Falcon Host event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>CrowdStrike Falcon Host</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>
Table 232. CrowdStrike Falcon Host log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name where the Falcon SIEM Connector is installed.</td>
</tr>
</tbody>
</table>

The following table shows a sample event message from CrowdStrike Falcon Host:

Table 233. CrowdStrike Falcon Host sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| Suspicious Activity | Suspicious Activity| LEEF:1.0|CrowdStrike|FalconHost
|                     |                    | devTime=2016-06-09 02:57:28                                                         |
|                     |                    | src=<Source_IP_address>                                                             |
|                     |                    | srcPort=49220                                                                      |
|                     |                    | dst=<Destination_IP_address>                                                       |
|                     |                    | domain=INITECH                                                                     |
|                     |                    | cat=NetworkAccesses                                                                |
|                     |                    | usrName=<Username>                                                                 |
|                     |                    | devTimeFormat=yyyy-MM-dd HH:mm:ss                                                   |
|                     |                    | connDir=0                                                                           |
|                     |                    | dstPort=443                                                                        |
|                     |                    | resource=<Resource>                                                                |
|                     |                    | proto=TCP                                                                          |
|                     |                    | url=https://example.com/url                                                         |

Related tasks

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 CrowdStrike Falcon Host to communicate with QRadar

To send LEEF events from CrowdStrike Falcon Host to IBM QRadar, you must install and configure Falcon SIEM connector.

Before you begin

You must have access with administrator privileges to the Falcon Streaming API. To enable access, contact Crowdstrike support (support@crowdstrike.com).

Procedure

1. Obtain an API key and UUID to configure SIEM Connector.
   a) Log in to the Falcon user interface.
   b) Select People App, and then click the Customer tab.
      The People App option is only visible to admin users.
   c) Click Generate new API key.
   d) Make a copy of the API key and the UUID.
2. Install the Falcon SIEM Connector.

   Note: The Falcon SIEM Connector needs to be deployed on premise on a system running either CentOS or RHEL 6.x-7.x. Internet connectivity to the CrowdStrike Cloud is also required.

   Note: You must have Admin (root) privileges.

   • Use the provided RPM to install the Falcon SIEM Connector.
The Falcon SIEM Connector installs in the /opt/crowdstrike/ directory by default. A service is created in the /etc/init.d/cs.falconhoseclientd/ directory.

3. Configure the SIEM Connector to forward LEEF events to QRadar.

The configuration files are located in the /opt/crowdstrike/etc/ directory.

- Rename cs.falconhoseclient.leeef.cfg to cs.falconhoseclient.cfg for LEEF configuration settings. The SIEM Connector uses cs.falconhoseclient.cfg configuration by default.

The following table describes some of the key parameter values for forwarding LEEF events to QRadar.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>The version of authentication to be used. In this case, it is the API Key Authentication version.</td>
<td>2</td>
</tr>
<tr>
<td>api_url</td>
<td>The SIEM connector connects to this endpoint URL.</td>
<td><a href="https://firehose.crowdstrike.com/sensors/entities/datafeed/v1">https://firehose.crowdstrike.com/sensors/entities/datafeed/v1</a></td>
</tr>
<tr>
<td>app_id</td>
<td>An arbitrary string identifier for connecting to Falcon Streaming API.</td>
<td>Any string. For example, FHAPI-LEEF</td>
</tr>
<tr>
<td>api_key</td>
<td>The API key is used as the credential for client verification.</td>
<td>Obtained at step 1</td>
</tr>
<tr>
<td>api_uuid</td>
<td>The UUID is used as the credential for client verification.</td>
<td>Obtained at step 1</td>
</tr>
<tr>
<td>send_to_syslog_server</td>
<td>To enable or disable syslog push to syslog server, set the flag to true or false.</td>
<td>true</td>
</tr>
<tr>
<td>host</td>
<td>The IP or host name of the SIEM.</td>
<td>The QRadar SIEM IP or host name where the Connector is forwarding the LEEF events.</td>
</tr>
<tr>
<td>header_delim</td>
<td>Header prefix and fields are delimited by this value.</td>
<td>The value must be a pipe (</td>
</tr>
<tr>
<td>field_delim</td>
<td>The delimiter value that is used to separate key-value pairs.</td>
<td>The value must be a tab (\t).</td>
</tr>
<tr>
<td>time_fields</td>
<td>This datetime field value is converted to specified time format.</td>
<td>The default field is devTime (device time). If a custom LEEF key is used for setting device time, use a different field name.</td>
</tr>
</tbody>
</table>

4. Start the SIEM Connector service by typing the following command:

   service cs.falconhoseclientd start

a) If you want to stop the service, type the following command:

   service cs.falconhoseclientd stop

b) If you want to restart the service, type the following command:
service cs.falconhoseclientd restart

What to do next
Verify that Falcon SIEM Connector is configured to send events to QRadar.
Chapter 49. CRYPTOCard CRYPTO-Shield

The IBM QRadar CRYPTOCard CRYPTO-Shield DSM for QRadar accepts events by using syslog.

To integrate CRYPTOCard CRYPTO-Shield events with QRadar, you must manually create a log source to receive syslog events.

Before you can receive events in QRadar, you must configure a log source, then configure your CRYPTOCard CRYPTO-Shield to forward syslog events. Syslog events that are forwarded from CRYPTOCard CRYPTO-Shield devices are not automatically discovered. QRadar can receive syslog events on port 514 for both TCP and UDP.

Configuring a log source

IBM QRadar does not automatically discover or create log sources for syslog events from CRYPTOCard CRYPTO-Shield devices.

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 CRYPTOCard CRYPTOShield.
9. From the Protocol Configuration list, select Syslog.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your CRYPTOCard CRYPTO-Shield device.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

Configuring syslog for CRYPTOCard CRYPTO-Shield

To configure your CRYPTOCard CRYPTO-Shield device to forward syslog events:

Procedure

1. Log in to your CRYPTOCard CRYPTO-Shield device.
2. Configure the following System Configuration parameters:

   **Important:** You must have CRYPTOCard Operator access with the assigned default Super-Operator system role to access the System Configuration parameters.

   - `log4j.appender.<protocol>` - Directs the logs to a syslog host where:
- `<protocol>` is the type of log appender, that determines where you want to send logs for storage. The options are as follows: ACC, DBG, or LOG. For this parameter, type the following entry:
  `org.apache.log4j.net.SyslogAppender`
- `log4j.appender.<protocol>.SyslogHost <IP address>` - Type the IP address or host name of the syslog server where:
  - `<protocol>` is the type of log appender, that determines where you want to send logs for storage. The options are as follows: ACC, DBG, or LOG.
  - `<IP address>` is the IP address of the IBM QRadar host to which you want to send logs.

Specify the `IP address` parameter after the `log4j.appender.<protocol>` parameter is configured.

The configuration is complete. Events that are forwarded to QRadar by CRYPTOCard CRYPTO-Shield are displayed on the **Log Activity** tab.
IBM QRadar supports several CyberArk DSMs.

## CyberArk Privileged Threat Analytics

The IBM QRadar DSM for CyberArk Privileged Threat Analytics collects events from a CyberArk Privileged Threat Analytics device.

The following table describes the specifications for the CyberArk Privileged Threat Analytics DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>CyberArk</td>
</tr>
<tr>
<td>DSM name</td>
<td>CyberArk Privileged Threat Analytics</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-CyberArkPrivilegedThreatAnalytics-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V3.1</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Detected security events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>CyberArk website (<a href="http://www.cyberark.com">http://www.cyberark.com</a>)</td>
</tr>
</tbody>
</table>

To integrate CyberArk Privileged Threat Analytics 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:
   - CyberArk Privileged Threat Analytics DSM RPM
   - DSMCommon RPM
2. Configure your CyberArk Privileged Threat Analytics device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a CyberArk Privileged Threat Analytics log source on the QRadar Console. The following table describes the parameters that require specific values for CyberArk Privileged Threat Analytics event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>CyberArk Privileged Threat Analytics</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4
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 CyberArk Privileged Threat Analytics to communicate with QRadar**

To collect all events from CyberArk Privileged Threat Analytics, you must specify IBM QRadar as the syslog server and configure the syslog format. The CyberArk Privileged Threat Analytics device sends syslog events that are formatted as Log Event Extended Format (LEEF).

**Procedure**

1. On the CyberArk Privileged Threat Analytics machine, go to the `/opt/tomcat/diamond-resources/local/` directory, and open the `systemparm.properties` file in a text editor such as `vi`.
2. Uncomment the `syslog_outbound` property and then edit the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The host name or IP address of the QRadar system.</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
</tr>
<tr>
<td>Format</td>
<td>QRadar</td>
</tr>
</tbody>
</table>

   **Example:** The following is an example of the `syslog_outbound` property:

   ```json
   syslog_outbound=[{"host": "SIEM_MACHINE_ADDRESS", "port": 514, "format": "QRadar", "protocol": "UDP"}]
   ```

   **Example:** The following is an example of the `syslog_outbound` property specifying multiple syslog recipients, separated by commas:

   ```json
   syslog_outbound=[{"host": "SIEM_MACHINE_ADDRESS", "port": 514, "format": "QRadar", "protocol": "UDP"},{"host": "SIEM_MACHINE_ADDRESS1", "port": 514, "format": "QRadar", "protocol": "UDP"}, ...]
   ```
3. Save the `systemparm.properties` configuration file, and then close it.
4. Restart CyberArk Privileged Threat Analytics.

**CyberArk Vault**

The CyberArk Vault DSM for IBM QRadar accepts events by using syslog that is formatted for Log Enhanced Event Format (LEEF).

QRadar records both user activities and safe activities from the CyberArk Vault in the audit event logs. CyberArk Vault integrates with QRadar to forward audit logs by using syslog to create a detailed log of privileged account activities.

**Event type format**

CyberArk Vault must be configured to generate events in Log Enhanced Event Protocol (LEEF) and to forward these events by using syslog. The LEEF format consists of a pipe ( | ) delimited syslog header, and tab separated fields in the log payload section.

If the syslog events from CyberArk Vault are not formatted properly, examine your device configuration or software version to ensure that your appliance supports LEEF. Properly formatted LEEF event messages are automatically discovered and added as a log source to QRadar.
Configuring syslog for CyberArk Vault

To configure CyberArk Vault to forward syslog events to IBM QRadar:

Procedure
1. Log in to your CyberArk device.
2. Edit the DBParm.ini file.
3. Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SyslogServerIP</td>
<td>Type the IP address of QRadar.</td>
</tr>
<tr>
<td>SyslogServerPort</td>
<td>Type the UDP port that is used to connect to QRadar. The default value is 514.</td>
</tr>
<tr>
<td>SyslogMessageCodeFilter</td>
<td>Configure which message codes are sent from the CyberArk Vault to QRadar. You can define specific message numbers or a range of numbers. By default, all message codes are sent for user activities and safe activities. <strong>Example:</strong> To define a message code of 1,2,3,30 and 5-10, you must type: 1,2,3,5-10,30.</td>
</tr>
<tr>
<td>SyslogTranslatorFile</td>
<td>Type the file path to the LEEF.xsl translator file. The translator file is used to parse CyberArk audit records data in the syslog protocol.</td>
</tr>
</tbody>
</table>

4. Copy LEEF.xsl to the location specified by the **SyslogTranslatorFile** parameter in the DBParm.ini file.

Results
The configuration is complete. The log source is added to QRadar as CyberArk Vault events are automatically discovered. Events that are forwarded by CyberArk Vault are displayed on the Log Activity tab of QRadar.

Configuring a log source for CyberArk Vault
IBM QRadar automatically discovers and creates a log source for syslog events from CyberArk Vault.

About this task
The following configuration steps are optional.

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 CyberArk Vault.

10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your CyberArk Vault appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.

12. On the Admin tab, click Deploy Changes.
Chapter 51. CyberGuard Firewall/VPN Appliance

The CyberGuard Firewall VPN Appliance DSM for IBM QRadar accepts CyberGuard events by using syslog. QRadar records all relevant CyberGuard events for CyberGuard KS series appliances that are forwarded by using syslog.

Configuring syslog events

To configure a CyberGuard device to forward syslog events:

Procedure
1. Log in to the CyberGuard user interface.
2. Select the Advanced page.
4. Type the IP address of IBM QRadar.
5. Click Apply.

The configuration is complete. The log source is added to QRadar as CyberGuard events are automatically discovered. Events that are forwarded by CyberGuard appliances are displayed on the Log Activity tab of QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from CyberGuard appliances.

About this task
The following configuration steps are optional.

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 CyberGuard TSP Firewall/VPN.
9. From the Protocol Configuration list, select Syslog.
10. For the Log Source Identifier parameter, enter the IP address or host name for the log source as an identifier for events from your CyberGuard appliance.
11. Click Save.
12. On the Admin tab, click Deploy Changes.
Chapter 52. Damballa Failsafe

The Failsafe DSM for IBM QRadar accepts syslog events by using the Log Event Extended Format (LEEF), enabling QRadar to record all relevant Damballa Failsafe events.

Damballa Failsafe must be configured to generate events in Log Event Extended Format (LEEF) and forward these events by using syslog. The LEEF format consists of a pipe (|) delimited syslog header, and tab separated fields in the log event payload.

If the syslog events that are forwarded from your Damballa Failsafe are not correctly formatted in LEEF format, you must check your device configuration or software version to ensure that your appliance supports LEEF. Properly formatted LEEF event messages are automatically discovered and added as a log source to QRadar.

Configuring syslog for Damballa Failsafe

To collect events, you must configure your Damballa Failsafe device to forward syslog events to IBM QRadar.

**Procedure**

1. Log in to your Damballa Failsafe Management Console.
2. From the navigation menu, select Setup > Integration Settings.
3. Click the QRadar tab.
4. Select Enable Publishing to IBM QRadar.
5. Configure the following options:
   - **Hostname** - Type the IP address or Fully Qualified Name (FQN) of your QRadar Console.
   - **Destination Port** - Type 514. By default, QRadar uses port 514 as the port for receiving syslog events.
   - **Source Port** - This input is not a requirement. Type the Source Port your Damballa Failsafe device uses for sending syslog events.
6. Click Save.

The configuration is complete. The log source is added to QRadar as Damballa Failsafe events are automatically discovered. Events that are forwarded by Damballa Failsafe are displayed on the Log Activity tab of QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Damballa Failsafe devices.

**About this task**

The following configuration steps are optional.

**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 Damballa Failsafe.


10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 240. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.

12. On the Admin tab, click Deploy Changes.

The configuration is complete.
Chapter 53. DG Technology MEAS

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>DG Technology</td>
</tr>
<tr>
<td>Log source type</td>
<td>DG Technology MEAS</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-DGTechnologyMEAS-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>8.x</td>
</tr>
<tr>
<td>Protocol configuration</td>
<td>LEEF Syslog</td>
</tr>
<tr>
<td>Supported event types</td>
<td>Mainframe events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom event properties</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>DG Technology website (<a href="http://www.dgtechllc.com">http://www.dgtechllc.com</a>)</td>
</tr>
</tbody>
</table>

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 DSM” on page 4

“Adding a log source” on page 4

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
   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 54. Digital China Networks (DCN)

The Digital China Networks (DCN) DCS/DCRS Series DSM for IBM QRadar can accept events from Digital China Networks (DCN) switches by using syslog.

IBM QRadar records all relevant IPv4 events that are forwarded from DCN switches. To integrate your device with QRadar, you must configure a log source, then configure your DCS or DCRS switch to forward syslog events.

Supported Appliances
The DSM supports the following DCN DCS/DCRS Series switches:
- DCS - 3650
- DCS - 3950
- DCS - 4500
- DCRS - 5750
- DCRS - 5960
- DCRS - 5980
- DCRS - 7500
- DCRS - 9800

Configuring a log source
IBM QRadar does not automatically discover incoming syslog events from DCN DCS/DCRS Series switches.

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 DCN DCS/DCRS Series.
10. Configure the following value:

<table>
<thead>
<tr>
<th>Table 242. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>
11. Click Save.
12. On the Admin tab, click Deploy Changes.
The log source is added to QRadar. You are now ready to configure your Digital China Networks DCS or DCRS Series switch to forward events to QRadar.

**Configuring a DCN DCS/DCRS Series Switch**

To collect events, you must configure your DCN DCS/DCRS Series switch in IBM QRadar.

**Procedure**

1. Log in to your DCN DCS/DCRS Series Switch command-line interface (CLI).
2. Type the following command to access the administrative mode:
   ```
   enable
   ```
3. Type the following command to access the global configuration mode:
   ```
   config
   ```
   The command-line interface displays the configuration mode prompt:
   ```
   Switch(Config)#
   ```
4. Type the following command to configure a log host for your switch:
   ```
   logging <IP address> facility <local> severity <level>
   ```
   Where:
   - `<IP address>` is the IP address of the QRadar Console.
   - `<local>` is the syslog facility, for example, local0.
   - `<level>` is the severity of the syslog events, for example, informational. If you specify a value of informational, you forward all information level events and later (more severe), such as, notifications, warnings, errors, critical, alerts, and emergencies.
   For example,
   ```
   logging <IP_address> facility local0 severity informational
   ```
5. Type the following command to save your configuration changes:
   ```
   write
   ```

   The configuration is complete. You can verify the events that are forwarded to QRadar by viewing events in the **Log Activity** tab.
Chapter 55. Enterprise-IT-Security.com SF-Sherlock

The IBM QRadar DSM for Enterprise-IT-Security.com SF-Sherlock collects logs from your Enterprise-IT-Security.com SF-Sherlock servers.

The following table describes the specifications for the Enterprise-IT-Security.com SF-Sherlock DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Enterprise-IT-Security.com</td>
</tr>
<tr>
<td>DSM name</td>
<td>Enterprise-IT-Security.com SF-Sherlock</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-EnterpriseITSecuritySFSherlock-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>v8.1 and later</td>
</tr>
<tr>
<td>Event format</td>
<td>Log Event Extended Format (LEEF)</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Enterprise-IT-Security website (<a href="http://www.enterprise-it-security.com">http://www.enterprise-it-security.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Enterprise-IT-Security.com SF-Sherlock 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:
   - Enterprise-IT-Security.com SF-Sherlock DSM RPM
   - DSM Common RPM

2. Configure your Enterprise-IT-Security.com SF-Sherlock device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Enterprise-IT-Security.com SF-Sherlock log source on the QRadar Console. The following table describes the parameters that require specific values for Enterprise-IT-Security.com SF-Sherlock event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Enterprise-IT-Security.com SF-Sherlock</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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 Enterprise-IT-Security.com SF-Sherlock to communicate with QRadar

Before you can send SF-Sherlock events and assessment details to QRadar, implement the SF-Sherlock 2 QRadar connection kit.

**About this task**

The information that is sent to QRadar can be defined and selected in detail. Regardless of the selected transfer method, all information reaches QRadar as LEEF-formatted records.

**Procedure**

1. Install the UMODQR01 and UMODQR02 SF-Sherlock SMP/E user modifications by using the corresponding SHERLOCK.SSHKSAMP data set members.
2. If you send SF-Sherlock’s LEEF records to a QRadar syslog daemon, which is generally the preferred transfer method, you must install the SF-Sherlock universal syslog message router in the USS environment of z/OS. You will find all installation details within the UNIXCMDL member of the SHERLOCK.SSHKSAMP data set.
3. Optional: If you transfer the logs by FTP or another technique, you must adapt the UMODQR01 user modification.
4. Enter the IP address for the QRadar LEEF syslog server, transfer method (UDP or TCP), and port number (514) in the QRADARSE member of SF-Sherlock’s init-deck parameter configuration file.
5. Allocate the QRadar related log data set by using the ALLOCQRG job of the SHERLOCK.SSHKSAMP data set. It is used by the SHERLOCK started procedure (STC) to keep all QRadar LEEF records transferring to QRadar.
6. The QRDARTST member of the SHERLOCK.SSHKSAMP data set can be used to test the SF-Sherlock 2 QRadar message routing connection. If QRadar receives the test events, the implementation was successful.
7. Enable the SF-Sherlock 2 QRadar connection in your SF-Sherlock installation by activating QRADAR00 (event monitoring) and optionally, the QRADAR01 (assessment details) init-deck members, through the already prepared ADD QRADARxx statements within the $BUILD00 master control member.
8. Refresh or recycle the SHERLOCK started procedure to activate the new master control member that enables the connection of SF-Sherlock to QRadar.
Chapter 56. Epic SIEM

The IBM QRadar DSM for Epic SIEM can collect event logs from your Epic SIEM. The following table identifies the specifications for the Epic SIEM DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Epic</td>
</tr>
<tr>
<td>DSM name</td>
<td>Epic SIEM</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-EpicSIEM-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>Epic 2014, Epic 2015, Epic 2017</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit, Authentication</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Epic website (<a href="http://www.epic.com/">http://www.epic.com/</a>)</td>
</tr>
</tbody>
</table>

To integrate Epic SIEM DSM 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:
   - Epic SIEM DSM RPM
   - DSMCommon RPM
2. Configure your Epic SIEM device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an Epic SIEM log source on the QRadar Console. The following table describes the parameters that require specific values for Epic SIEM event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Epic SIEM</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Epic SIEM 2014 to communicate with QRadar

To collect syslog events from Epic SIEM 2014, you must add an external syslog server for the IBM QRadar host.

**Procedure**

1. If all web services are not enabled for your instance of Interconnect, complete the following steps to run the required `SendSIEMSyslogAudit` service:
   a) To access the Interconnect Configuration Editor, click **Start > Epic 2014 > Interconnect > your_instance > Configuration Editor**.
   b) In the Configuration Editor, select the Business Services form.
   c) On the Service Category tab, click **SendSIEMSyslogAudit**.
   d) Click **Save**

2. Log in to your Epic server.

3. Click **Epic System Definitions (%ZeUSTBL) > Security > Auditing Options > SIEM Syslog Settings > SIEM Syslog Configuration**.

4. Use the following table to configure the parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIEM Host</td>
<td>The host name or IP address of the QRadar appliance.</td>
</tr>
<tr>
<td>SIEM Port</td>
<td>514</td>
</tr>
<tr>
<td>SIEM Format</td>
<td>LEEF (Log Event Extended Format).</td>
</tr>
</tbody>
</table>

5. From the **SIEM Syslog Settings** menu, click **SIEM Syslog** and set it to enabled.

   The SIEM Syslog Sending daemon is automatically started when the environment is set to runlevel Up or when you enable **SIEM Syslog**.

6. If you want to stop the daemon, from the **SIEM Syslog Settings** menu, click **SIEM Syslog** and set it to disabled.

   **Important:** If you stop the daemon when the syslog setting is enabled, the system continues to log data without purging. If you want to stop the daemon when the syslog setting is enabled, contact your Epic representative or your system administrator.

### Configuring Epic SIEM 2015 to communicate with QRadar

To collect events in IBM QRadar, you must configure the messaging queue values on your Epic SIEM 2015 system.

**Procedure**

1. From the command line, select **Interconnect Administrator's Menu > Messaging Queues Setup**.
2. Type an asterisk (*) to create the EMPSYNC queue.
3. Enter the queue values identified in the following table for each of the prompts.

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue ID</td>
<td>Type an ID for the queue.</td>
</tr>
</tbody>
</table>
### Table 247. Queue values for EMPSYNC prompts (continued)

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue Name</td>
<td>EMPSYNC</td>
</tr>
<tr>
<td>Descriptor</td>
<td>EMPSYNC</td>
</tr>
<tr>
<td>Run on Node</td>
<td>Press the <strong>Enter</strong> key. The value is automatically populated.</td>
</tr>
<tr>
<td>IC Servers</td>
<td>Press the <strong>Enter</strong> key, without typing a value.</td>
</tr>
<tr>
<td>Edit advanced settings for this queue?</td>
<td>Yes</td>
</tr>
<tr>
<td>Does this queue handle synchronous outgoing messages?</td>
<td>Yes</td>
</tr>
<tr>
<td>Associate this descriptor with a queue type for outgoing communication?</td>
<td>Yes</td>
</tr>
<tr>
<td>Queue Type</td>
<td>EMP</td>
</tr>
</tbody>
</table>

4. Type an asterisk (*) to create the EMPASYNC queue.
5. Enter the queue values identified in the following table for each of the prompts.

### Table 248. Queue values for EMPASYNC prompts

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue ID</td>
<td>Type an ID for the queue.</td>
</tr>
<tr>
<td>Queue Name</td>
<td>EMPASYNC</td>
</tr>
<tr>
<td>Descriptor</td>
<td>EMPASYNC</td>
</tr>
<tr>
<td>Run on Node</td>
<td>Press the <strong>Enter</strong> key. The value is automatically populated.</td>
</tr>
<tr>
<td>IC Servers</td>
<td>Press the <strong>Enter</strong> key, without typing a value.</td>
</tr>
<tr>
<td>Edit advanced settings for this queue?</td>
<td>Yes</td>
</tr>
<tr>
<td>Does this queue handle synchronous outgoing messages?</td>
<td>No</td>
</tr>
<tr>
<td>Associate this descriptor with a queue type for outgoing communication?</td>
<td>Yes</td>
</tr>
<tr>
<td>Queue Type</td>
<td>EMP</td>
</tr>
</tbody>
</table>

6. Deploy a new interconnect instance by using Kuiper.
7. Access the **Interconnect Configuration Editor** in Windows, by clicking **Start > Epic 2015 > Interconnect > your_instance > Configuration Editor**.
8. Select the **General Web Service Host** role.
9. In **Cache Connections**, manually add the queue by the queue type, **EMP**.
10. Set the number of threads to 2.

For more information about thread count recommendations, refer to your Epic documentation.

**Important:** Do not enable any services on the **Business Services** tab.
11. Log in to your Epic server.
12. Click **Epic System Definitions (%ZeUSTBL) > Security > Auditing Options > SIEM Syslog Settings**.
13. Select **SIEM Syslog Configuration**, and then configure the following parameters:
### Configuring Epic SIEM 2017 to communicate with QRadar

To collect events in IBM QRadar, you must configure the messaging queue values on your Epic SIEM 2017 system.

**Procedure**

1. From the command line, select **Interconnect Administrator’s Menu > Messaging Queues Setup**.
2. Type an asterisk (*) to create the EMPSYNC queue.
3. Enter the queue values identified in the following table for each of the prompts.

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue ID</td>
<td>Type an ID for the queue.</td>
</tr>
<tr>
<td>Queue Name</td>
<td>EMPSYNC</td>
</tr>
<tr>
<td>Descriptor</td>
<td>EMPSYNC</td>
</tr>
<tr>
<td>Run on Node</td>
<td>Press the <strong>Enter</strong> key. The value is automatically populated.</td>
</tr>
<tr>
<td>IC Servers</td>
<td>Press the <strong>Enter</strong> key, without typing a value.</td>
</tr>
<tr>
<td>Edit advanced settings for this queue?</td>
<td>Yes</td>
</tr>
<tr>
<td>Does this queue handle synchronous outgoing messages?</td>
<td>Yes</td>
</tr>
<tr>
<td>Associate this descriptor with a queue type for outgoing communication?</td>
<td>Yes</td>
</tr>
<tr>
<td>Queue Type</td>
<td>EMP</td>
</tr>
</tbody>
</table>

4. Type an asterisk (*) to create the EMPASYNC queue.
5. Enter the queue values identified in the following table for each of the prompts.

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue ID</td>
<td>Type an ID for the queue.</td>
</tr>
<tr>
<td>Queue Name</td>
<td>EMPASYNC</td>
</tr>
</tbody>
</table>
Table 250. Queue values for EMPASYNC prompts (continued)

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Descriptor</td>
<td>EMPASYNC</td>
</tr>
<tr>
<td>Run on Node</td>
<td>Press the Enter key. The value is automatically populated.</td>
</tr>
<tr>
<td>IC Servers</td>
<td>Press the Enter key, without typing a value.</td>
</tr>
<tr>
<td>Edit advanced settings for this queue?</td>
<td>Yes</td>
</tr>
<tr>
<td>Does this queue handle synchronous outgoing messages?</td>
<td>No</td>
</tr>
<tr>
<td>Associate this descriptor with a queue type for outgoing communication?</td>
<td>Yes</td>
</tr>
<tr>
<td>Queue Type</td>
<td>EMP</td>
</tr>
</tbody>
</table>

6. Deploy a new interconnect instance by using Kuiper.

7. Access the Interconnect Configuration Editor in Windows, by clicking Start > Epic 2017 > Interconnect > your_instance > Configuration Editor.

8. Select the General Web Service Host role.

9. In Cache Connections, manually add the queue by the queue type, EMP.

10. Set the number of threads to 2.

For more information about thread count recommendations, see your Epic documentation.

**Important:** Do not enable any services on the Business Services tab.

11. Log in to your Epic server.

12. Click Epic System Definitions (%ZeUSTBL) > Security > Auditing Options > SIEM Syslog Settings.

13. Select SIEM Syslog Configuration, and then configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIEM Host</td>
<td>Your QRadar Event Collector host name or IP address.</td>
</tr>
<tr>
<td>SIEM Port</td>
<td>514</td>
</tr>
<tr>
<td>SIEM Format</td>
<td>LEEF (Log Event Extended Format)</td>
</tr>
<tr>
<td>Check Application Layer Response</td>
<td>Disable</td>
</tr>
</tbody>
</table>

14. Return to the SIEM Syslog Settings Menu.

15. If you want to reduce traffic that comes in to your SIEM system, disable the auditing events that your system does not require:

   a) Click SIEM Syslog Configuration Options > Edit Events List.
   
   b) From the Edit Events List, select T for each event that you want to disable.
   
   c) Click Q to quit.

16. Select SIEM Syslog and set it to Enabled.

   **Note:** The SIEM Syslog Sending daemon is automatically started when the environment is set to runlevel Up or when you enable SIEM Syslog. If you want to stop the daemon, from the SIEM Syslog Settings menu, click SIEM Syslog and set it to Disabled.
Chapter 57. ESET Remote Administrator

The IBM QRadar DSM for ESET Remote Administrator collects logs from ESET Remote Administrator. The following table describes the specifications for the ESET Remote Administrator DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>ESET</td>
</tr>
<tr>
<td>DSM name</td>
<td>ESET Remote Administrator</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-ESETRemoteAdministrator-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>6.4.270</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Log Extended Event Format (LEEF)</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Threat, Firewall aggregated, Host Intrusion Protection System (HIPS) aggregated, Audit</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate ESET Remote Administrator with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs in the order that they are listed, on your QRadar Console:
   - DSMCommon RPM
   - ESET Remote Administrator DSM RPM
2. Configure your ESET Remote Administrator server to send LEEF formatted syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an ESET Remote Administrator log source on the QRadar Console. The following table describes the parameters that require specific values for ESET Remote Administrator event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>ESET Remote Administrator</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the ESET Remote Administration server.</td>
</tr>
</tbody>
</table>
4. To check that QRadar parses the events correctly, review the following sample event message.

The following table shows a sample event message from ESET Remote Administrator:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native user login</td>
<td>User Login Success</td>
<td>&lt;14&gt;1 2016-08-15T14:52:31.888Z hostname ERAServer 28021 - - LEEF:1.0</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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 ESET Remote Administrator to communicate with QRadar

Configure your ESET Remote Administrator (ERA) server to send LEEF formatted syslog events to IBM QRadar.

**About this task**
To complete the configuration, you must enable the Syslog server, and then configure the logging settings.

**Note:**
The required parameters listed in the following steps are configured in the Server Settings pane. To see a graphic, go to the ESET website. (http://help.eset.com/era_admin/64/en-US/index.html?admin_server_settings_export_to_syslog.htm)

**Procedure**
1. Log in to your ERA web console.
2. In the Admin navigation pane, click Server Settings.
3. In the SYSLOG SERVER area, select the Use Syslog server check box.
4. In the Host field, type the host name for your QRadar Event Collector.
5. In the Port field, type 514.
6. In the LOGGING area, select the Export logs to Syslog check box.
7. From the Exported logs format list, select LEEF.
8. Click Save.
Chapter 58. Exabeam

The IBM QRadar DSM for Exabeam collects events from an Exabeam device.
The following table describes the specifications for the Exabeam DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Exabeam</td>
</tr>
<tr>
<td>DSM name</td>
<td>Exabeam</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-ExabeamExabeam-Qradar_version-</td>
</tr>
<tr>
<td></td>
<td>build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>v1.7 and v2.0</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Critical Anomalous</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Exabeam website (<a href="http://www.exabeam.com">http://www.exabeam.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Exabeam with QRadar, complete the following steps:

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Exabeam</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Exabeam to communicate with QRadar**

To collect syslog events from Exabeam, you must add a destination that specifies QRadar as the syslog server.

**Procedure**

2. Select https://<Exabeam_IP>:8484 and type #setup at the end of the url address.
3. In the Navigation pane, click Incident Notification.
4. Select Send via Syslog and configure the following syslog parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address or Hostname</td>
<td>The IP address of the QRadar Event Collector.</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
<tr>
<td>Syslog Severity Level</td>
<td>Emergency</td>
</tr>
</tbody>
</table>

**IBM QRadar : QRadar DSM Configuration Guide**
Chapter 59. Extreme

IBM QRadar accepts events from a range of Extreme DSMs.

Extreme 800-Series Switch

The Extreme 800-Series Switch DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant audit, authentication, system, and switch events. Before you configure your Extreme 800-Series Switch in QRadar, you must configure your switch to forward syslog events.

Configuring your Extreme 800-Series Switch

Configuring the Extreme 800-Series Switch to forward syslog events.

About this task

To manually configure the Extreme 800-Series Switch:

Procedure

1. Log in to your Extreme 800-Series Switch command-line interface.
   You must be a system administrator or operator-level user to complete these configuration steps.
2. Type the following command to enable syslog:
   ```
   enable syslog
   ```
3. Type the following command to create a syslog address for forwarding events to QRadar:
   ```
   create syslog host 1 <IP address> severity informational facility local7 udp_port 514 state enable
   ```
   Where: `<IP address>` is the IP address of your QRadar Console or Event Collector.
4. Type the following command to forward syslog events by using an IP interface address:
   ```
   create syslog source_ipif <name> <IP address>
   ```
   Where:
   - `<name>` is the name of your IP interface.
   - `<IP address>` is the IP address of your QRadar Console or Event Collector.

The configuration is complete. The log source is added to QRadar as Extreme 800-Series Switch events are automatically discovered. Events that are forwarded to QRadar by Extreme 800-Series Switches are displayed on the Log Activity tab of QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Extreme 800-Series Switches.

About this task

The following configuration steps are optional. To manually configure a log source:

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 **Extreme 800-Series Switch**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th><strong>Table 256. Syslog parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

---

**Extreme Dragon**

The Extreme Dragon DSM for IBM QRadar accepts Extreme events by using syslog to record all relevant Extreme Dragon events.

**About this task**

To configure your QRadar Extreme Dragon DSM, use the following procedure:

**Procedure**

1. Create an Alarm Tool policy by using a Syslog notification rule. See “Creating a Policy for Syslog” on page 438.
2. Configure the log source within QRadar. See “Configuring a log source” on page 440.
3. Configure Dragon Enterprise Management Server (EMS) to forward syslog messages. See “Configure the EMS to forward syslog messages” on page 440.

**Creating a Policy for Syslog**

This procedure describes how to configure an Alarm Tool policy by using a syslog notification rule in the Log Event Extended Format (LEEF) message format.

**About this task**

LEEF is the preferred message format for sending notifications to Dragon Network Defense when the notification rate is high or when IPv6 addresses are displayed. If you do not want to use syslog notifications in LEEF format, refer to your Extreme Dragon documentation for more information.

To configure Extreme Dragon with an Alarm Tool policy by using a syslog notification rule, complete the following steps:

**Procedure**

1. Log in to the Extreme Dragon EMS.
2. Click the **Alarm Tool** icon.
3. Configure the Alarm Tool Policy:
In the **Alarm Tool Policy View > Custom Policies** menu tree, right-click and select **Add Alarm Tool Policy**.

4. In the **Add Alarm Tool Policy** field, type a policy name. For example:

   QRadar

5. Click **OK**.

6. In the menu tree, select **QRadar**.

7. To configure the event group:

   - Click the **Events Group** tab.

8. Click **New**.

   The **Event Group Editor** is displayed.

9. Select the event group or individual events to monitor.

10. Click **Add**.

    A prompt is displayed.

11. Click **Yes**.

12. In the right column of the **Event Group Editor**, type **Dragon-Events**.

13. Click **OK**.

14. Configure the Syslog notification rule:

    - Click the **Notification Rules** tab.

15. Click **New**.

16. In the name field, type **QRadar-RuleSys**.

17. Click **OK**.

18. In the **Notification Rules** pane, select the newly created **QRadar-RuleSys** item.

19. Click the **Syslog** tab.

20. Click **New**.

    The **Syslog Editor** is displayed.

21. Update the following values:

    - **Facility** - Using the **Facility** list, select a facility.
    - **Level** - Using the **Level** list, select **notice**.
    - **Message** - Using the **Type** list, select **LEEF**.

    

    LEEF:Version=1.0|Vendor|Product|ProductVersion|eventID|devTime|

    

    proto|src|sensor|dst|srcPort|dstPort|direction| eventData|

    The LEEF message format delineates between fields by using a pipe delimiter between each keyword.

22. Click **OK**.

23. Verify that the notification events are logged as separate events:

    - Click the **Global Options** tab.

24. Click the **Main** tab.

25. Make sure that **Concatenate Events** is not selected.

26. Configure the alarm information:

    - Click the **Alarms** tab.

27. Click **New**.

28. Type values for the parameters:
• **Name** - Type QRadar-Alarm.
• **Type** - Select **Real Time**.
• **Event Group** - Select **Dragon-Events**.
• **Notification Rule** - Select the QRadar-RuleSys check box.

29. Click **OK**.
30. Click **Commit**.
31. Navigate to the **Enterprise View**.
32. Right-click on the **Alarm Tool** and select **Associate Alarm Tool Policy**.
33. Select the newly created QRadar **policy**. Click **OK**.
34. In the **Enterprise** menu, right-click the policy and select **Deploy**.

You are now ready to configure a syslog log source in QRadar.

### Configuring a log source
You are now ready to configure the log source in IBM QRadar.

**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 **Extreme Dragon Network IPS**.
9. From the **Protocol Configuration** list, select **Syslog**.

For more information about Extreme Dragon device, see your **Extreme Dragon documentation**.

**Note:** Using the event mapping tool in the **Log Activity** tab, you can map a normalized or raw event to a high-level and low-level category (or QID). However, you cannot map combination Dragon messages using the event mapping tool. For more information, see the **IBM QRadar User Guide**.

### Configure the EMS to forward syslog messages
Starting with Dragon Enterprise Management Server (EMS) v7.4.0 appliances, you must use syslog-ng for forwarding events to a Security and Information Manager such as IBM QRadar.

Syslogd has been replaced by syslog-ng in Dragon EMS v7.4.0 and later.

To configure EMS to forward syslog messages, you must choose one of the following:

- If you are using syslog-ng and Extreme Dragon EMS v7.4.0 and later, see “**Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later**” on page 440.
- If you are using syslogd and Extreme Dragon EMS v7.4.0 and below, see “**Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier**” on page 441.

### Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later
This section describes the steps to configure syslog-ng in non-encrypted mode and syslogd to forward syslog messages to IBM QRadar.

**About this task**
If you are using encrypted syslog-ng, refer to your **Extreme documentation**.

Do not run both syslog-ng and syslogd at the same time.
To configure syslog-ng in non-encrypted mode:

**Procedure**

1. On your EMS system, open the following file:
   
   `/opt/syslog-ng/etc/syslog-ng.conf`

2. Configure a **Facility** filter for the Syslog notification rule.
   
   For example, if you selected `facility local1`:
   
   ```
   filter filt_facility_local1 {facility(local1); };
   ```

3. Configure a **Level** filter for the Syslog notification rule.
   
   For example, if you selected `level notice`:
   
   ```
   filter filt_level_notice {level(notice); };
   ```

4. Configure a destination statement for the QRadar.
   
   For example, if the IP address of the QRadar is 192.0.2.1 and you want to use syslog port of 514, type:
   
   ```
   destination siem { tcp("192.0.2.1" port(514)); };
   ```

5. Add a log statement for the notification rule:
   
   ```
   log { source(s_local); filter (filt_facility_local1); filter (filt_level_notice); destination(siem); };
   ```

6. Save the file and restart syslog-ng.
   
   ```
   cd /etc/rc.d ./rc.syslog-ng stop ./rc.syslog-ng start
   ```

7. The Extreme Dragon EMS configuration is complete.

**Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier**

If your Dragon Enterprise Management Server (EMS) is using a version earlier than V7.4.0 on the appliance, you must use syslogd for forwarding events to a Security and Information Manager such as IBM QRadar.

**Procedure**

1. On the Dragon EMS system, open the following file:
   
   `/etc/syslog.conf`

2. Add a line to forward the **facility** and **level** you configured in the syslog notification rule to QRadar.
   
   For example, to define the `facility local1` and `level notice`:
   
   ```
   local1notice @<IP address>
   ```

   Where:
   
   `<IP address>` is the IP address of the QRadar system.

3. Save the file and restart syslogd.
   
   ```
   cd /etc/rc.d ./rc.syslog stop ./rc.syslog start
   ```

   The Extreme Dragon EMS configuration is complete.

**Extreme HiGuard Wireless IPS**

The Extreme HiGuard Wireless IPS DSM for IBM QRadar records all relevant events by using syslog

Before you configure the Extreme HiGuard Wireless IPS device in QRadar, you must configure your device to forward syslog events.
Configuring Enterasys HiGuard
To configure the device to forward syslog events:

Procedure
1. Log in to the HiGuard Wireless IPS user interface.
2. In the left navigation pane, click **Syslog**, which allows the management server to send events to designated syslog receivers.
   
   The **Syslog Configuration** pane is displayed.
3. In the **System Integration Status** section, **enable** syslog integration.
   
   Enabling syslog integration allows the management server to send messages to the configured syslog servers. By default, the management server enables syslog.
   
   The **Current Status** field displays the status of the syslog server. The choices are: **Running** or **Stopped**. An error status is displayed if one of the following occurs:
   
   • One of the configured and enabled syslog servers includes a host name that cannot be resolved.
   • The management server is stopped.
   • An internal error occurred. If this error occurs, contact Enterasys Technical Support.
4. From **Manage Syslog Servers**, click **Add**.
   
   The **Syslog Configuration** window is displayed.
5. Type values for the following parameters:
   
   • **Syslog Server (IP Address/Hostname)** - Type the IP address or host name of the syslog server where events are sent.
   
   **Note:** Configured syslog servers use the DNS names and DNS suffixes configured in the **Server initialization and Setup Wizard** on the HWMH Config Shell.
   
   • **Port Number** - Type the port number of the syslog server to which HWMH sends events. The default is 514.
   
   • **Message Format** - Select **Plain Text** as the format for sending events.
   
   • **Enabled?** - Select **Enabled?** if you want events to be sent to this syslog server.
6. Save your configuration.
   
   The configuration is complete. The log source is added to IBM QRadar as HiGuard events are automatically discovered. Events that are forwarded to QRadar by Enterasys HiGuard are displayed on the **Log Activity** tab of QRadar.

Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Extreme HiGuard.

About this task
The following configuration steps are optional. To manually configure a log source for Extreme HiGuard:

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 Extreme HiGuard.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for</td>
</tr>
<tr>
<td></td>
<td>events from your Extreme HiGuard.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The configuration is complete.

**Extreme HiPath Wireless Controller**

The Extreme HiPath Wireless Controller DSM for IBM QRadar records all relevant events by using syslog. QRadar supports the following Extreme HiPath Wireless Controller events:

- Wireless access point events
- Application log events
- Service log events
- Audit log events

**Configuring your HiPath Wireless Controller**

To integrate your Extreme HiPath Wireless Controller events with IBM QRadar, you must configure your device to forward syslog events.

**About this task**

To forward syslog events to QRadar:

**Procedure**

1. Log in to the HiPath Wireless Assistant.
2. Click Wireless Controller Configuration.
   
   The HiPath Wireless Controller Configuration window is displayed.
3. From the menu, click System Maintenance.
4. From the Syslog section, select the Syslog Server IP check box and type the IP address of the device that receives the syslog messages.
5. Using the Wireless Controller Log Level list, select Information.
7. Using the Application Logs list, select local.0.
8. Using the Service Logs list, select local.3.
9. Using the Audit Logs list, select local.6.
10. Click Apply.

You are now ready to configure the log source in QRadar.
Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Extreme HiPath. The following configuration steps are optional.

About this task
To manually configure a log source for Extreme HiPath:

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 Extreme HiPath.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Extreme HiPath.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The configuration is complete. For more information about your Extreme HiPath Wireless Controller device, see your vendor documentation.

Extreme Matrix Router
The Extreme Matrix Router DSM for IBM QRadar accepts Extreme Matrix events by using SNMPv1, SNMPv2, SNMPv3, and syslog.

About this task
You can integrate Extreme Matrix Router version 3.5 with QRadar. QRadar records all SNMP events, syslog login, logout, and login failed events. Before you configure QRadar to integrate with Extreme Matrix, you must take the following steps:

Procedure
1. Log in to the switch/router as a privileged user.
2. Type the following command:

   set logging server <server number> description <description> facility <facility> ip_addr <IP address> port <port> severity <severity>

   Where:
   - <server number> is the server number with values 1 - 8.
   - <description> is a description of the server.
• `<facility>` is a syslog facility, for example, local0.
• `<IP address>` is the IP address of the server that receives the syslog messages.
• `<port>` is the default UDP port that the client uses to send messages to the server. Use port 514 unless otherwise stated.
• `<severity>` is the server severity level with values 1 - 9, where 1 indicates an emergency, and 8 is debug level.

For example:

```bash
set logging server 5 description ourlogserver facility local0 ip_addr 192.0.2.1 port 514 severity 8
```

3. You are now ready to configure the log source in QRadar.

Select **Extreme Matrix E1 Switch** from the **Log Source Type** list.

**Related tasks**

“Adding a log source” on page 4

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

---

**Extreme Matrix K/N/S Series Switch**

The Extreme Matrix Series DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant Matrix K-Series, N-Series, or S-Series standalone device events.

**About this task**

Before you configure QRadar to integrate with a Matrix K-Series, N-Series, or S-Series, take the following steps:

**Procedure**

1. Log in to your Extreme Matrix device command-line interface (CLI).
2. Type the following commands:
   a. `set logging server 1 ip-addr <IP Address of Event Processor> state enable`
   b. `set logging application RtrAcl level 8`
   c. `set logging application CLI level 8`
   d. `set logging application SNMP level 8`
   e. `set logging application Webview level 8`
   f. `set logging application System level 8`
   g. `set logging application RtrFe level 8`
   h. `set logging application Trace level 8`
   i. `set logging application RtrLSNat level 8`
   j. `set logging application FlowLimit level 8`
   k. `set logging application UPN level 8`
   l. `set logging application AAA level 8`
   m. `set logging application Router level 8`
   n. `set logging application AddrNtfy level 8`
   o. `set logging application OSPF level 8`
   p. `set logging application VRRP level 8`
   q. `set logging application RtrArpProc level 8`
For more information on configuring the Matrix Series routers or switches, consult your vendor documentation.

3. You are now ready to configure the log sources in QRadar.

To configure QRadar to receive events from an Extreme Matrix Series device, select **Extreme Matrix K/N/S Series Switch** from the Log Source Type list.

Related tasks
“Adding a log source” on page 4

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

**Extreme NetSight Automatic Security Manager**

The Extreme NetSight Automatic Security Manager DSM for IBM QRadar accepts events by using syslog.

**About this task**

QRadar records all relevant events. Before you configure an Extreme NetSight Automatic Security Manager device in QRadar, you must configure your device to forward syslog events.

To configure the device to send syslog events to QRadar:

**Procedure**

1. Log in to the Automatic Security Manager user interface.
2. Click the Automated Security Manager icon to access the Automated Security Manager Configuration window.
   
   **Note:** You can also access the Automated Security Manager Configuration window from the Tool menu.
3. From the left navigation menu, select Rule Definitions.
4. Choose one of the following options:
   
   If a rule is configured, highlight the rule. Click Edit.
5. To create a new rule, click Create.
6. Select the Notifications check box.
7. Click Edit.
   
   The Edit Notifications window is displayed.
8. Click Create.
   
   The Create Notification window is displayed.
9. Using the Type list, select Syslog.
10. In the Syslog Server IP/Name field, type the IP address of the device that receives syslog traffic.
11. Click Apply.
12. Click Close.
13. In the Notification list, select the notification that is configured.
14. Click OK.
15. You are now ready to configure the log source in QRadar.
To configure QRadar to receive events from an Extreme NetSight Automatic Security Manager device, select **Extreme NetsightASM** from the **Log Source Type** list.

For more information about your Extreme NetSight Automatic Security Manager device, see your vendor documentation.

**Related tasks**

“Adding a log source” on page 4

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

---

**Extreme NAC**

The Extreme NAC DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant events.

For details on configuring your Extreme NAC appliances for syslog, consult your vendor documentation. After the Extreme NAC appliance is forwarding syslog events to QRadar, the configuration is complete. The log source is added to QRadar as Extreme NAC events are automatically discovered. Events that are forwarded by Extreme NAC appliances are displayed on the **Log Activity** tab of QRadar.

**Configuring a log source**

IBM QRadar automatically discovers and creates a log source for syslog events from Extreme NAC.

**About this task**

The following configuration steps are optional. To manually configure a log source for Extreme NAC:

**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 **Extreme NAC**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th><strong>Table 259. Syslog parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Log Source Identifier</strong></td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.
Extreme stackable and stand-alone switches

The Extreme stackable and stand-alone switches DSM for IBM QRadar accepts events by using syslog.

About this task
QRadar records all relevant events. Before you configure an Extreme stackable and stand-alone switches device in QRadar, you must configure your device to forward syslog events.

To configure the device to forward syslog events to QRadar:

Procedure
1. Log in to the Extreme stackable and stand-alone switch device.
2. Type the following command:

```
set logging server <index> [ip-addr <IP address>] [facility <facility>] [severity <severity>] [descr <description>] [port <port] [state <enable | disable>]
```

Where:
- `<index>` is the server table index number (1 - 8) for this server.
- `<IP address>` is the IP address of the server you want to send syslog messages. You do not have to enter an IP address. If you do not define an IP address, an entry in the Syslog server table is created with the specified index number, and a message is displayed indicating that there is no assigned IP address.
- `<facility>` is a syslog facility. Valid values are local0 to local7. You do not have to enter a facility value. If the value is not specified, the default value that is configured with the `set logging default` command is applied.
- `<description>` is a description of the facility/server. You do not have to enter a description.
- `<port>` is the default UDP port that the client uses to send messages to the server. If not specified, the default value that is configured with the `set logging default` command is applied. You do not have to enter a port value.
- `<enable | disable>` enables or disables this facility/server configuration. You do not have to choose an option. If the state is not specified, it does not default to either enable or disable.
- `<severity>` is the server severity level that the server will log messages. The valid range is 1 - 8. If not specified, the default value that is configured with the `set logging default` command is applied. You do not have to input a severity value. The following are valid values:
  - 1: Emergencies (system is unusable)
  - 2: Alerts (immediate action needed)
  - 3: Critical conditions
  - 4: Error conditions
  - 5: Warning conditions
  - 6: Notifications (significant conditions)
  - 7: Informational messages
  - 8: Debugging message
3. You can now ready to configure the log source in QRadar.

To configure QRadar to receive events from an Extreme stackable and stand-alone switch device:

From the Log Source Type list, select one of the following options:

- Extreme stackable and stand-alone switches
- Extreme A-Series
• Extreme B2-Series
• Extreme B3-Series
• Extreme C2-Series
• Extreme C3-Series
• Extreme D-Series
• Extreme G-Series
• Extreme I-Series

For more information about your Extreme stackable and stand-alone switches, see your vendor documentation.

Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Extreme Networks ExtremeWare

The Extreme Networks ExtremeWare DSM for IBM QRadar records all relevant Extreme Networks ExtremeWare and Extremeware XOS device events from using syslog.

To integrate QRadar with an ExtremeWare device, you must configure a log source in QRadar, then configure your Extreme Networks ExtremeWare and Extremeware XOS devices to forward syslog events. QRadar does not automatically discover or create log sources for syslog events from ExtremeWare appliances.

Configuring a log source
To integrate with IBM QRadar, you must manually create a log source to receive the incoming ExtremeWare events that are forwarded to QRadar.

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 Extreme Networks ExtremeWare Operating System (OS).
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 260. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
The log source is added to QRadar. Events that are forwarded to QRadar by Extreme Networks ExtremeWare appliances are displayed on the Log Activity tab.

For information on configuring syslog forwarding for your Extremeware appliances, see your vendor documentation.

**Extreme XSR Security Router**

The Extreme XSR Security Router DSM for IBM QRadar accepts events by using syslog.

**About this task**

QRadar records all relevant events. Before you configure an Extreme XSR Security Router in QRadar, you must configure your device to forward syslog events.

To configure the device to send syslog events to QRadar:

**Procedure**

1. Using Telnet or SSH, log in to the XSR Security Router command-line interface.
2. Type the following commands to access config mode:
   a. `enable`
   b. `config`
3. Type the following command:
   ```bash
   logging <IP address> low
   ```
   Where: `<IP address>` is the IP address of your QRadar.
4. Exit from config mode.
   ```bash
   exit
   ```
5. Save the configuration:
   ```bash
   copy running-config startup-config
   ```
6. You are now ready to configure the log sources in QRadar.

   Select Extreme XSR Security Routers from the Log Source Type list.

For more information about your Extreme XSR Security Router, see your vendor documentation.

**Related tasks**

“Adding a log source” on page 4

If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.
IBM QRadar accepts events from a range of F5 Networks DSMs.

F5 Networks BIG-IP AFM

The F5 Networks BIG-IP Advanced Firewall Manager (AFM) DSM for IBM QRadar accepts syslog events that are forwarded from F5 Networks BIG-IP AFM systems in name-value pair format.

About this task

QRadar can collect the following events from F5 BIG-IP appliances with Advanced Firewall Managers:

• Network events
• Network Denial of Service (DoS) events
• Protocol security events
• DNS events
• DNS Denial of Service (DoS) events

Before you can configure the Advanced Firewall Manager, you must verify that your BIG-IP appliance is licensed and provisioned to include Advanced Firewall Manager.

Procedure

1. Log in to your BIG-IP appliance Management Interface.
2. From the navigation menu, select System > License.
3. In the License Status column, verify that the Advanced Firewall Manager is licensed and enabled.
4. To enable the Advanced Firewall Manager, select System > Resource > Provisioning.
5. From the Provisioning column, select the check box and select Nominal from the list.
6. Click Submit to save your changes.

Configuring a logging pool

A logging pool is used to define a pool of servers that receive syslog events. The pool contains the IP address, port, and a node name that you provide.

Procedure

1. From the navigation menu, select Local Traffic > Pools.
2. Click Create.
3. In the Name field, type a name for the logging pool.
   For example, Logging_Pool.
4. From the Health Monitor field, in the Available list, select TCP and click <<.
   This clicking action moves the TCP option from the Available list to the Selected list.
5. In the Resource pane, from the Node Name list, select Logging_Node or the name you defined in “Configuring a logging pool” on page 451.
6. In the Address field, type the IP address for the QRadar Console or Event Collector.
7. In the Service Port field, type 514.
8. Click Add.
9. Click Finish.
Creating a high-speed log destination

The process to configure logging for BIG-IP AFM requires that you create a high-speed logging destination.

Procedure
1. From the navigation menu, select **System > Logs > Configuration > Log Destinations**.
2. Click **Create**.
3. In the **Name** field, type a name for the destination.
   For example, Logging_HSL_dest.
4. In the **Description** field, type a description.
5. From the **Type** list, select **Remote High-Speed Log**.
6. From the **Pool Name** list, select a logging pool from the list of remote log servers.
   For example, Logging_Pool.
7. From the **Protocol** list, select **TCP**.
8. Click **Finish**.

Creating a formatted log destination

The formatted log destination is used to specify any special formatting that is required on the events that are forwarded to the high-speed logging destination.

Procedure
1. From the navigation menu, select **System > Logs > Configuration > Log Destinations**.
2. Click **Create**.
3. In the **Name** field, type a name for the logging format destination.
   For example, Logging_Format_dest.
4. In the **Description** field, type a description.
5. From the **Type** list, select **Remote Syslog**.
6. From the **Syslog Format** list, select **Syslog**.
7. From the **High-Speed Log Destination** list, select your high-speed logging destination.
   For example, Logging_HSL_dest.
8. Click **Finish**.

Creating a log publisher

Creating a publisher allows the BIG-IP appliance to publish the formatted log message to the local syslog database.

Procedure
1. From the navigation menu, select **System > Logs > Configuration > Log Publishers**.
2. Click **Create**.
3. In the **Name** field, type a name for the publisher.
   For example, Logging_Pub.
4. In the **Description** field, type a description.
5. From the **Destinations** field, in the Available list, select the log destination name that you created in “Configuring a logging pool” on page 451 and click << to add items to the Selected list.
   This clicking action moves your logging format destination from the Available list to the Selected list.
   To include local logging in your publisher configuration, you can add **local-db** and **local-syslog** to the Selected list.
Creating a logging profile

Use the Logging profile to configure the types of events that your Advanced Firewall Manager is producing and to associate these events with the logging destination.

Procedure

1. From the navigation menu, select Security > Event Logs > Logging Profile.
2. Click Create.
3. In the Name field, type a name for the log profile.
   For example, Logging_Profile.
4. In the Network Firewall field, select the Enabled check box.
5. From the Publisher list, select the log publisher that you configured.
   For example, Logging_Pub.
6. In the Log Rule Matches field, select the Accept, Drop, and Reject check boxes.
7. In the Log IP Errors field, select the Enabled check box.
8. In the Log TCP Errors field, select the Enabled check box.
9. In the Log TCP Events field, select the Enabled check box.
10. In the Storage Format field, from the list, select Field-List.
11. In the Delimiter field, type , (comma) as the delimiter for events.
12. In the Storage Format field, select all of the options in the Available Items list and click <<.
   This clicking action moves all of the Field-List options from the Available list to the Selected list.
13. In the IP Intelligence pane, from the Publisher list, select the log publisher that you configured.
   For example, Logging_Pub.
14. Click Finished.

Associating the profile to a virtual server

The log profile you created must be associated with a virtual server in the Security Policy tab. This association allows the virtual server to process your network firewall events, along with local traffic.

About this task
Take the following steps to associate the profile to a virtual server.

Procedure

1. From the navigation menu, select Local Traffic > Virtual Servers.
2. Click the name of a virtual server to modify.
3. From the Security tab, select Policies.
4. From the Log Profile list, select Enabled.
5. From the Profile field, in the Available list, select Logging_Profile or the name you specified in “Creating a logging profile” on page 453 and click <<.
   This clicking action moves the Logging_Profile option from the Available list to the Selected list.
6. Click Update to save your changes.

The configuration is complete. The log source is added to IBM QRadar as F5 Networks BIG-IP AFM syslog events are automatically discovered. Events that are forwarded to QRadar by F5 Networks BIG-IP AFM are displayed on the Log Activity tab of QRadar.
Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from F5 Networks BIG-IP AFM. However, you can manually create a log source for QRadar to receive syslog events.

About this task

The following configuration steps are optional.

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 F5 Networks BIG-IP AFM.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 261. Syslog protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The configuration is complete.

F5 Networks BIG-IP APM

The F5 Networks BIG-IP Access Policy Manager (APM) DSM for IBM QRadar collects access and authentication security events from a BIG-IP APM device by using syslog.

To configure your BIG-IP LTM device to forward syslog events to a remote syslog source, choose your BIG-IP APM software version:

- “Configuring Remote Syslog for F5 BIG-IP APM V11.x to V14.x ” on page 454
- “Configuring a Remote Syslog for F5 BIG-IP APM 10.x ” on page 455

Configuring Remote Syslog for F5 BIG-IP APM V11.x to V14.x

You can configure syslog for F5 BIG-IP APM V11.x to V14.x.

About this task

To configure a remote syslog for F5 BIG-IP APM V11.x to V14.x take the following steps:

Procedure

1. Log in to the command-line of your F5 BIG-IP device.
2. Type the following command to add a single remote syslog server:

   \texttt{tmsh\ syslog\ remote\ server\ \{<Name>\\} \{host <IP address>\}}
Where:
- `<Name>` is the name of the F5 BIG-IP APM syslog source.
- `<IP address>` is the IP address of the QRadar Console.

For example,
```
bigpipe syslog remote server {BIGIP_APM {host 192.0.2.1}}
```

3. Type the following to save the configuration changes:
```
tmsh save sys config partitions all
```

The configuration is complete. The log source is added to QRadar as F5 Networks BIG-IP APM events are automatically discovered. Events that are forwarded to QRadar by F5 Networks BIG-IP APM are displayed on the Log Activity tab in QRadar.

### Configuring a Remote Syslog for F5 BIG-IP APM 10.x

You can configure syslog for F5 BIG-IP APM 10.x

#### About this task

To configure a remote syslog for F5 BIG-IP APM 10.x take the following steps:

**Procedure**

1. Log in to the command-line of your F5 BIG-IP device.
2. Type the following command to add a single remote syslog server:
   ```
   bigpipe syslog remote server {
   `<Name>` {host `<IP address>`}}
   ```
   Where:
   - `<Name>` is the name of the F5 BIG-IP APM syslog source.
   - `<IP address>` is the IP address of QRadar Console.
   For example,
   ```
   bigpipe syslog remote server {BIGIP_APM {host 192.0.2.1}}
   ```
3. Type the following to save the configuration changes:
   ```
   bigpipe save
   ```

   The configuration is complete. The log source is added to IBM QRadar as F5 Networks BIG-IP APM events are automatically discovered. Events that are forwarded to QRadar by F5 Networks BIG-IP APM are displayed on the Log Activity tab.

### Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from F5 Networks BIG-IP APM appliances.

#### About this task

These configuration steps are optional.

**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 F5 Networks BIG-IP APM.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your F5 Networks BIG-IP APM appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.

**Configuring F5 Networks BIG-IP ASM**

The IBM QRadar F5 Networks BIG-IP Application Security Manager (ASM) DSM collects web application security events from BIG-IP ASM appliances by using syslog.

**About this task**

To forward syslog events from an F5 Networks BIG-IP ASM appliance to QRadar, you must configure a logging profile.

A logging profile can be used to configure remote storage for syslog events, which can be forwarded directly to QRadar.

**Procedure**

1. Log in to the F5 Networks BIG-IP ASM appliance user interface.
2. In the navigation pane, select Application Security > Options.
3. Click Logging Profiles.
4. Click Create.
5. From the Configuration list, select Advanced.
6. Type a descriptive name for the Profile Name property.
7. Optional: Type a Profile Description.
   If you do not want data logged both locally and remotely, clear the Local Storage check box.
8. Select the Remote Storage check box.
9. From the Type list, select 1 of the following options:
   a) In BIG-IP ASM V12.1.2 or earlier, select Reporting Server.
   b) In BIG-IP ASM V13.0.0 or later, select key-value pairs.
10. From the Protocol list, select TCP.
11. In the IP Address field, type the IP address of the QRadar Console and in the Port field, type a port value of 514.
12. Select the Guarantee Logging check box.
   **Note:** Enabling the Guarantee Logging option ensures the system log requests continue for the web application when the logging utility is competing for system resources. Enabling the Guarantee Logging option can slow access to the associated web application.
13. Select the Report Detected Anomalies check box to allow the system to log details.
14. Click **Create**.
   The display refreshes with the new logging profile. The log source is added to QRadar as F5 Networks BIG-IP ASM events are automatically discovered. Events that are forwarded by F5 Networks BIG-IP ASM are displayed on the Log Activity tab of QRadar.

**Configuring a log source**
IBM QRadar automatically discovers and creates a log source for syslog events from F5 Networks BIG-IP ASM appliances.

**About this task**
These configuration steps are optional.

**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 **F5 Networks BIG-IP ASM**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

```markdown
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your F5 Networks BIG-IP ASM appliance.</td>
</tr>
</tbody>
</table>
```

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
   The configuration is complete.

**F5 Networks BIG-IP LTM**
The F5 Networks BIG-IP Local Traffic Manager (LTM) DSM for IBM QRadar collects networks security events from a BIG-IP device by using syslog.

Before events can be received in QRadar, you must configure a log source for QRadar, then configure your BIG-IP LTM device to forward syslog events. Create the log source before events are forwarded as QRadar does not automatically discover or create log sources for syslog events from F5 BIG-IP LTM appliances.

**Configuring a log source**
To integrate F5 BIG-IP LTM with IBM QRadar, you must manually create a log source to receive syslog 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. 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 **F5 Networks BIG-IP LTM**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type the IP address or host name for the log source as an identifier for events from your BIG-IP LTM appliance.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

You are now ready to configure your BIG-IP LTM appliance to forward syslog events to QRadar.

### Configuring syslog forwarding in BIG-IP LTM

You can configure your BIG-IP LTM device to forward syslog events.

You can configure syslog for the following BIG-IP LTM software version:

- “Configuring Remote Syslog for F5 BIG-IP LTM V11.x to V14.x” on page 458
- “Configuring Remote Syslog for F5 BIG-IP LTM V10.x” on page 459
- “Configuring Remote Syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8” on page 459

### Configuring Remote Syslog for F5 BIG-IP LTM V11.x to V14.x

You can configure syslog for F5 BIG-IP LTM 11.x to V14.x.

#### About this task

To configure syslog for F5 BIG-IP LTM V11.x to V14.x take the following steps:

#### Procedure

1. Log in to the command-line of your F5 BIG-IP device.
2. To log in to the Traffic Management Shell (tmsh), type the following command:
   
   tmsh

3. To add a syslog server, type the following command:

   ```bash
   modify /sys syslog remote-servers add {<Name> {host <IP address> remote-port 514}}
   ```

   Where:

   - `<Name>` is a name that you assign to identify the syslog server on your BIG-IP LTM appliance.
   - `<IP address>` is the IP address of IBM QRadar.

   For example,

   ```bash
   modify /sys syslog remote-servers add {BIGIPsyslog {host 192.0.2.1 remote-port 514}}
   ```

4. Save the configuration changes:
Configuring Remote Syslog for F5 BIG-IP LTM V10.x

You can configure syslog for F5 BIG-IP LTM V10.x.

About this task
To configure syslog for F5 BIG-IP LTM V10.x take the following steps:

Procedure
1. Log in to the command line of your F5 BIG-IP device.
2. Type the following command to add a single remote syslog server:
   ```
   bigpipe syslog remote server {<Name> {host <IP_address>}}
   ```
   Where:
   - `<Name>` is the name of the F5 BIG-IP LTM syslog source.
   - `<IP_address>` is the IP address of IBM QRadar.
   For example:
   ```
   bigpipe syslog remote server {BIGIPsyslog {host 192.0.2.1}}
   ```
3. Save the configuration changes:
   ```
   bigpipe save
   ```
   **Note:** F5 Networks modified the syslog output format in BIG-IP V10.x to include the use of `local/` before the host name in the syslog header. The syslog header format that contains `local/` is not supported in QRadar, but a workaround is available to correct the syslog header. For more information, see [http://www.ibm.com/support](http://www.ibm.com/support).

Events that are forwarded from your F5 Networks BIG-IP LTM appliance are displayed on the Log Activity tab in QRadar.

Configuring Remote Syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8

You can configure syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8.

About this task
To configure syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8 take the following steps:

Procedure
1. Log in to the command-line of your F5 BIG-IP device.
2. Type the following command to add a single remote syslog server:
   ```
   bigpipe syslog remote server <IP address>
   ```
   Where: `<IP address>` is the IP address of IBM QRadar.
   For example:
   ```
   bigpipe syslog remote server 192.0.2.1
   ```
3. Type the following to save the configuration changes:
   ```
   bigpipe save
   ```
   The configuration is complete. Events that are forwarded from your F5 Networks BIG-IP LTM appliance are displayed on the Log Activity tab in QRadar.
**F5 Networks FirePass**

The F5 Networks FirePass DSM for IBM QRadar collects system events from an F5 FirePass SSL VPN device using syslog.

By default, remote logging is disabled and must be enabled in the F5 Networks FirePass device. Before receiving events in QRadar, you must configure your F5 Networks FirePass device to forward system events to QRadar as a remote syslog server.

### Configuring syslog forwarding for F5 FirePass

To forward syslog events from an F5 Networks BIG-IP FirePass SSL VPN appliance to IBM QRadar, you must enable and configure a remote log server.

#### About this task

The remote log server can forward events directly to your QRadar Console or any Event Collector in your deployment.

#### Procedure

1. Log in to the F5 Networks FirePass Admin Console.
2. On the navigation pane, select **Device Management > Maintenance > Logs**.
3. From the **System Logs** menu, select the **Enable Remote Log Server** check box.
4. From the **System Logs** menu, clear the **Enable Extended System Logs** check box.
5. In the **Remote host** parameter, type the IP address or host name of your QRadar.
6. From the **Log Level** list, select **Information**.

   - The **Log Level** parameter monitors application level system messages.
7. From the **Kernel Log Level** list, select **Information**.

   - The **Kernel Log Level** parameter monitors Linux kernel system messages.
8. Click **Apply System Log Changes**.

   - The changes are applied and the configuration is complete. The log source is added to QRadar as F5 Networks FirePass events are automatically discovered. Events that are forwarded to QRadar by F5 Networks BIG-IP ASM are displayed on the **Log Activity** tab in QRadar.

### Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from F5 Networks FirePass appliances.

#### About this task

The following configuration steps are optional:

#### 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 **F5 Networks FirePass**.

10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for</td>
</tr>
<tr>
<td></td>
<td>events from your F5 Networks FirePass appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.

12. On the Admin tab, click Deploy Changes.
Chapter 61. Fair Warning

The Fair Warning DSM for IBM QRadar retrieves event files from a remote source by using the log file protocol.

QRadar records event categories from the Fair Warning log files about user activity that is related to patient privacy and security threats to medical records. Before you can retrieve log files from Fair Warning, you must verify that your device is configured to generate an event log. Instructions for generating the event log can be found in your Fair Warning documentation.

When you configure the log file protocol, make sure that the host name or IP address that is configured in the Fair Warning system is the same as configured in the Remote Host parameter in the log file protocol configuration.

Configuring a log source

You can configure IBM QRadar to download an event log from a Fair Warning device.

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 box, select Fair Warning.
9. Select the Log File option from the Protocol Configuration list.
10. In the FTP File Pattern field, type a regular expression that matches the log files that are generated by the Fair Warning system.
11. In the Remote Directory field, type the path to the directory that contains logs from your Fair Warning device.
12. From the Event Generator list, select Fair Warning.
13. Click Save.

The configuration is complete. For more information on full parameters for the log file protocol, see the IBM QRadar Managing Log Sources Guide.

For more information on configuring Fair Warning, consult your vendor documentation.

Related tasks

“Adding a log source” on page 4

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 62. Fasoo Enterprise DRM

The IBM QRadar DSM for Fasoo Enterprise DRM (Digital Rights Management) collects logs from a Fasoo Enterprise DRM device.

The following table describes the specifications for the Fasoo Enterprise DRM DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Fasoo</td>
</tr>
<tr>
<td>DSM name</td>
<td>Fasoo Enterprise DRM</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-FasooFED-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>5.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>JDBC</td>
</tr>
<tr>
<td>Event format</td>
<td>name-value pair (NVP)</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Usage events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Fasoo website (<a href="http://en.fasoo.com/Fasoo-Enterprise-DRM">http://en.fasoo.com/Fasoo-Enterprise-DRM</a>)</td>
</tr>
</tbody>
</table>

To integrate Fasoo Enterprise DRM 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:
   - JDBC Protocol RPM
   - DSMCommon RPM
   - FasooFED DSM RPM

2. Configure a log source to connect to the Fasoo Enterprise DRM database and retrieve event.

3. Add a Fasoo Enterprise DRM log source on the QRadar Console. The following table describes the parameters that require specific values to collect event from Fasoo Enterprise DRM:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Fasoo Enterprise DRM</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
</tbody>
</table>
### Table 266. Fasoo Enterprise DRM JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn’t collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td><strong>Database Type</strong></td>
<td>From the list, select the type of the Fasoo Enterprise DRM database.</td>
</tr>
<tr>
<td><strong>Database Name</strong></td>
<td>The name of the Fasoo Enterprise DRM database.</td>
</tr>
<tr>
<td><strong>IP or Hostname</strong></td>
<td>The IP address or host name of the Fasoo Enterprise DRM database server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port number that is used by the database server.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>The user name that is required to connect to the database.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password that is required to connect to the database. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>The confirmation password must be identical to the password that you typed for the Password parameter.</td>
</tr>
<tr>
<td><strong>Authentication Domain</strong></td>
<td>If you did not select Use Microsoft JDBC, Authentication Domain is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td><strong>Database Instance</strong></td>
<td>The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the Database Instance parameter must be blank in the log source configuration.</td>
</tr>
<tr>
<td><strong>Predefined Query (Optional)</strong></td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the none option.</td>
</tr>
<tr>
<td><strong>Table Name</strong></td>
<td>view_fut_log The name of the view that includes the event records.</td>
</tr>
</tbody>
</table>
Table 266. Fasoo Enterprise DRM JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select List</strong></td>
<td>Type an asterisk (*) to select all fields from the table or view. The list of fields to include when the table is polled for events.</td>
</tr>
<tr>
<td><strong>Compare Field</strong></td>
<td>log_date</td>
</tr>
<tr>
<td></td>
<td>The <strong>Compare Field</strong> is used to identify new events that are added between queries to the table.</td>
</tr>
<tr>
<td><strong>Start Date and Time</strong> (Optional)</td>
<td>Type the start date and time for database polling in the following format: 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.</td>
</tr>
<tr>
<td><strong>Use Prepared Statements</strong></td>
<td>Select the check box if you want to use prepared statements. Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td><strong>Use Named Pipe Communication</strong></td>
<td>If you did not select <strong>Use Microsoft JDBC, Use Named Pipe Communication</strong> is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
<tr>
<td><strong>Database Cluster Name</strong></td>
<td>If you selected <strong>Use Named Pipe Communication</strong>, the <strong>Database</strong> parameter displays. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.</td>
</tr>
</tbody>
</table>
Table 266. Fasoo Enterprise DRM JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select <strong>Use Microsoft JDBC</strong>, <strong>Use NTLMv2</strong> is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable <strong>Use Microsoft JDBC</strong>.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option if your connection supports SSL.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected <strong>Use Microsoft JDBC</strong> and <strong>Use SSL</strong>, the <strong>Microsoft SQL Server Hostname</strong> parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC parameters, see [c_logsource_JDBCprotocol.dita](#).

4. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Fasoo Enterprise DRM:
Table 267. Fasoo Enterprise DRM sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit - successful</td>
<td>Update Activity Succeeded</td>
<td>log_id: &quot;xxxxxxxxxxxxxxxxxxxxxxxxxxxxx&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>log_date: &quot;2016-03-21 14:17:36.000&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>log_type: &quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>product: &quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>purpose: &quot;16&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>license_status: &quot;0&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ip: &quot;&lt;Numeric&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user_code: &quot;usercode&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user_name: &quot;username&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user_dept_code: &quot;xxxxxxxxxxxxxxxxxxxxxx&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user_dept_name: &quot;userdeptname&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>position_code: &quot;P001&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>position_name: &quot;Employee&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>content_code: &quot;xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>content_name: &quot;New Microsoft PowerPoint Presentation.pptx&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>content_create_date: &quot;2016-03-21 03:41:28.000&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>entry_date: &quot;2016-03-21 13:18:26.670&quot;</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 Fasoo Enterprise DRM to communicate with QRadar

For IBM QRadar to collect log event data, you must create a database view.

Before you begin

The script in this procedure is only intended for MS SQL Servers. For other database types, modifications to the script will be required for the target database type.

Procedure

1. Log in to SQL Server Management Studio.
2. Create a custom view in your Fasoo database.

```
USE fed5;
GO
CREATE VIEW view_fut_log
AS
SELECT
dbo.fut_log.log_id,
```

Chapter 62. Fasoo Enterprise DRM 469
dbo.fut_log.log_date,
dbo.fut_log.log_type,
dbo.fut_log.product,
dbo.fut_log.purpose,
dbo.fut_log.usage_result,
dbo.fut_log.license_status,
dbo.fut_log.ip,
dbo.fut_user.user_code,
dbo.fut_user.user_name,
dbo.fut_user.user_dept_code,
dbo.fut_user.user_dept_name,
dbo.fut_log.position_code,
dbo.fut_log.position_name,
dbo.fut_content.content_code,
dbo.fut_content.current_content_name,
dbo.fut_content.content_name,
dbo.fut_content.sec_level_code,
dbo.fut_content.sec_level_name,
dbo.fut_content.system_code,
dbo.fut_content.system_name,
dbo.fut_log.owner_code,
dbo.fut_log.owner_name,
dbo.fut_log.owner_dept_code,
dbo.fut_log.owner_dept_name,
dbo.fut_log.owner_dept_code,
dbo.fut_log.entry_date
FROM dbo.fut_log
INNER JOIN dbo.fut_user
ON dbo.fut_log.user_id =
dbo.fut_user.user_id
INNER JOIN dbo.fut_content
ON dbo.fut_log.content_id =
dbo.fut_content.content_id
GO
Chapter 63. Fidelis XPS

The Fidelis XPS DSM for IBM QRadar accepts events that are forwarded in Log Enhanced Event Protocol (LEEF) from Fidelis XPS appliances by using syslog.

QRadar can collect all relevant alerts that are triggered by policy and rule violations that are configured on your Fidelis XPS appliance.

Event type format

Fidelis XPS must be configured to generate events in Log Enhanced Event Protocol (LEEF) and forward these events by using syslog. The LEEF format consists of a pipe ( | ) delimited syslog header, and tab separated fields that are positioned in the event payload.

If the syslog events forwarded from your Fidelis XPS are not formatted in LEEF format, you must examine your device configuration or software version to ensure that your appliance supports LEEF. Properly formatted LEEF event messages are automatically discovered and added as a log source to QRadar.

Configuring Fidelis XPS

You can configure syslog forwarding of alerts from your Fidelis XPS appliance.

Procedure

1. Log in to CommandPost to manage your Fidelis XPS appliance.
2. From the navigation menu, select System > Export.

   A list of available exports is displayed. The list is empty the first time you use the export function.
3. Select one of the following options:
   - Click New to create a new export for your Fidelis XPS appliance.
   - Click Edit next to an export name to edit an existing export on your Fidelis XPS appliance.

   The Export Editor is displayed.

4. From the Export Method list, select Syslog LEEF.
5. In the Destination field, type the IP address or host name for IBM QRadar.

   For example, 192.0.2.1:::514

   The Destination field does not support non-ASCII characters.
6. From Export Alerts, select one of the following options:
   - All alerts - Select this option to export all alerts to QRadar. This option is resource-intensive and it can take time to export all alerts.
   - Alerts by Criteria - Select this option to export specific alerts to QRadar. This option displays a new field where you can define your alert criteria.

7. From Export Malware Events, select None.
8. From Export Frequency, select Every Alert / Malware.
9. In the Save As field, type a name for your export.
10. Click Save.
11. Optional: To verify that events are forwarded to QRadar, you can click Run Now.

   Run Now is intended as a test tool to verify that alerts selected by criteria are exported from your Fidelis appliance. This option is not available if you selected to export all events in “Configuring Fidelis XPS” on page 471.
The configuration is complete. The log source is added to QRadar as Fidelis XPS syslog events are automatically discovered. Events that are forwarded to QRadar by Fidelis XPS are displayed on the Log Activity tab of QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Fidelis XPS. However, you can manually create a log source for QRadar to receive syslog events.

About this task

The following configuration steps are optional:

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 Fidelis XPS.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 268. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The configuration is complete.
The IBM QRadar DSM for 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>FireEye</td>
</tr>
<tr>
<td>DSM name</td>
<td>FireEye MPS</td>
</tr>
<tr>
<td>Supported versions</td>
<td>CMS, MPS, EX, AX, NX, FX, and HX</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-FireEyeMPS-QRadar_version-Build_number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog and TLS Syslog</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>All relevant events</td>
</tr>
<tr>
<td>Auto discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>FireEye website (<a href="http://www.fireeye.com">www.fireeye.com</a>)</td>
</tr>
</tbody>
</table>

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. Download and install the latest TLS Syslog Protocol RPM on QRadar.
3. For each instance of FireEye in your deployment, configure the FireEye system to forward events to QRadar.
4. For each instance of FireEye, create an FireEye log source on the QRadar Console. The following tables explain how to configure a log source in Syslog and TLS Syslog for FireEye.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>FireEye</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>FireEye</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>TLS Syslog</td>
</tr>
</tbody>
</table>
### Table 271. Configuring the TLS Syslog log source protocols for FireEye (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type the IP address or host name for the log source as an identifier for events from your device.</td>
</tr>
<tr>
<td><strong>TLS Listen Port</strong></td>
<td>The default TLS listen port is 6514.</td>
</tr>
<tr>
<td><strong>Authentication Mode</strong></td>
<td>The mode by which your TLS connection is authenticated. If you select the TLS and Client Authentication option, you must configure the certificate parameters.</td>
</tr>
<tr>
<td><strong>Certificate Type</strong></td>
<td>The type of certificate to use for authentication. If you select the <strong>Provide Certificate</strong> option, you must configure the file paths for the server certificate and the private key.</td>
</tr>
<tr>
<td><strong>Provided Server Certificate Path</strong></td>
<td>The absolute path to the server certificate.</td>
</tr>
<tr>
<td><strong>Provided Private Key Path</strong></td>
<td>The absolute path to the private key.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The corresponding private key must be a DER-encoded PKCS8 key. The configuration fails with any other key format.</td>
</tr>
<tr>
<td><strong>Maximum Connections</strong></td>
<td>The Maximum Connections parameter controls how many simultaneous connections the TLS Syslog protocol can accept for each Event Collector. The connection limit across all TLS syslog log source configurations is 1000 connections for each Event Collector. The default for each device connection is 50.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Automatically discovered log sources that share a listener with another log source, such as if you use the same port on the same event collector, count only one time towards the limit.</td>
</tr>
</tbody>
</table>

Look at “Adding a log source” on page 4 for more common parameters that occur in Syslog and “TLS syslog protocol configuration options” on page 93 for more TLS Syslog protocol-specific parameters and their configurations.

**Related tasks**

- “Configuring your FireEye HX system for communication with QRadar” on page 475
- “Configuring your FireEye system for communication with QRadar” on page 475
- “Adding a DSM” on page 4
- “Adding a log source” on page 4
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 IBM QRadar, configure your FireEye appliance to forward syslog events.

**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
   ```

**Related tasks**

“Configuring your FireEye HX system for communication with QRadar” on page 475

To enable FireEye HX to communicate with IBM QRadar, configure your FireEye HX appliance to forward syslog events.

**Configuring your FireEye HX system for communication with QRadar**

To enable FireEye HX to communicate with IBM QRadar, configure your FireEye HX appliance to forward syslog events.

**Procedure**

1. Log in to the FireEye HX appliance by using the CLI.
2. To activate configuration mode, type the following commands:
   
   ```
   enable
   configure terminal
   ```
3. To add a remote syslog server destination, type the following commands:
   
   ```
   logging <remote_IP_address> trap none
   ```
   ```
   logging <remote_IP_address> trap override class cef priority info
   ```
4. To save the configuration changes to the FireEye HX appliance, type the following command:
   
   ```
   write mem
   ```
Chapter 65. Forcepoint

IBM QRadar supports a range of Forcepoint DSMs.

FORCEPOINT is formerly known as Websense.

Related concepts
Websense
QRadar supports a range of Websense DSMs.

FORCEPOINT Stonesoft Management Center

The IBM QRadar DSM for FORCEPOINT Stonesoft Management Center collects events from a StoneGate device by using syslog.

The following table describes the specifications for the Stonesoft Management Center DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>FORCEPOINT</td>
</tr>
<tr>
<td>DSM name</td>
<td>Stonesoft Management Center</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-StonesoftManagementCenter-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>5.4 to 6.1</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Management Center, IPS, Firewall, and VPN events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>FORCEPOINT website (<a href="https://www.forcepoint.com">https://www.forcepoint.com</a>)</td>
</tr>
</tbody>
</table>

To integrate FORCEPOINT Stonesoft Management Center 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:
   a. DSMCommon RPM
   b. Stonesoft Management Center DSM RPM
2. Configure your StoneGate device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Stonesoft Management Center log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from Stonesoft Management Center:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Stonesoft Management Center</td>
</tr>
</tbody>
</table>
4. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Stonesoft Management Center:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic_UDP-Rugged-Director-Denial-Of-Service</td>
<td>Misc DoS</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 FORCEPOINT Stonesoft Management Center to communicate with QRadar**

Configure Stonesoft Management Center to communicate with QRadar by editing the LogServerConfiguration.txt file. Configuring the text file allows Stonesoft Management Center to forward events in LEEF format by using syslog to QRadar.

**Procedure**

1. Log in to the appliance that hosts your Stonesoft Management Center.
2. Stop the Stonesoft Management Center Log Server.
3. In Windows, select one of the following methods to stop the Log Server.
   - Stop the Log Server in the Windows **Services** list.
   - Run the batch file `<installation path>/bin/sgStopLogSrv.bat`.

   In Linux - To stop the Log Server in Linux, run the script `<installation path>/bin/sgStopLogSrv.sh`

4. Edit the LogServerConfiguration.txt file. The configuration file is located in the following directory:

   `<installation path>/data/LogServerConfiguration.txt`

5. Configure the following parameters in the LogServerConfiguration.txt file:
Table 275. Log server configuration options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSLOG_EXPORT_FORMAT</td>
<td>LEEF</td>
<td>Type LEEF as the export format to use for syslog.</td>
</tr>
</tbody>
</table>
| SYSLOG_EXPORT_ALERT | YES | Type one of the following values:  
• Yes - Exports alert entries to QRadar by using the syslog protocol.  
• No - Alert entries are not exported.                                      |
| SYSLOG_EXPORT_FW | YES | Type one of the following values:  
• Yes - Exports firewall and VPN entries to QRadar by using the syslog protocol.  
• No - Firewall and VPN entries are not exported.                             |
| SYSLOG_EXPORT_IPS | YES | Type one of the following values:  
• Yes - Exports IPS logs to QRadar by using the syslog protocol.  
• No - IPS logs are not exported.                                              |
| SYSLOG_PORT | 514         | Type 514 as the UDP port for forwarding syslog events to QRadar.                                                                            |
| SYSLOG_SERVER_ADDRESS | QRadar IPv4 Address | Type the IPv4 address of your QRadar Console or Event Collector.                                                                               |

7. Start the Log Server.
   - Windows - Type `<installation path>/bin/sgStartLogSrv.bat`.
   - Linux - Type `<installation path>/bin/sgStartLogSrv.sh`.

For detailed configuration instructions, see the StoneGate Management Center Administrator's Guide.

What to do next

You are now ready to configure a traffic rule for syslog.

Note: A firewall rule is only required if your QRadar Console or Event Collector is separated by a firewall from the Stonesoft Management Server. If no firewall exists between the Stonesoft Management Server and QRadar, you need to configure the log source in QRadar.

Configuring a syslog traffic rule for FORCEPOINT Stonesoft Management Center

If your Stonesoft Management Center and QRadar are separated by a firewall in your network, you must modify your firewall or IPS policy to allow traffic between the Stonesoft Management Center and QRadar.

Procedure

1. From the Stonesoft Management Center, select one of the following methods for modifying a traffic rule.
   - Firewall policies - Select Configuration > Configuration > Firewall.
   - IPS policies - Select Configuration > Configuration > IPS.
2. Select the type of policy to modify.
   - **Firewall** - Select **Firewall Policies > Edit Firewall Policy**.
   - **IPS** - Select **IPS Policies > Edit Firewall Policy**.
3. Add an IPv4 Access rule by configuring the following parameters for the firewall policy:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Type the IPv4 address of your Stonesoft Management Center Log server.</td>
</tr>
<tr>
<td>Destination</td>
<td>Type the IPv4 address of your QRadar Console or Event Collector.</td>
</tr>
<tr>
<td>Service</td>
<td>Select <strong>Syslog (UDP)</strong>.</td>
</tr>
<tr>
<td>Action</td>
<td>Select <strong>Allow</strong>.</td>
</tr>
<tr>
<td>Logging</td>
<td>Select <strong>None</strong>.</td>
</tr>
</tbody>
</table>

   **Note:** In most cases, you might want to set the logging value to **None**. Logging syslog connections without configuring a syslog filter can create a loop. For more information, see the *StoneGate Management Center Administrator's Guide*.

4. Save your changes and then refresh the policy on the firewall or IPS.

**What to do next**
You are now ready to configure the log source in QRadar.

---

**Forcepoint Sidewinder**

Forcepoint Sidewinder is formerly known as McAfee Firewall Enterprise. The IBM QRadar DSM for Forcepoint Sidewinder collects logs from a Forcepoint Sidewinder Firewall Enterprise device by using the Syslog protocol.

To integrate Forcepoint Sidewinder with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the Forcepoint Sidewinder DSM RPM on your QRadar Console.
2. Configure Forcepoint Sidewinder to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add a Forcepoint Sidewinder log source on the QRadar Console. The following table describes the parameters that require specific values for Forcepoint Sidewinder event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Forcepoint Sidewinder</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Related concepts**

“Configure Forcepoint Sidewinder to communicate with QRadar” on page 481

Before you can configure QRadar to integrate with Forcepoint Sidewinder, you must configure syslog on your Forcepoint Sidewinder Firewall Enterprise device.

**Related tasks**

“Adding a log source” on page 4
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 DSM” on page 4

**Forcepoint Sidewinder DSM specifications**

The following table describes the specifications for the Forcepoint Sidewinder DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Forcepoint</td>
</tr>
<tr>
<td>DSM name</td>
<td>Forcepoint Sidewinder</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-ForcepointSidewinder-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V6.1</td>
</tr>
<tr>
<td>Event format</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Forcepoint Sidewinder audit events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Forcepoint website (<a href="https://www.forcepoint.com">https://www.forcepoint.com</a>)</td>
</tr>
</tbody>
</table>

**Configure Forcepoint Sidewinder to communicate with QRadar**

Before you can configure QRadar to integrate with Forcepoint Sidewinder, you must configure syslog on your Forcepoint Sidewinder Firewall Enterprise device.

When you configure your Forcepoint Sidewinder device to forward syslog events to QRadar, export the logs in Sidewinder Export Format (SEF).

For more information about configuring your Forcepoint Sidewinder device, see the *Forcepoint Sidewinder Administration Guide* (https://www.websense.com/content/support/library/si/v70/mgmt/si_70103_ag_a_en-us.pdf).

**Related tasks**

“Adding a log source” on page 4

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

**Sample event messages**

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when you use the Syslog protocol for the Forcepoint Sidewinder DSM:
Table 278. Forcepoint Sidewinder sample message supported by Forcepoint Sidewinder.

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>nettraffic@status_conn_close</td>
<td>Firewall Session Closed</td>
<td><code>&lt;131&gt;May 16 11:41:11 auditd: date= &quot;May 16 15:41:11 2006 GMT&quot;, fac=f_fftpproxy, area=a_server,type=t_nettraffic,pri=p_major, pid=2718,ruid=0,euid=0,pgid=2718,logid=0,cmd=pftp,domain=PFTx,edomain=PFTx,srcip=192.168.0.1,srcport=4597,srcburb=Internal,dstip=192.168.0.2,dstport=21,dstburb=external,protocol=6,bytes_written_to_client=0,bytes_written_to_server=0,service_name=pftp,reason=&quot;closing connection&quot;,status=conn_close,ACL_id=default-outgoingrule,cache_hit=0,remote_logname=anonymous,request_command=QUIT,request_status=1,start_time=&quot;Tue May 16 11:41:06 2006&quot;,netsessid=4469f2920002870e0002870e</code></td>
</tr>
</tbody>
</table>

**Forcepoint TRITON**


**About this task**

Forcepoint TRITON collects and streams event information to QRadar by using the Forcepoint Multiplexer component. Before you configure QRadar, you must configure the Forcepoint TRITON solution to provide LEEF formatted syslog events.

Before you can configure Forcepoint TRITON Web Security solutions to forward events to QRadar, you must ensure that your deployment contains a Forcepoint Multiplexer.

The Forcepoint Multiplexer is supported on Windows, Linux, and on Forcepoint V-Series appliances.

To configure a Forcepoint Multiplexer on a Forcepoint Triton or V-Series appliance:

**Procedure**

1. Install an instance of Forcepoint Multiplexer for each Forcepoint Policy Server component in your network.
   - For Microsoft Windows - To install the Forcepoint Multiplexer on Windows, use the TRITON Unified Installer. The Triton Unified Installer is available for download at [http://www.myforcepoint.com](http://www.myforcepoint.com).
   - For Linux - To install the Forcepoint Multiplexer on Linux, use the Web Security Linux Installer. The Web Security Linux Installer is available for download at [http://www.myforcepoint.com](http://www.myforcepoint.com).
   For information on adding a Forcepoint Multiplexer to software installations, see your Forcepoint Security Information Event Management (SIEM) Solutions documentation.

2. Enable the Forcepoint Multiplexer on a V-Series appliance that is configured as a full policy source or user directory and filtering appliance:
   a) Log in to your Forcepoint TRITON Web Security Console or V-Series appliance.

3. From the Appliance Manager, select Administration > Toolbox > Command Line Utility.
4. Click the Forcepoint Web Security tab.
5. From the Command list, select multiplexer, then use the enable command.
6. Repeat “Forcepoint TRITON” on page 482 and “Forcepoint TRITON” on page 482 to enable one Multiplexer instance for each Policy Server instance in your network.
If more than one Multiplexer is installed for a Policy Server, only the last installed instance of the Forcepoint Multiplexer is used. The configuration for each Forcepoint Multiplexer instance is stored by its Policy Server.

**What to do next**
You can now configure your Forcepoint TRITON appliance to forward syslog events in LEEF format to QRadar.

### Configuring syslog for Forcepoint TRITON
To collect events, you must configure syslog forwarding for Forcepoint TRITON.

#### Procedure
1. Log in to your Forcepoint TRITON Web Security Console.
2. On the **Settings** tab, select **General > SIEM Integration**.
3. Select the **Enable SIEM integration for this Policy Server** check box.
4. In the **IP address or hostname** field, type the IP address of your QRadar.
5. In the **Port** field, type 514.
6. From the **Transport protocol** list, select either the **TCP** or **UDP** protocol option.
   - QRadar supports syslog events for TCP and UDP protocols on port 514.
7. From the **SIEM format** list, select **syslog/LEEF (QRadar)**
8. Click **OK** to cache any changes.
9. Click **Deploy** to update your Forcepoint TRITON security components or V-Series appliances.
   - The Forcepoint Multiplexer connects to Forcepoint Filtering Service and ensures that event log information is provided to QRadar.

### Configuring a log source for Forcepoint TRITON
IBM QRadar automatically discovers and creates a log source for syslog events in LEEF format from Forcepoint TRITON and V-Series appliances.

#### About this task
The configuration steps for creating a log source are optional.

#### 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 **Forcepoint V Series**.
   - **Note**: Forcepoint TRITON uses the Forcepoint V Series Content Gateway DSM for parsing events. When you manually add a log source to QRadar for Forcepoint TRITON, you should select **Forcepoint V Series**.
9. From the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:
Table 279. Syslog parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for</td>
</tr>
<tr>
<td></td>
<td>events from Forcepoint TRITON or V-Series appliance.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The log source is added to QRadar.

### Forcepoint V-Series Data Security Suite


#### Configuring syslog for Forcepoint V-Series Data Security Suite

The Forcepoint V-Series Data Security Suite DSM accepts events using syslog. Before you can integrate IBM QRadar you, must enable the Forcepoint V-Series appliance to forward syslog events in the Data Security Suite (DSS) Management Console.

**Procedure**

1. Select **Policies > Policy Components > Notification Templates**.
2. Select an existing Notification Template or create a new template.
3. Click the **General** tab.
4. Click **Send Syslog Message**.
5. Select **Options > Settings > Syslog** to access the Syslog window.

The syslog window enables administrators to define the IP address/host name and port number of the syslog in their organization. The defined syslog receives incident messages from the Forcepoint Data Security Suite DSS Manager.

6. The syslog is composed of the following fields:

   DSS Incident|ID={value}|action={display value - max}|urgency= {coded}|
policy categories={values,,,}|source={value-display name}|
destinations={values...}|channel={display name}|
matches= {value}|details={value}

   - Max length for policy categories is 200 characters.
   - Max length for destinations is 200 characters.
   - Details and source are reduced to 30 characters.

7. Click **Test Connection** to verify that your syslog is accessible.

**What to do next**

You can now configure the log source in QRadar. The configuration is complete. The log source is added to QRadar as OSSEC events are automatically discovered. Events that are forwarded to QRadar by OSSEC are displayed on the **Log Activity** tab of QRadar.
Configuring a log source for Forcepoint V-Series Data Security Suite

IBM QRadar automatically discovers and creates a log source for syslog events from Forcepoint V-Series Data Security Suite.

About this task
The following configuration steps are optional.

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 Forcepoint V Series.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Forcepoint V-Series Data Security Suite DSM</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The configuration is complete.

Forcepoint V-Series Content Gateway

The Forcepoint V-Series Content Gateway DSM for IBM QRadar supports events for web content on Forcepoint V-Series appliances with the Content Gateway software.

The Forcepoint V-Series Content Gateway DSM accepts events using syslog to stream events or by using the log file protocol to provide events to QRadar. Before you can integrate your appliance with QRadar, you must select one of the following configuration methods:

- To configure syslog for your Forcepoint V-Series, see Configure Syslog for Forcepoint V-Series Data Security Suite.
- To configure the log file protocol for your Forcepoint V-Series, see Log file protocol for Forcepoint V-Series Content Gateway.

Configure syslog for Forcepoint V-Series Content Gateway

The Forcepoint V-Series DSM supports Forcepoint V-Series appliances that run the Forcepoint Content Gateway on Linux software installations.

Before you configure IBM QRadar, you must configure the Forcepoint Content Gateway to provide LEEF formatted syslog events.
Configuring the Management Console for Forcepoint V-Series Content Gateway

You can configure event logging in the Content Gateway Manager.

Procedure

1. Log into your Forcepoint Content Gateway Manager.
2. Click the **Configure** tab.
3. Select **Subsystems > Logging**.
   The General Logging Configuration window is displayed.
4. Select **Log Transactions and Errors**.
5. Select **Log Directory** to specify the directory path of the stored event log files.
   The directory that you define must exist and the Forcepoint user must have read and write permissions for the specified directory.
   The default directory is `/opt/WGC/logs`.
6. Click **Apply**.
7. Click the **Custom** tab.
8. In the **Custom Log File Definitions** window, type the following text for the LEEF format.

   ```
   <LogFormat>
   <Name = "leef"/>
   <Format = "LEEF:1.0\Forcepoint\WCG|7.6|\%<wsds>|\cat=%<wc>
   src=%<cli> \devTime=%<ctn>
   devTimeFormat=dd/MMM/yyyy:HH:mm:ss Z
   http-username=%<caun> \url=%<cquc>
   method=%<cqhm> \httpversion=%<cqhv>
   cachecode=%<czc> dstBytes=%<sscl> dst=%<pqui>
   srcBytes=%<pscl> proxy-status-code=%<pssc>
   server-status-code=%<sssc> usrName=%<wui>
   duration=%<ttms"></Format>
   </LogFormat>

   <LogObject>
   <Format = "leef"/>
   <Filename = "leef"/>
   </LogObject>
   ```

   **Note:** The fields in the LEEF format string are **tab separated**. You might be required to type the LEEF format in a text editor and then cut and paste it into your web browser to retain the tab separations. The definitions file ignores extra white space, blank lines, and all comments.
9. Select **Enabled** to enable the **custom logging** definition.
10. Click **Apply**.

**What to do next**
You can now enable event logging for your Forcepoint Content Gateway.

Enabling Event Logging for Forcepoint V-Series Content Gateway

If you are using a Forcepoint V-Series appliance, contact Forcepoint Technical Support to enable this feature.

Procedure

1. Log in to the command-line Interface (CLI) of the server running Forcepoint Content Gateway.
2. Add the following lines to the end of the `/etc/rc.local` file:

   ```
   ( while [ 1 ] ; do tail -n1000 -F /opt/WCG/logs/leef.log |  
   nc <IP Address> 514 sleep 1 done ) &
   ```
Where <IP Address> is the IP address for IBM QRadar.

3. To start logging immediately, type the following command:

```bash
nohup /bin/bash -c "while [ 1 ] ; do
tail -F /opt/WCG/logs/leef.log | nc <IP Address> 514;
sleep 1; done" &
```

**Note:** You might need to type the logging command in “Enabling Event Logging for Forcepoint V-Series Content Gateway” on page 486 or copy the command to a text editor to interpret the quotation marks.

The configuration is complete. The log source is added to QRadar as syslog events from Forcepoint V-Series Content Gateway are automatically discovered. Events forwarded by Forcepoint V-Series Content Gateway are displayed on the **Log Activity** tab of QRadar.

### Configuring a log source for Forcepoint V-Series Content Gateway

QRadar automatically discovers and creates a log source for syslog events from Forcepoint V-Series Content Gateway.

**About this task**

The following configuration steps are optional.

**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 **Forcepoint V Series**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 281. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

### Log file protocol for Forcepoint V-Series Content Gateway

The log file protocol allows IBM QRadar to retrieve archived log files from a remote host.

The Forcepoint V-Series DSM supports the bulk loading of log files from your Forcepoint V-Series Content Gateway using the log file protocol to provide events on a scheduled interval. The log files contain transaction and error events for your Forcepoint V-Series Content Gateway:
Configuring the Content Management Console for Forcepoint V-Series Content Gateway
Configure event logging in the Content Management Console.

Procedure
1. Log into your Forcepoint Content Gateway interface.
2. Click the Configure tab.
4. Select Log Transactions and Errors.
5. Select Log Directory to specify the directory path of the stored event log files.
   The directory you define must already exist and the Forcepoint user must have read and write
   permissions for the specified directory.
   The default directory is /opt/WGC/logs.
6. Click Apply.
7. Click the Formats tab.
8. Select Netscape Extended Format as your format type.
9. Click Apply.

What to do next
You can now enable event logging for your Forcepoint V-Series Content Gateway.

Configuring a log file protocol log source for Forcepoint V-Series Content Gateway
When you configure your Forcepoint V-Series DSM to use the log file protocol, ensure that the host name
or IP address that is configured in the Forcepoint V-Series is configured the same as the Remote Host
parameter in the log file protocol configuration.

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 the Forcepoint V Series.
9. From the Protocol Configuration list, select the Log File.
10. From the Service Type list, select the Secure File Transfer Protocol (SFTP) option.
11. In the FTP File Pattern field, type extended.log_.*.old.
   This is the default directory for storing the Forcepoint V-Series log files that you specified in
   “Configuring the Content Management Console for Forcepoint V-Series Content Gateway” on page
   488.
13. From the Event Generator list, select LINEBYLINE.
14. Click Save.
15. On the Admin tab, click Deploy Changes.
   The log source is added to QRadar.
Chapter 66. ForeScout CounterACT

The ForeScout CounterACT DSM for IBM QRadar accepts Log Extended Event Format (LEEF) events from CounterACT using syslog. QRadar records the following ForeScout CounterACT events:

- Denial of Service (DoS)
- Authentication
- Exploit
- Suspicious
- System

Configuring a log source

To integrate ForeScout CounterACT with IBM QRadar, you must manually create a log source to receive policy-based syslog events.

About this task

QRadar does not automatically discover or create log sources for syslog events from ForeScout CounterACT appliances.

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 ForeScout CounterACT.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your ForeScout CounterACT appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The log source is added to QRadar.
**Configuring the ForeScout CounterACT Plug-in**

Before you configure IBM QRadar, you must install a plug-in for your ForeScout CounterACT appliance and configure ForeScout CounterACT to forward syslog events to QRadar.

**About this task**

To integrate QRadar with ForeScout CounterACT, you must download, install, and configure a plug-in for CounterACT. The plug-in extends ForeScout CounterACT and provides the framework for forwarding LEEF events to QRadar.

**Procedure**

1. From the ForeScout website, download the plug-in for ForeScout CounterACT.
2. Log in to your ForeScout CounterACT appliance.
3. From the CounterACT Console toolbar, select Options > Plugins > Install. Select the location of the plug-in file.
   
   The plug-in is installed and displayed in the Plug-ins pane.
4. From the Plug-ins pane, select the QRadar plug-in and click Configure.

   The Add QRadar wizard is displayed.
5. In the Server Address field, type the IP address of QRadar.
6. From the Port list, select 514.
7. Click Next.
8. From the Assigned CounterACT devices pane, choose one of the following options:
   
   • Default Server - Select this option to make all devices on this ForeScout CounterACT, forward events to QRadar.
   
   • Assign CounterACT devices - Select this option to assign which individual devices that are running on ForeScout CounterACT forward events to QRadar. The Assign CounterACT devices option is only available if you have one or more ForeScout CounterACT servers.
9. Click Finish.

The plug-in configuration is complete. You are now ready to define the events that are forwarded to QRadar by ForeScout CounterACT policies.

**Configuring ForeScout CounterACT Policies**

ForeScout CounterACT policies test conditions to trigger management and remediation actions on the appliance.

**About this task**

The plug-in provides an extra action for policies to forward the event to the IBM QRadar by using syslog. To forward events to QRadar, you must define a CounterACT policy that includes the QRadar update action.

The policy condition must be met at least one time to initiate an event send to QRadar. You must configure each policy to send updates to QRadar for events you want to record.

**Procedure**

1. Select a policy for ForeScout CounterACT.
2. From the Actions tree, select Audit > Send Updates to QRadar Server.
3. From the Contents tab, configure the following value:
Select the **Send host property results** check box.

4. Choose one of the type of events to forward for the policy:

   - **Send All** - Select this option to include all properties that are discovered for the policy to QRadar.
   - **Send Specific** - Select this option to select and send only specific properties for the policy to QRadar.

5. Select the **Send policy status** check box.

6. From the **Trigger** tab, select the interval ForeScout CounterACT uses for forwarding the event to QRadar:

   - **Send when the action starts** - Select this check box to send a single event to QRadar when the conditions of your policy are met.
   - **Send when information is updated** - Select this check box to send a report when there is a change in the host properties that are specified in the **Contents** tab.
   - **Send periodically every** - Select this check box to send a reoccurring event to QRadar on an interval if the policy conditions are met.

7. Click **OK** to save the policy changes.

8. Repeat this process to configure any additional policies with an action to send updates to QRadar.

   The configuration is complete. Events that are forwarded by ForeScout CounterACT are displayed on the **Log Activity** tab of QRadar.
Chapter 67. Fortinet FortiGate Security Gateway

The IBM QRadar SIEM DSM for Fortinet FortiGate Security Gateway collects events from Fortinet FortiGate Security Gateway and Fortinet FortiAnalyzer products.

The following table identifies the specifications for the Fortinet FortiGate Security Gateway DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Fortinet</td>
</tr>
<tr>
<td>DSM name</td>
<td>Fortinet FortiGate Security Gateway</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-FortinetFortiGate-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>FortiOS V5.6 and earlier</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>Syslog Redirect</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Auto discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td>Fortinet website (<a href="http://www.fortinet.com">http://www.fortinet.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Fortinet FortiGate Security Gateway DSM with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the Fortinet FortiGate Security Gateway RPM on your QRadar Console:

2. Download and install the Syslog Redirect protocol RPM to collect events through Fortinet FortiAnalyzer. When you use the Syslog Redirect protocol, QRadar can identify the specific Fortinet FortiGate Security Gateway firewall that sent the event.

3. For each instance of Fortinet FortiGate Security Gateway, configure your Fortinet FortiGate Security Gateway system to send syslog events to QRadar.

4. If QRadar does not automatically detect the log source for Fortinet FortiGate Security Gateway, you can manually add the log source. For the protocol configuration type, select Syslog, and then configure the parameters.

5. If you want QRadar to receive events from Fortinet FortiAnalyzer, manually add the log source. For the protocol configuration type, select Syslog Redirect, and then configure the parameters.

The following table lists the specific parameter values that are required for Fortinet FortiAnalyzer event collection:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier Regex</td>
<td><code>devname=&quot;?([\w-]+)</code></td>
</tr>
<tr>
<td>Listen Port</td>
<td>517</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
</tr>
</tbody>
</table>

**Related tasks**

**Configuring a syslog destination on your Fortinet FortiGate Security Gateway device**
To forward Fortinet FortiGate Security Gateway events to IBM QRadar, you must configure a syslog destination.

**Procedure**

1. Log in to the command line on your Fortinet FortiGate Security Gateway appliance.
2. Type the following commands, in order, replacing the variables with values that suit your environment.

   ```
   config log syslogd setting
   set status enable
   set facility <facility_name>
   set csv {disable | enable}
   set port <port_integer>
   set reliable enable
   set server <IP_address>
   end
   example: set facility syslog
   ```

   **Note:** If you set the value of `reliable` as `enable`, it sends as TCP; if you set the value of `reliable` as `disable`, it sends as UDP.

**What to do next**
Your deployment might have multiple Fortinet FortiGate Security Gateway instances that are configured to send event logs to FortiAnalyzer. If you want to send FortiAnalyzer events to QRadar, see Configuring a syslog destination on your Fortinet FortiAnalyzer device.

**Configuring a syslog destination on your Fortinet FortiAnalyzer device**
To forward Fortinet FortiAnalyzer events to IBM QRadar, you must configure a syslog destination.

**Procedure**

1. Log in to your FortiAnalyzer device.
2. On the **Advanced** tree menu, select **Syslog Server**.
3. On the toolbar, click **Create New**.
4. Configure the **Syslog Server** parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The default port is 514.</td>
</tr>
</tbody>
</table>

5. Click **OK**.
Chapter 68. Foundry FastIron

You can integrate a Foundry FastIron device with IBM QRadar to collect all relevant events using syslog. To do this you must configure syslog and your log source.

Configuring syslog for Foundry FastIron

To integrate IBM QRadar with a Foundry FastIron RX device, you must configure the appliance to forward syslog events.

Procedure

1. Log in to the Foundry FastIron device command-line interface (CLI).
2. Type the following command to enable logging:
   ```
   logging on
   ```
   Local syslog is now enabled with the following defaults:
   - Messages of all syslog levels (Emergencies - Debugging) are logged.
   - Up to 50 messages are retained in the local syslog buffer.
   - No syslog server is specified.
3. Type the following command to define an IP address for the syslog server:
   ```
   logging host <IP Address>
   ```
   Where `<IP Address>` is the IP address of your QRadar.
   You are now ready to configure the log source in QRadar.

Configuring a log source

QRadar automatically discovers and creates a log source for syslog events from Foundry FastIron. The following configuration steps are optional.

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 Foundry FastIron.
10. Configure the following values:
### Syslog protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Foundry FastIron appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.
Chapter 69. FreeRADIUS

The IBM QRadar DSM for FreeRADIUS collects events from your FreeRADIUS device. The following table lists the specifications for the FreeRADIUS DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>FreeRADIUS</td>
</tr>
<tr>
<td>DSM name</td>
<td>FreeRADIUS</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-FreeRADIUS-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V2.x</td>
</tr>
<tr>
<td>Event format</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>FreeRADIUS website (<a href="http://freeradius.org">http://freeradius.org</a>)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>FreeRADIUS</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Operating system distribution</th>
<th>Command to restart daemon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux</td>
<td>service syslog restart</td>
</tr>
<tr>
<td>Debian Linux or Ubuntu Linux</td>
<td>/etc/init.d/syslog restart</td>
</tr>
<tr>
<td>FreeBSD operating system</td>
<td>/etc/rd.d/syslogd restart</td>
</tr>
</tbody>
</table>

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 70. Generic

IBM QRadar supports a range of Generic DSMs.

Generic Authorization Server

The generic authorization server DSM for IBM QRadar records all relevant generic authorization events by using syslog.

You need to configure QRadar to interpret the incoming generic authorization events, and manually create a log source.

Configuring event properties

To configure IBM QRadar to interpret the incoming generic authorization events:

Procedure

1. Forward all authentication server logs to your QRadar system.
   
   For information on forwarding authentication server logs to QRadar, see your generic authorization server vendor documentation.

2. Open the following file:

   `/opt/QRadar/conf/genericAuthServer.conf`

   Make sure you copy this file to systems that host the Event Collector and the QRadar Console.

3. Restart the Tomcat server:

   `service tomcat restart`

   A message is displayed indicating that the Tomcat server is restarted.

4. Enable or disable regular expressions in your patterns by setting the `regex_enabled` property. By default, regular expressions are disabled.

   For example:

   `regex_enabled=false`

   When you set the `regex_enabled` property to false, the system generates regular expressions (regex) based on the tags you entered when you try to retrieve the corresponding data values from the logs.

   When you set the `regex_enabled` property to true, you can define custom regex to control patterns. These regex configurations are applied directly to the logs and the first captured group is returned. When you define custom regex patterns, you must adhere to regex rules, as defined by the Java programming language. For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

   To integrate the generic authorization server with QRadar, make sure that you specify the classes directly instead of using the predefined classes. For example, the digit class `(/\d/)` becomes `/[0-9]/`. Also, instead of using numeric qualifiers, rewrite the expression to use the primitive qualifiers `(/?/,/+/ and /+/).

5. Review the file to determine a pattern for successful login:

   For example, if your authentication server generates the following log message for accepted packets:

   `Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from <IP_address> port 1727 ssh2`

   The pattern for successful login is:

   `Accepted password`
6. Add the following entry to the file:

   \texttt{login\_success\_pattern=<login\ success\ pattern>}

   Where: \texttt{<login success pattern>} is the pattern that is determined in “Configuring event properties ” on page 501.

   For example:

   \texttt{login\_success\_pattern=\textit{Accepted password}}

   All entries are case insensitive.

7. Review the file to determine a pattern for login failures.

   For example, if your authentication server generates the following log message for login failures:

   \texttt{Jun 27 12:58:33 expo sshd[20627]: Failed password for root from <IP\_address> port 1849 ssh2}

   The pattern for login failures is \texttt{Failed password}.

8. Add the following to the file:

   \texttt{login\_failed\_pattern=<login\ failure\ pattern>}

   Where: \texttt{<login failure pattern>} is the pattern that is determined for login failure.

   For example:

   \texttt{login\_failed\_pattern=\textit{Failed password}}

   All entries are case insensitive.

9. Review the file to determine a pattern for logout:

   For example, if your authentication server generates the following log message for logout:

   \texttt{Jun 27 13:00:01 expo su(<Username>)[22723]: session closed for user genuser}

   The pattern for logout is \texttt{session closed}.

10. Add the following to the \texttt{genericAuthServer.conf} file:

    \texttt{logout\_pattern=<logout\ pattern>}

    Where: \texttt{<logout pattern>} is the pattern that is determined for logout in “Configuring event properties ” on page 501.

    For example:

    \texttt{logout\_pattern=\textit{session}}

    All entries are case insensitive.

11. Review the file to determine a pattern, if present, for source IP address and source port.

    For example, if your authentication server generates the following log message:

    \texttt{Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from <IP\_address> port 1727 ssh2}

    The pattern for source IP address is \textit{from} and the pattern for source port is \textit{port}.

12. Add an entry to the file for source IP address and source port:

    \texttt{source\_ip\_pattern=<source\ IP\ pattern>}

    \texttt{source\_port\_pattern=<source\ port\ pattern>}

    Where: \texttt{<source IP pattern>} and \texttt{<source port pattern>} are the patterns that are identified in “Configuring event properties ” on page 501 for source IP address and source port.

    For example:
source_ip_pattern=from
source_port_pattern=port

13. Review the file to determine whether a pattern exists for user name.

For example:

Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from
<IP_address> port 1727 ssh2

The pattern for user name is for.

14. Add an entry to the file for the user name pattern:

For example:

user_name_pattern=for

You are now ready to configure the log source in QRadar.

Configuring a log source

To integrate generic authorization appliance event with IBM QRadar, you must manually create a log source to receive the events as QRadar does not automatically discover or create log sources for events from generic authorization appliances.

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 Configurable Authentication message filter.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 286. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The log source is added to QRadar. Events that are forwarded to QRadar by generic authorization appliances are displayed on the Log Activity tab.

Generic Firewall

The generic firewall server DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant events.

Configure QRadar to interpret the incoming generic firewall events, and manually create a log source.
Configuring event properties
Configuration of IBM QRadar to interpret the incoming generic firewall events.

About this task
Use the following procedure to configure event properties:

Procedure
1. Forward all firewall logs to your QRadar.
   For information on forwarding firewall logs from your generic firewall to QRadar, see your firewall vendor documentation.
2. Open the following file:
   `/opt/QRadar/conf/genericFirewall.conf`
   Make sure you copy this file to systems that host the Event Collector and the QRadar Console.
3. Restart the Tomcat server:
   `service tomcat restart`
   A message is displayed indicating that the Tomcat server is restarted.
4. Enable or disable regular expressions in your patterns by setting the `regex_enabled` property. By default, regular expressions are disabled.
   For example:
   `regex_enabled=false`
   When you set the `regex_enabled` property to false, the system generates regular expressions based on the tags you entered while you try to retrieve the corresponding data values from the logs.
   When you set the `regex_enabled` property to true, you can define custom regex to control patterns. These regex configurations are directly applied to the logs and the first captured group is returned. When you define custom regex patterns, you must adhere to regex rules, as defined by the Java programming language. For more information, see the following website: `http://download.oracle.com/javase/tutorial/essential/regex/`
   To integrate a generic firewall with QRadar, make sure that you specify the classes directly instead of using the predefined classes. For example, the digit class (`/\d/`) becomes `/\[0-9]/`. Also, instead of using numeric qualifiers, rewrite the expression to use the primitive qualifiers (`/\?/`, `/\*` and `/\+/`).
5. Review the file to determine a pattern for accepted packets.
   For example, if your device generates the following log messages for accepted packets:
   Aug. 5, 2005 08:30:00 Packet accepted. Source IP: <Source_IP_address>
   Source Port: 80 Destination IP: <Destination_IP_address> Destination Port: 80 Protocol: tcp
   The pattern for accepted packets is `Packet accepted`.
6. Add the following to the file:
   `accept_pattern=<accept_pattern>`
   Where: `<accept_pattern>` is the pattern that is determined in “Configuring event properties” on page 504. For example:
   `accept_pattern=Packet accepted`
   Patterns are case insensitive.
7. Review the file to determine a pattern for denied packets.
   For example, if your device generates the following log messages for denied packets:

The pattern for denied packets is Packet denied.

8. Add the following to the file:
   
   deny_pattern=<deny pattern>

   Where: <deny pattern> is the pattern that is determined in “Configuring event properties” on page 504.

   Patterns are case insensitive.

9. Review the file to determine a pattern, if present, for the following parameters:
   - source ip
   - source port
   - destination ip
   - destination port
   - protocol

   For example, if your device generates the following log message:


   The pattern for source IP is Source IP.

10. Add the following to the file:

    - source_ip_pattern=<source ip pattern>
    - source_port_pattern=<source port pattern>
    - destination_ip_pattern=<destination ip pattern>
    - destination_port_pattern=<destination port pattern>
    - protocol_pattern=<protocol pattern>

    Where: <source ip pattern>, <source port pattern>, <destination ip pattern>, <destination port pattern>, and <protocol pattern> are the corresponding patterns that are identified in “Configuring event properties” on page 504.

    **Note:** Patterns are case insensitive and you can add multiple patterns. For multiple patterns, separate by using a # symbol.

11. Save and exit the file.

You are now ready to configure the log source in QRadar.

**Configuring a log source**

To integrate generic firewalls with IBM QRadar, you must manually create a log source to receive the events as QRadar does not automatically discover or create log sources for events from generic firewall appliances.

**Procedure**

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
The Log Sources window is displayed.

5. Click Add.
The Add a log source window is displayed.

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 Configurable Firewall Filter.

The syslog protocol configuration is displayed.

10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 287. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.

12. On the Admin tab, click Deploy Changes.

The log source is added to QRadar. Events that are forwarded to QRadar by generic firewalls are displayed on the Log Activity tab.
Chapter 71. genua genugate

The IBM 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 specific parsing for these logs, install the specific DSM for that device.

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>genua</td>
</tr>
<tr>
<td>DSM name</td>
<td>genua genugate</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-GenuaGenugate-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>8.2 and later</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>General error messages</td>
</tr>
<tr>
<td></td>
<td>High availability</td>
</tr>
<tr>
<td></td>
<td>General relay messages</td>
</tr>
<tr>
<td></td>
<td>Relay-specific messages</td>
</tr>
<tr>
<td></td>
<td>genua programs/daemons</td>
</tr>
<tr>
<td></td>
<td>EPSI</td>
</tr>
<tr>
<td></td>
<td>Accounting Daemon - gg/src/acctd</td>
</tr>
<tr>
<td></td>
<td>Configfw</td>
</tr>
<tr>
<td></td>
<td>FWConfig</td>
</tr>
<tr>
<td></td>
<td>ROFWConfig</td>
</tr>
<tr>
<td></td>
<td>User-Interface</td>
</tr>
<tr>
<td></td>
<td>Webserver</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>genua genugate</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Related tasks**

Adding a DSM
Configuring genua genugate to send events to QRadar
Configure genua genugate to send events to IBM QRadar.

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.

**Configuring genua genugate to send events to QRadar**

Configure genua genugate to send events to IBM 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 72. Great Bay Beacon

The Great Bay Beacon DSM for IBM QRadar supports syslog alerts from the Great Bay Beacon Endpoint Profiler.

QRadar records all relevant Endpoint security events. Before you can integrate Great Bay Beacon with QRadar, you must configure your Great Bay Beacon Endpoint Profiler to forward syslog event messages to QRadar.

Configuring syslog for Great Bay Beacon

You can configure your Great Bay Beacon Endpoint Profiler to forward syslog events.

Procedure

1. Log in to your Great Bay Beacon Endpoint Profiler.
2. To create an event, select Configuration > Events > Create Events.
   A list of currently configured events is displayed.
3. From the Event Delivery Method pane, select the Syslog check box.
4. To apply your changes, select Configuration Apply Changes > Update Modules.
5. Repeat “Configuring syslog for Great Bay Beacon” on page 509 to configure all of the events that you want to monitor in IBM QRadar.
6. Configure QRadar as an external log source for your Great Bay Beacon Endpoint Profiler.
   For information on configuring QRadar as an external log source, see the Great Bay Beacon Endpoint Profiler Configuration Guide.
   You are now ready to configure the log source in QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Great Bay Beacon.

About this task
The following configuration steps are optional:

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 Great Bay Beacon.
10. Configure the following values:
Table 290. Syslog parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Great Bay Beacon appliance.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

   The configuration is complete.
Chapter 73. HBGary Active Defense

The HBGary Active Defense DSM for IBM QRadar accepts several event types that are forwarded from HBGary Active Defense devices, such as access, system, system configuration, and policy events.

Events from Active Defense are forwarded in the Log Event Extended Format (LEEF) to QRadar using syslog. Before you can configure QRadar, you must configure a route for your HBGary Active Defense device to forward events to a syslog destination.

Configuring HBGary Active Defense

You can configure a route for syslog events in Active Defense for QRadar.

Procedure
1. Log in to the Active Defense Management Console.
2. From the navigation menu, select Settings > Alerts.
3. Click Add Route.
4. In the Route Name field, type a name for the syslog route you are adding to Active Defense.
5. From the Route Type list, select LEEF (Q1 Labs).
6. In the Settings pane, configure the following values:
   - Host - Type the IP address or hostname for your QRadar Console or Event Collector.
   - Port - Type 514 as the port number.
7. In the Events pane, select any events that you want to forward to QRadar.
8. Click OK to save your configuration changes.

   The Active Defense device configuration is complete. You are now ready to configure a log source in QRadar. For more information on configuring a route in Active Defense, see your HBGary Active Defense User Guide.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for LEEF formatted syslog events that are forwarded from Active Defense.

About this task
The following configuration steps are optional:

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 Name field, type a name for the log source.
7. In the Log Source Description field, type a description for the log source.
8. From the Log Source Type list, select HBGary Active Defense.
9. From the Protocol Configuration list, select Syslog.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for your HBGary Active Defense device.</td>
</tr>
<tr>
<td></td>
<td>The IP address or host name identifies your HBGary Active Defense device as a unique event source in QRadar.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The HBGary Active Defense configuration is complete.
IBM QRadar accepts events from a range of H3C Technologies DSMs.

### H3C Comware Platform

The IBM QRadar DSM for the H3C Comware Platform collects events from a number of network devices from H3C Technologies. QRadar supports H3C Switches, H3C Routers, H3C Wireless LAN Devices, and H3C IP Security Devices.

The following table describes the specifications for the H3C Comware Platform DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>H3C Technologies Co., Limited</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-H3CComware-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V7</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>NVP</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>System</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>H3C Technologies (<a href="http://www.h3c.com">http://www.h3c.com</a>)</td>
</tr>
</tbody>
</table>

To integrate H3C Comware Platform, H3C Switches, H3C Routers, H3C Wireless LAN Devices, or H3C IP Security Devices with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the H3C Comware Platform DSM RPM on your QRadar Console.
2. Configure your H3C Comware Platform router or device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a H3C Comware Platform log source on the QRadar Console. The following table describes the parameters that require specific values for H3C Comware Platform event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>H3C Comware Platform</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

The following table provides a sample syslog event message for the H3C Comware Platform DSM:
Table 294. H3C Comware Platform sample syslog message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user's AAA request is rejected</td>
<td>AAA Session Denied</td>
<td>&lt;188&gt;Jun 14 17:11:11 2013 HP %10AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain =domain1-Service=login- UserName=cwf@system; AAA is failed.</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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 H3C Comware Platform to communicate with QRadar**

To collect H3C Comware Platform events, enable syslog settings and configure a log host. H3C Switches, H3C Routers, H3C Wireless LAN Devices, and H3C IP Security Devices are supported by QRadar.

**Procedure**

1. Log in to the **command line** interface by using the console port, or by using Telnet or SSH.
   For more information about login methods, see the **Logging into the CLI** section in the configuration guide for your H3C devices.
2. To access the system view, type the `<system_name> system-view` command.
3. To enable the syslog settings, type the following commands in the order that they are listed.
   a. `info-center source default loghost deny`
   b. `info-center source AAA loghost level informational`
   c. `info-center source ACL loghost level informational`
   d. `info-center source FIPS loghost level informational`
   e. `info-center source HTTPD loghost level informational`
   f. `info-center source IKE loghost level informational`
   g. `info-center source IPSEC loghost level informational`
   h. `info-center source LOGIN loghost level informational`
   i. `info-center source LS loghost level informational`
   j. `info-center source PKI loghost level informational`
   k. `info-center source PORTSEC loghost level informational`
   l. `info-center source PWDCTL loghost level informational`
   m. `info-center source RADIUS loghost level informational`
   n. `info-center source SHELL loghost level informational`
   o. `info-center source SNMP loghost level informational`
   p. `info-center source SSHS loghost level informational`
   q. `info-center source TACACS loghost level informational`
   r. `info-center loghost <QRadar Event Collector IP> 514`
4. To exit the system view, type the `quit <system_name>` command.
Chapter 75. Honeycomb Lexicon File Integrity Monitor (FIM)

You can use the Honeycomb Lexicon File Integrity Monitor (FIM) DSM with IBM QRadar to collect detailed file integrity events from your network.

QRadar supports syslog events that are forwarded from Lexicon File Integrity Monitor installations that use Lexicon mesh v3.1 and later. The syslog events that are forwarded by Lexicon FIM are formatted as Log Extended Event Format (LEEF) events by the Lexicon mesh service.

To integrate Lexicon FIM events with QRadar, you must complete the following tasks:

1. On your Honeycomb installation, configure the Lexicon mesh service to generate syslog events in LEEF.
2. On your Honeycomb installation, configure any Lexicon FIM policies for your Honeycomb data collectors to forward FIM events to your QRadar Console or Event Collector.
3. On your QRadar Console, verify that a Lexicon FIM log source is created and that events are displayed on the Log Activity tab.
4. Optional. Ensure that no firewall rules block communication between your Honeycomb data collectors and the QRadar Console or Event Collector that is responsible for receiving events.

Supported Honeycomb FIM event types logged by QRadar

The Honeycomb FIM DSM for IBM QRadar can collect events from several event categories. Each event category contains low-level events that describe the action that is taken within the event category. For example, file rename events might have a low-level category of either file rename successful or file rename failed.

The following list defines the event categories that are collected by QRadar for Honeycomb file integrity events:

- Baseline events
- Open file events
- Create file events
- Rename file events
- Modify file events
- Delete file events
- Move file events
- File attribute change events
- File ownership change events

QRadar can also collect Windows and other log files that are forwarded from Honeycomb Lexicon. However, any event that is not a file integrity event might require special processing by a Universal DSM or a log source extension in QRadar.
Configuring the Lexicon mesh service

To collect events in a format that is compatible with IBM QRadar, you must configure your Lexicon mesh service to generate syslog events in LEEF.

Procedure

1. Log in to the Honeycomb LexCollect system that is configured as the dbContact system in your network deployment.
2. Locate the Honeycomb installation directory for the installImage directory.
   For example, c:\Program Files\Honeycomb\installImage\data.
3. Open the mesh.properties file.
   If your deployment does not contain Honeycomb LexCollect, you can edit mesh.properties manually.
   For example, c:\Program Files\mesh
4. To export syslog events in LEEF, edit the formatter field.
   For example, formatter=leef.
5. Save your changes.

The mesh service is configured to output LEEF events. For information about the Lexicon mesh service, see your Honeycomb documentation.

Configuring a Honeycomb Lexicon FIM log source in QRadar

IBM QRadar automatically discovers and creates a log source for file integrity events that are forwarded from the Honeycomb Lexicon File Integrity Monitor.

About this task

The following procedure is optional:

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 Name field, type a name for your log source.
7. Optional: In the Log Source Description field, type a description for your log source.
8. From the Log Source Type list, select Honeycomb Lexicon File Integrity Monitor.
9. From the Protocol Configuration list, select Syslog.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Honeycomb Lexicon FIM installation. The Log Source Identifier must be unique value.</td>
</tr>
</tbody>
</table>
### Table 295. Syslog protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled</strong></td>
<td>Select this check box to enable the log source. By default, the check box is selected.</td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
<td>From the list, select the Credibility of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
<td>From the list, select the <strong>Target Event Collector</strong> to use as the target for the log source.</td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
<td>Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the <strong>Coalescing Events</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td><strong>Incoming Event Payload</strong></td>
<td>From the list, select the incoming payload encoder for parsing and storing the logs.</td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
<td>Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the <strong>Store Event Payload</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

11. Click **Save**.

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

Honeycomb Lexicon File Integrity Monitor events that are forwarded to QRadar are displayed on the **Log Activity** tab.
Chapter 76. Hewlett Packard (HP)

IBM QRadar can be integrated with several Hewlett Packard (HP) DSMs.

HP Network Automation

The IBM QRadar DSM for HP Network Automation collects events from HP Network Automation software. The following table describes the specifications for the HP Network Automation DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Hewlett Packard</td>
</tr>
<tr>
<td>DSM name</td>
<td>HP Network Automation</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-HPNetworkAutomation-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V10.11</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All operational and configuration network events.</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate HP Network Automation software with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs in the order that they are listed, on your QRadar Console:
   - DSMCommon DSM RPM
   - HP Network Automation DSM RPM
2. Configure your HP Network Automation software to send LEEF events to QRadar.
3. If QRadar does not automatically detect the log source, add an HP Network Automation log source on the QRadar Console. The following table describes the parameters that require specific values for HP Network Automation event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>HP Network Automation</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the device from where QRadar collects HP Network Automation events.</td>
</tr>
</tbody>
</table>
The following table shows a sample LEEF message from the HP Network Automation DSM:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Snapshot</td>
<td>Information</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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 HP Network Automation Software to communicate with QRadar

Configure HP Network Automation Software to send LEEF events to IBM QRadar.

**Before you begin**

You must have administrator access to the HP Network Automation Software user interface.

**Procedure**

1. Log in to the HP Network Automation Software user interface.
2. In the Admin menu, select Event Notification & Response Rules.
4. Configure the parameters for HP Network Automation.

   The following table describes the parameter values to send LEEF events to QRadar:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Email and Event Rule named</td>
<td>You can use any string. For example, QRadar_logs.</td>
</tr>
<tr>
<td>To take this action</td>
<td>Select Send Syslog Message from the list.</td>
</tr>
<tr>
<td>When the following events occur</td>
<td>a. Select all of the events.</td>
</tr>
<tr>
<td></td>
<td>b. Enable the of any importance button.</td>
</tr>
<tr>
<td></td>
<td>c. To take action for For Policy No-Compliance events, enable the for all policies button.</td>
</tr>
<tr>
<td>Rule Status</td>
<td>Enable the Active button.</td>
</tr>
<tr>
<td>Syslog Hostname</td>
<td>QRadar host name or IP address.</td>
</tr>
<tr>
<td>Syslog Port</td>
<td>514</td>
</tr>
<tr>
<td>Syslog Message</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>$EventDate$</td>
<td>devTimeFormat=EE E MMM dd HH:mm:ss Z</td>
</tr>
<tr>
<td></td>
<td>src=$IPAddress$</td>
</tr>
<tr>
<td></td>
<td>eventId=$EventID$</td>
</tr>
<tr>
<td></td>
<td>usrName=$EventUserName$</td>
</tr>
<tr>
<td></td>
<td>eventText=$EventText$</td>
</tr>
</tbody>
</table>

**Note:** All event attributes are tab delimited. For example, devTime, devTimeFormat, and more. Copy the **Syslog Message** value into a text editor, and then verify that the attributes are tab delimited and remove any new line characters.

**Note:** The version number v10 in the LEEF header can be replaced with the exact version of your HP Network Automation software. If you change any other components of the format string, events might not normalize or unknown events might occur.

5. Click **Save**.

**HP ProCurve**

You can integrate an HP ProCurve device with IBM QRadar to record all relevant HP Procurve events using syslog.

**About this task**

Take the following steps to configure your HP ProCurve device to forward syslog events to QRadar.

**Procedure**

1. Log into the HP ProCurve device.
2. Type the following command to make global configuration level changes.
   ```
   config
   
   If successful, the CLI will change to the following prompt:
   ```
   ```
   ProCurve(config)#
   ```
3. Type the following command:
   ```
   logging <syslog-ip-addr>
   
   Where: `<syslog-ip-addr>` is the IP address of QRadar.
   ```
4. To exit config mode, press CTRL+Z.
5. Type the following command: `write mem` to save the current configuration to the startup configuration for your HP ProCurve device.

You are now ready to configure the log source in QRadar.

**Configuring a log source**

IBM QRadar automatically discovers and creates a log source for LEEF formatted syslog events that are forwarded from Active Defense.

**About this task**

These configuration steps are optional:
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 Name field, type a name for the log source.
7. In the Log Source Description field, type a description for the log source.
8. From the Log Source Type list, select HP ProCurve.
9. From the Protocol Configuration list, select Syslog.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for your HP ProCurve device.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
The configuration is complete.

HP Tandem

You can integrate an HP Tandem device with IBM QRadar. An HP Tandem device accepts SafeGuard Audit file events by using a log file protocol source.

About this task
A log file protocol source allows QRadar to retrieve archived log files from a remote host. The HP Tandem DSM supports the bulk loading of log files by using the log file protocol source.

When you configure your HP Tandem device to use the log file protocol, ensure that the host name or IP address that is configured in the HP Tandem device and in the Remote Host parameter are the same.

The SafeGuard Audit file names use the following format:
A
nnnnnnnnnn
The single alphabet character A is followed by a seven-digit decimal integer nnnnnnnn, which increments by 1 each time a name is generated in the same audit pool.

You are now ready to configure the log source and protocol in QRadar.

Procedure
1. From the Log Source Type list, select HP Tandem.
2. To configure the log file protocol, from the Protocol Configuration list, select Log File.
3. From the Event Generator list, select HPTANDEM

   Note: Your system must be running the current version of the log file protocol to integrate with an HP Tandem device:

   For more information about HP Tandem, see your vendor documentation.
To forward events from Hewlett Packard UniX (HP-UX) to IBM QRadar, configure your HP-UX device to send syslog events to QRadar.

**About this task**

You can configure syslog on your HP-UX device to forward events to QRadar.

**Procedure**

1. Log in to the HP-UX device command-line interface.
2. Open the following file:
   `/etc/syslog.conf`
3. Add the following line:
   `<facility>.<level><destination>`
   Where:
   - `<facility>` is `auth`.
   - `<level>` is `info`.
   - `<destination>` is the IP address of the QRadar Console.
4. Save and exit the file.
5. Type the following command to ensure that syslogd enforces the changes to the `syslog.conf` file.
   ```
   kill -HUP `cat /var/run/syslog.pid`
   ```
   **Note:** Back quotation marks are used in the command-line.

**What to do next**

Add a log source in QRadar.

**Related tasks**

- “Adding a log source” on page 523
- To collect Syslog events from your HP-UX device, manually add a log source in IBM QRadar by completing the following steps:

**Adding a log source**

To collect Syslog events from your HP-UX device, manually add a log source in IBM QRadar by completing the following steps:

**Procedure**

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Click **Add**.
4. Configure the Hewlett Packard UniX parameters.

The following table describes the parameters that require specific values to collect events from HP-UX:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a name for the log source.</td>
</tr>
</tbody>
</table>
Table 300. Hewlett Packard UniX Syslog parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>Hewlett Packard UniX</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for your Hewlett Packard UniX device.</td>
</tr>
</tbody>
</table>

5. Click **Save**.
6. On the **Admin** tab, click **Deploy Changes**.

**Related tasks**

“Adding a log source” on page 4

If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.
IBM QRadar can integrate with several Huawei DSMs.

**Huawei AR Series Router**

The Huawei AR Series Router DSM for IBM QRadar can accept events from Huawei AR Series Routers by using syslog.

QRadar records all relevant IPv4 events that are forwarded from Huawei AR Series Router. To integrate your device with QRadar, you must create a log source, then configure your AR Series Router to forward syslog events.

**Supported routers**

The DSM supports events from the following Huawei AR Series Routers:

- AR150
- AR200
- AR1200
- AR2200
- AR3200

**Configuring a log source**

IBM QRadar does not automatically discover incoming syslog events from Huawei AR Series Routers.

**About this task**

If your events are not automatically discovered, you must manually create a log source from the Admin tab in QRadar.

**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 **Huawei AR Series Router**.
9. From the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address, host name, or name for the log source as an identifier for your Huawei AR Series Router. Each log source that you create for your Huawei AR Series Router must include a unique identifier, such as an IP address or host name.</td>
</tr>
</tbody>
</table>

11. Click **Save**.

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

The log source is added to QRadar. You are now ready to configure your Huawei AR Series Router to forward events to QRadar.

**Configuring Your Huawei AR Series Router**

To forward syslog events to IBM QRadar, you must configure your Huawei AR Series Router as an information center, then configure a log host.

**About this task**

The log host that you create for your Huawei AR Series Router can forward events to your QRadar Console or an Event Collector.

**Procedure**

1. Log in to your Huawei AR Series Router command line Interface (CLI).
2. Type the following command to access the system view:
   ```
   system-view
   ```
3. Type the following command to enable the information center:
   ```
   info-center enable
   ```
4. Type the following command to send informational level log messages to the default channel:
   ```
   info-center source default channel loghost log level informational debug state off trap state off
   ```
5. Optional: To verify your Huawei AR Series Router source configuration, type the command:
   ```
   display channel loghost
   ```
6. Type the following command to configure the IP address for QRadar as the log host for your switch:
   ```
   info-center loghost <IP address> facility <local>
   ```
   Where:
   - `<IP address>` is the IP address of the QRadar Console or Event Collector.
   - `<local>` is the syslog facility, for example, local0.
   
   For example,
   ```
   info-center loghost <IP_address> facility local0
   ```
7. Type the following command to exit the configuration:
   ```
   quit
   ```

The configuration is complete. You can verify events that are forwarded to QRadar by viewing events on the **Log Activity** tab.
Huawei S Series Switch

The Huawei S Series Switch DSM for IBM QRadar can accept events from Huawei S Series Switch appliances by using syslog.

QRadar records all relevant IPv4 events that are forwarded from Huawei S Series Switches. To integrate your device with QRadar, you must configure a log source, then configure your S Series Switch to forward syslog events.

Supported switches
The DSM supports events from the following Huawei S Series Switches:
- S5700
- S7700
- S9700

Configuring a log source
IBM QRadar does not automatically discover incoming syslog events from Huawei S Series Switches.

About this task
If your events are not automatically discovered, you must manually create a log source from the Admin tab in QRadar.

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 Huawei S Series Switch.
9. From the Protocol Configuration list, select Syslog.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 301. Syslog protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The log source is added to QRadar. You are now ready to configure your Huawei S Series Switch to forward events to QRadar.
Configuring Your Huawei S Series Switch

To forward syslog events to IBM QRadar, you must configure your Huawei S Series Switch as an information center, then configure a log host.

About this task

The log host that you create for your Huawei S Series Switch can forward events to your QRadar Console or an Event Collector.

Procedure

1. Log in to your Huawei S Series Switch command line Interface (CLI).
2. Type the following command to access the system view:
   ```
   system-view
   ```
3. Type the following command to enable the information center:
   ```
   info-center enable
   ```
4. Type the following command to send informational level log messages to the default channel:
   ```
   info-center source default channel loghost log level informational debug state off trap state off
   ```
5. Optional: To verify your Huawei S Series Switch source configuration, type the command:
   ```
   display channel loghost
   ```
6. Type the following command to configure the IP address for QRadar as the log host for your switch:
   ```
   info-center loghost <IP_address> facility <local>
   ```
   Where:
   - `<IP address>` is the IP address of the QRadar Console or Event Collector.
   - `<local>` is the syslog facility, for example, local0.
   For example,
   ```
   info-center loghost <IP_address> facility local0
   ```
7. Type the following command to exit the configuration:
   ```
   quit
   ```
   The configuration is complete. You can verify events that are forwarded to QRadar by viewing events on the Log Activity tab.
Chapter 78. HyTrust CloudControl

The IBM QRadar DSM for HyTrust CloudControl collects events from HyTrust CloudControl devices. The following table lists the specifications for the HyTrust CloudControl DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Hytrust</td>
</tr>
<tr>
<td>DSM name</td>
<td>HyTrust CloudControl</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-HyTrustCloudControl-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V3.0.2 through V3.6.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Hytrust web site (<a href="http://www.hytrust.com">http://www.hytrust.com</a>)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>HyTrust CloudControl</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks

Adding a DSM
Configuring HyTrust CloudControl to communicate with QRadar
To collect HyTrust CloudControl events, you must configure your third-party device to send events to IBM QRadar

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.

**Configuring HyTrust CloudControl to communicate with QRadar**

To collect HyTrust CloudControl events, you must configure your third-party device to send events to IBM 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 79. IBM

IBM QRadar supports a number of IBM DSMs.

IBM AIX

IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM names</td>
<td>IBM AIX Server</td>
</tr>
<tr>
<td>RPM file names</td>
<td>DSM-IBMAIXServer-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol type</td>
<td>Syslog</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Login or logoff events</td>
</tr>
<tr>
<td></td>
<td>Session opened or session closed events</td>
</tr>
<tr>
<td></td>
<td>Accepted password and failed password events</td>
</tr>
<tr>
<td></td>
<td>Operating system events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td>IBM website (<a href="http://www.ibm.com/">http://www.ibm.com/</a>)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>IBM AIX Server</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks

Adding a DSM
Configuring your IBM AIX Server device to send syslog events to QRadar
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.

**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 @<IP_address>
   # 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM names</td>
<td>IBM AIX Audit</td>
</tr>
<tr>
<td>RPM file names</td>
<td>DSM-IBMAIXAudit-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V6.1 and V7.1</td>
</tr>
<tr>
<td>Protocol type</td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>Log File Protocol</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Audit events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>IBM website (<a href="http://www.ibm.com/">http://www.ibm.com/</a>)</td>
</tr>
</tbody>
</table>

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 534.
   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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>IBM AIX Audit</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>IBM AIX Audit</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Log File</td>
</tr>
<tr>
<td>Service Type</td>
<td>The protocol to retrieve log files from a remote server.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong>: 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.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>If the host for your event files uses a non-standard port number for FTP, SFTP, or SCP, adjust the port value.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>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.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Restriction</strong>: 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.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>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_<em>.</em>.</td>
</tr>
<tr>
<td>FTP Transfer Mode</td>
<td>ASCII is required for text event logs that are retrieved by the log file protocol by using FTP.</td>
</tr>
</tbody>
</table>
### Related tasks

**Adding a DSM**

**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 QRadar Console or Event Collector.

**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.

**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.

**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 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 | /usr/sbin/auditselect -m -e "command != logger && command != auditstream && command != auditpr && command != auditselect" | auditpr -t0 -h eclrRdi -v | sed -e :a -e '$!N;s/\n / ;ta' -e 'P;D' | /usr/bin/logger -p local0.debug -r &
   ```
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:

\[
\begin{align*}
\text{trail} &= \text{/audit/trail} \\
\text{bin1} &= \text{/audit/bin1} \\
\text{bin2} &= \text{/audit/bin2} \\
\text{binsize} &= 10240 \\
\text{cmds} &= \text{/etc/security/audit/bincmds}
\end{align*}
\]

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:

\[
\text{audit start}
\]

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-r</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-n</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-l</code></td>
<td>Defines the name of the last record file.</td>
</tr>
<tr>
<td><code>-m</code></td>
<td>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 <code>-m</code> parameter, the script deletes the audit file with the oldest time stamp.</td>
</tr>
<tr>
<td><code>-t</code></td>
<td>Defines the directory that contains the audit trail file. The default directory is /audit/trail.</td>
</tr>
</tbody>
</table>
**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.

---

**IBM i**

The IBM QRadar DSM for IBM i, formerly known as AS/400 iSeries, collects audit records and event information from IBM i systems.

The following table identifies the specifications for the IBM i DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM i</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V5R4 and later</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMi-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>Log File Protocol</td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit records and events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>IBM website (<a href="http://www.ibm.com/">http://www.ibm.com/</a>)</td>
</tr>
</tbody>
</table>

To collect events from IBM i systems, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM i DSM RPM on your QRadar Console.
2. Configure your IBM i system to communicate with QRadar.
3. Add an IBM i log source on the QRadar Console by using the following table to configure the parameters that are required to collect IBM i events:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>IBM i</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Log File</td>
</tr>
<tr>
<td></td>
<td>If you are using the PowerTech Interact or LogAgent for System i® software to collect CEF formatted syslog messages, you must select the <strong>Syslog</strong> option</td>
</tr>
<tr>
<td>Service Type</td>
<td>Secure File Transfer Protocol (SFTP)</td>
</tr>
</tbody>
</table>

**Related tasks**

*Configuring IBM i to integrate with IBM QRadar*
You can integrate IBM i with IBM QRadar.

Adding a DSM
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.

Configuring Townsend Security Alliance LogAgent to integrate with QRadar
You can collect all audit logs and system events from Townsend Security Alliance LogAgent. You must configure Alliance LogAgent for the IBM QRadar LEEF and configure a destination that specifies QRadar as the syslog server.

Configuring IBM i to integrate with IBM QRadar
You can integrate IBM i with IBM QRadar.

Procedure
1. From IBM Fix Central (http://www.ibm.com/support/fixcentral), download the following file:
   AJLIB.SAVF
2. Copy the AJLIB.SAVF file to a computer or terminal that has FTP access to IBM i.
3. Create a generic online SAVF file on the IBM i by typing the following command:
   CRTSAVF QGPL/SAVF
4. Use FTP on the computer or terminal to replace the IBM i generic SAVF file with the AJLIB.SAVF file that you downloaded.
   Type the following commands:
   ```
   bin
cd qgpl
lcd c:\
put ajlib.savf savf
quit
   ```
   If you are transferring your SAVF file from another IBM i system, send the file by placing the FTP sub-command mode BINARY before the GET or PUT statement.
5. Restore the AJLIB file on IBM i by typing the following command:
   RSTLIB SAVLIB(AJLIB) DEV(\*SAVF) SAVF(QGPL/AJLIB)
   AJLIB provides the mapping and data transfer support that is needed to send IBM i audit journal entries to QRadar.
6. Run AJLIB/SETUP
   The setup screen is used to configure AJLIB for FTP, SFTP, or a local path to receive the processed entries.
   The server user ID is required for FTP or SFTP, and a password is required for FTP. While FTP handles line delimiter conversions, you set the line feed to the expected value for the type of system that receives the SFTP transfers.
7. If you want to use SFTP, run AJLIB/GENKEY.
   This command generates the SSH key pair that is required for SFTP authentication. If the key pair exists, it is not replaced. If you want to generate a new key pair, before you run this command, remove the existing key files from the /ajlib/.ssh directory.
   For more information about SSH key pair configuration on the IBM i, see http://www-01.ibm.com/support/docview.wss?uid=nas8N1012710
8. After you generate a key pair, use the following steps to enable the use of the key pair on the server:
   a) Copy the id_rsa.pub file from the /ajlib directory to the SSH server, and then install it in the appropriate folder.
b) Ensure that the SSH server is added to the known_hosts file of the user profile that runs the AJLIB/AUDITJRN command.

9. Use the appropriate user profile to do the following steps:
   a) Start a PASE (Portable Application Solutions Environment) shell by typing the following command:
      ```
call qp2term
      ```
   b) Start a session with the SSH server by typing the following command:
      ```
ssh -T <user>@<serveraddress>
      ```
   c) If prompted, accept the system key, and enter a password.
   d) Type exit, to close the SSH session.

If you want to run these steps under a different IBM i profile than the one that runs the AJLIB/AUDITJRN command, copy the .ssh directory and known_hosts file to the home directory of the profile that is used to run this command.

10. To configure the filtering of specific entry types, use the AJLIB/SETENTTYP command.

11. Set up the data collection start date and time for the audit journal library (AJLIB) by typing the following command:

   **AJLIB/DATETIME**

   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.

   To preserve your previous start date and time information from a previous installation, you must run **AJLIB/DATETIME**. Record the previous start date and time and type those values when you run **AJLIB/SETUP**. 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.

12. Run **AJLIB/AUDITJRN**.

   The audit journal collection program starts and sends the records to your remote FTP server. If the transfer to the FTP server fails, a message is sent to QSYSOPR. The process for starting AJLIB/AUDITJRN is typically automated by an IBM i job Scheduler, which collects records periodically.

   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.

**Manually extracting journal entries for IBM i**

You can run the DSPJRN command to extract journal entries for IBM i when an audit journal receiver chain is broken.

**About this task**

Run the ALJIB/DATETIME command to set the Start Date to *OUTF. This command forces the processing program to use the pre-built QTEMP/AUDITJRN outfile for parsing, instead of using the date time to extract journal entries. After you run the parsing program command AJLIB/AUDITJRN, the DATETIME is set to the new processing date.

**Procedure**

1. Log in to your IBM i system command-line interface (CLI).
2. Run **DSPJRN**.

   The only changeable parameters in the following example are **RCVRNG** and **ENTTYP**. Do not change any other command parameters. Ensure that **ENTTP** matches the AJLIB/SETENTTYP command settings.
3. To set the **Date Time** to use outfile *OUTF* support, run the **AJLIB/DATETIME** command.

4. Run **AJLIB/AUDITJRN**.

**Results**

The **DATETIME** is set to the next start date.

**Pulling Data Using Log File Protocol**

You can configure IBM i as the log source, and to use the log file protocol in IBM QRadar:

**Procedure**

1. To configure QRadar to receive events from an IBM i system, you must select the IBM i option from the **Log Source Type** list.
2. To configure the log file protocol for the IBM i DSM, you must select the **Log File** option from the **Protocol Configuration** list and define the location of your FTP server connection settings.

   **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 from the **Protocol Configuration** list.
3. Use the log file protocol option that you select a secure protocol for transferring files, such as Secure File Transfer Protocol (SFTP).
Configuring Townsend Security Alliance LogAgent to integrate with QRadar
You can collect all audit logs and system events from Townsend Security Alliance LogAgent. You must configure Alliance LogAgent for the IBM QRadar LEEF and configure a destination that specifies QRadar as the syslog server.

Procedure
1. Log in to your Townsend Security Alliance LogAgent appliance.
2. Add the ALLSYL100 to your library list by typing the following command: addlible allsy1100.
3. To display the main menu select go symain.
4. Select the option for Configuration
5. Select Configure Alliance LogAgent and configure the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface version</td>
<td>4=IBM QRadar LEEF</td>
</tr>
<tr>
<td>Transmit</td>
<td>1=Yes</td>
</tr>
<tr>
<td>Data queue control</td>
<td>1=Yes</td>
</tr>
<tr>
<td>Format</td>
<td>4=IBM QRadar LEEF</td>
</tr>
</tbody>
</table>

6. From the configuration menu, select Work With TCP Clients.
7. Select option 2 to change the SYSLOGD client and configure the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>1=Active</td>
</tr>
<tr>
<td>Autostart client</td>
<td>1=Yes</td>
</tr>
<tr>
<td>Remote IP address</td>
<td>IP address of QRadar</td>
</tr>
<tr>
<td>Remote port number</td>
<td>514</td>
</tr>
</tbody>
</table>

8. From the Configuration menu, select Start LogAgent Subsystem. Events flow to QRadar.

What to do next
After TCP services start, consider automatically starting the Alliance LogAgent subsystem by modifying your IPL QSTRUP program to include the following statements:

```c
/* START ALLIANCE LOGAGENT */
QSYS/STRSBS ALLSYL100/ALLSYL100
MONMSG MSGID(CPF0000)
```

For more information about installing and configuring for Independent Auxiliary Storage Pool operation, and more filter options for events, see your vendor documentation.

**IBM BigFix**
The IBM BigFix DSM for IBM QRadar accepts system events in Log Extended Event Format (LEEF) retrieved from IBM BigFix.

IBM BigFix is formerly known as IBM Tivoli® Endpoint Manager.

QRadar uses the IBM BigFix SOAP protocol to retrieve events on a 30-second interval. As events are retrieved, the IBM BigFix DSM parses and categorizes the events for QRadar. The SOAP API for IBM BigFix is only available after you install the Web Reports application. The Web Reports application for IBM BigFix is required to retrieve and integrate IBM BigFix system event data with QRadar.

**Note:** QRadar supports IBM BigFix versions 8.2.x to 9.5.2.
To integrate IBM BigFix with QRadar, you must manually configure a log source. Events from IBM BigFix are not automatically discovered.

- Log in to QRadar.
- Click the Admin tab.
- Click the Log Sources icon.
- Click Add.
- In the Log Source Name field, type a name for the log source.
- In the Log Source Description field, type a description for the log source.
- From the Log Source Type list, select BigFix.
- From the Protocol Configuration list, select BigFix SOAP.

Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for your IBM BigFix appliance. The IP address or host name identifies your IBM BigFix as a unique event source in QRadar.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number that is used to connect to the IBM BigFix by using the SOAP API. By default, port 80 is the port number for communicating with IBM BigFix. If you are use HTTPS, you must update this field to the HTTPS port number for your network. Most configurations use port 443 for HTTPS communications.</td>
</tr>
<tr>
<td>Use HTTPS</td>
<td>Select this check box to connect by using HTTPS. If you select this check box, the host name or IP address you specify uses HTTPS to connect to your IBM BigFix. If a certificate is required to connect by using HTTPS, you must copy any certificates that are required by the QRadar Console or managed host to the following directory: /opt/qradar/conf/trusted_certificates. QRadar support certificates with the following file extensions: .crt, cert, or .der. Copy any required certificates to the trusted certificates directory before you save and deploy your changes.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name that is required to access your IBM BigFix.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password that is required to access your IBM BigFix.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password necessary to access your IBM BigFix.</td>
</tr>
</tbody>
</table>

For more information about configuring QRadar to import IBM BigFix vulnerabilities assessment information, see the IBM QRadar Vulnerability Assessment Configuration Guide.

Click Save.

On the Admin tab, click Deploy Changes.

Related concepts
“IBM BigFix SOAP protocol configuration options” on page 54
To receive Log Extended Event Format (LEEF) formatted events from IBM BigFix® appliances, configure a log source that uses the IBM BigFix SOAP protocol.

**IBM BigFix Detect**

The IBM QRadar DSM for IBM BigFix Detect collects events from the IBM BigFix Detect platform. The following table describes the specifications for the IBM BigFix Detect DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM BigFix Detect</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMBigFixDetect-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V9.5</td>
</tr>
<tr>
<td>Protocol</td>
<td>IBM BigFix EDR REST API Protocol</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>IOC and IOA alerts</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>IBM BigFix website (<a href="http://www-03.ibm.com/security/bigfix/index.html">http://www-03.ibm.com/security/bigfix/index.html</a>)</td>
</tr>
</tbody>
</table>

To integrate IBM BigFix Detect 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:
   - Protocol Common RPM
   - IBM BigFix EDR REST API Protocol RPM
   - DSM Common RPM
   - IBM BigFix Detect DSM RPM

2. Configure your IBM BigFix Detect for API access.

3. Add an IBM BigFix Detect log source on the QRadar Console. The following table describes the parameters that require specific values to collect event from IBM BigFix Detect:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>IBM BigFix Detect</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>IBM BigFix EDR REST API</td>
</tr>
<tr>
<td>API Hostname or IP</td>
<td>The host name or IP address of the BigFix EDR API</td>
</tr>
<tr>
<td>API Port</td>
<td>The port number that is used to access the API. The default is 443.</td>
</tr>
</tbody>
</table>
Table 309. IBM BigFix Detect log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Certificate Filename</td>
<td>The PKCS12 certificate file name in the /opt/qradar/conf/trusted_certificates/ibmbigfixedr directory in QRadar.</td>
</tr>
<tr>
<td>Client Certificate Password</td>
<td>The password that you used for the Client Certificate.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses the BigFix EDR API by using a proxy, enable Use Proxy.</td>
</tr>
<tr>
<td></td>
<td>If the proxy requires authentication, configure the Proxy Server, Proxy Port, Proxy Username, and Proxy Password fields.</td>
</tr>
<tr>
<td></td>
<td>If the proxy does not require authentication, configure the Proxy Server and Proxy Port fields.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second. The default is 5000.</td>
</tr>
</tbody>
</table>

4. To verify that QRadar is configured correctly, review the following table to see an example of a normalized event message.

The following table shows a sample LEEF event message from IBM BigFix Detect:

Table 310. IBM BigFix Detect sample LEEF message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOC Detected</td>
<td>Suspicious Activity</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 BigFix Detect to communicate with QRadar**

To configure IBM QRadar to collect IOC and IOA alerts from an IBM BigFix Detect system, you must obtain information that is required for the configuration from your IBM BigFix administrator.

**Before you begin**

Before you can configure QRadar to receive alerts from IBM BigFix Detect, you must contact your IBM BigFix Administrator and obtain the following information:

- Hostname or IP address
- Port number
- Private key and corresponding certificate, and Trusteer® CA certificate

For more information about the information that is required for sending alerts from BigFix Detect, see the IBM BigFix documentation (https://www.ibm.com/support/knowledgecenter/SSMNRU_9.5.0/com.ibm.bigfix.detect.doc/BigFixDetectionandResponse/EDRBigFixAdministratorGuide/EDR_alerts_QRadar.html).

**Procedure**

1. Generate the pkcs12 formatted client keystore.
   a) Log in to QRadar using SSH.
   b) Type the following command:
      ```
      openssl pkcs12 -inkey <private_key_filename> -in <certificate_filename> -export -out <PKCS#12_filename>
      ```
      The parameters are described in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>private_key_filename</td>
<td>The Private key that you obtained from the BigFix administrator.</td>
</tr>
<tr>
<td>certificate_filename</td>
<td>The corresponding certificate that you obtained from the BigFix administrator.</td>
</tr>
<tr>
<td>PKCS#12_filename</td>
<td>The output keystore file name. For example, bigfix_client_certificate.pkcs12</td>
</tr>
</tbody>
</table>

**Note:** Record the password that you created when you generated the pkcs12 client keystore. The password is required when you configure the log source.

2. Store the keystore and CA certificate in QRadar.
   a) Copy the Trusteer CA certificate in the /opt/qradar/conf/trusted_certificates/ directory in QRadar.
   b) Create a directory named ibmbigfixedr in the /opt/qradar/conf/trusted_certificates/ directory.
   c) Copy the keystore.pkcs12 file to the /opt/qradar/conf/trusted_certificates/ibmbigfixedr/ directory that you created. Do not store the client keystore file in any other location.

**What to do next**

Configure the log source in QRadar by using only the file name of the client keystore file in the /opt/qradar/conf/trusted_certificates/ibmbigfixedr/ directory. Ensure that you type the file
name correctly in the **Client Certificate Filename** field. Type the password that you created when you generated the pkcs12 client keystore, in the **Client Certificate Password** field.

### IBM Bluemix Platform

The IBM QRadar DSM for the IBM Bluemix Platform collects events logs from your Bluemix Platform.

The following table identifies the specifications for the IBM Bluemix Platform DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM Bluemix Platform</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMBluemixPlatform-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog, TLS Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All System (Cloud Foundry) events, some application events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>IBM website for Bluemix (IBM website for Bluemix)</td>
</tr>
</tbody>
</table>

To integrate IBM Bluemix Platform with QRadar, complete the following steps:

You must perform the installation, third-party configuration, and QRadar configuration procedures in the order. Installation must always be first, but you can invert the order of the other two procedures. In some cases, no action is required for the third-party configuration and you can omit the procedure.

1. If automatic updates are not enabled, download and install the most recent version of the IBM Bluemix Platform DSM RPM on your QRadar Console:
2. Configure your IBM Bluemix Platform device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an IBM Bluemix Platform log source on the QRadar Console.

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 Bluemix Platform to communicate with QRadar

To collect IBM Bluemix Platform events, you must configure your third-party instance to send events to QRadar.

**Before you begin**

You must have an app running in IBM Bluemix so that you can create log drains.
Procedure

1. From the Cloud Foundry command-line interface, type the following command to create a drain:

```bash
cf cups drain_name -l syslog://QRadar_IP_Address:514
```

Alternatively, use the following command:

```bash
cf cups drain_name -l syslog-tls://QRadar_IP_Address:1513
```

1513 is the port that is used to communicate with QRadar.

2. Bind the service instance with the following command:

```bash
cf bind-service BusinessApp_name drain_name
```

Integrating IBM Bluemix Platform with QRadar

In most installations, there is only the RPM. For installations where there are multiple RPMs required, (for example a PROTOCOL RPM and a DSMCommon RPM), ensure that the installation sequence reflects RPM dependency.

Procedure

1. If required, download and install the latest TLS Syslog RPM on your QRadar Console. You can install a protocol by using the procedure to manually install a DSM. If automatic updates are configured to install protocol updates, this procedure is not necessary.

2. Download and install the latest DSMCommon RPM on your QRadar Console. If automatic updates are configured to install DSM updates, this procedure is not necessary.

3. Download and install the latest IBM Bluemix Platform RPM on your QRadar Console. If automatic updates are configured to install DSM updates, this procedure is not necessary.

What to do next

You must configure a IBM Bluemix log source in QRadar by using Syslog or Syslog TLS.

Configuring an IBM Bluemix log source to use Syslog

You can configure an IBM Bluemix log source in IBM QRadar.

Procedure

1. Log in to QRadar to use **Syslog**.
2. On the **Admin** tab, click **Data Sources > Log Sources > Add**.
3. From the **Log Source Type** list, select **IBM Bluemix Platform**.
4. From the **Protocol Configuration** list, select **Syslog**.
5. In the **Log Source Identifier** field, enter the IP address of the Bluemix Loggregator.

   **Important:** It might be necessary to include the IP address and the port, as the Log Source Identifier. For example, `192.0.2.1:1513`.

6. Configure the remaining fields in the **Log Sources** window as required and click **Save**.
7. On the **Admin** tab toolbar, click **Deploy Changes**.

Related tasks

- “Adding a DSM” on page 4
- “Adding a log source” on page 4
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 Bluemix log source with TLS Syslog**

You can configure an IBM Bluemix log source in IBM QRadar to use TLS Syslog.

**Procedure**

1. Log in to QRadar.
2. On the **Admin** tab, click **Data Sources** > **Log Sources** > **Add**.
3. From the **Log Source Type** list, select **IBM Bluemix Platform**.
4. From the **Protocol Configuration** list, select **TLS Syslog**.
5. In the **Log Source Identifier** field, enter the IP address of the Bluemix Loggregator.
6. In the **TLS Listen Port** field, enter a port number.
7. From the **Authentication Mode** list, select **TLS**.
8. From the **Certificate Type** list, select **Provide Certificate**.
9. In the **Provided Server Certificate Path** field, enter the absolute path to the server certificate, for example:
   ```
   syslog-tls.cert
   ```
10. In the **Provided Private Key Path** field, enter the absolute path the private key.
    
    The private key must be a DER-encoded PKCS8 key.
11. Configure the remaining fields in the **Log Sources** window as required and click **Save**.
12. On the **Admin** tab toolbar, click **Deploy Changes**.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4
- If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

### IBM CICS

The IBM CICS DSM collects events from IBM Custom Information Control System (CICS®) on an IBM z/OS® mainframe that uses IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.

To collect IBM CICS events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html).
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 (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).
3. Create a log source in QRadar for IBM CICS.

Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

• You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
• The SCKRLOAD library must be APF-authorized.
• If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)
• You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
• If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
• If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.


Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4

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

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:

• IBM z/OS
• IBM CICS
• IBM RACF
• IBM DB2
• CA Top Secret
• CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:
### Table 312. Log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Select your DSM name from the list.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>

### Creating a log source for Log File protocol

The Log File protocol enables IBM QRadar to retrieve archived log files from a remote host for the IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, and CA ACF2 DSM's.

### 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 z/OS with zSecure writes log files to a specified directory as gzipped archives. 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 that uses the Log File protocol. QRadar requires credentials to log in to the system that hosts your LEEF formatted event files and a polling interval.

### Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. In the **Log Source Name** field, type a name for the log source.
6. In the **Log Source Description** field, type a description for the log source.
7. From the **Log Source Type** list, select your DSM name.
8. From the **Protocol Configuration** list, select **Log File**.
9. Configure the Log File protocol parameters.

The following table describes the parameters that require specific values for the DSM event collection:

### Table 313. Log File protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| **Log Source Identifier** | Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested as they allow QRadar to identify a log file to a unique event source.  
For example, if your network contains multiple z/OS images or a file repository that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify. |
### Table 313. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| **Service Type**   | From the **Service Type** list, select the protocol that 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 that is used to retrieve log files for the SCP and SFTP service type requires that the server that is 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 that stores 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 - 65535.  
  The options include ports:  
  • 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. |
| **Remote User**    | Type the user name or user ID necessary to log in to the system that contains your event files.  
  • If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length.  
  • If your log files are 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 gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.                              |
| **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.                                                                                                                                 |
| **Recursive**      | If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear.  
  If you configure SCP as the Service Type, the Recursive option is ignored. |
### Table 313. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FTP File Pattern</strong></td>
<td>If you select <strong>SFTP</strong> or <strong>FTP</strong> as the <strong>Service Type</strong>, you can configure the regular expression (regex) needed to filter the list of files that are specified in the <strong>Remote Directory</strong>. All matching files are included in the processing. The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <code>&lt;product_name&gt;\.&lt;timestamp&gt;.gz</code> The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with <code>zOS</code> and end with <code>.gz</code>, type the following code: <code>zOS.*\..gz</code> Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions. (<a href="http://download.oracle.com/javase/tutorial/essential/regex/">http://download.oracle.com/javase/tutorial/essential/regex/</a>)</td>
</tr>
<tr>
<td><strong>FTP Transfer Mode</strong></td>
<td>This option displays only if you select <strong>FTP</strong> as the <strong>Service Type</strong>. From the list, select <strong>Binary</strong>. The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as <code>zip</code>, <code>gzip</code>, <code>tar</code>, or <code>tar+gzip</code> archive files.</td>
</tr>
<tr>
<td><strong>SCP Remote File</strong></td>
<td>If you select <strong>SCP</strong> as the <strong>Service Type</strong> you must type the file name of the remote file.</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>Type the time of day you want the processing to begin. For example, type <code>00:00</code> 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.</td>
</tr>
<tr>
<td><strong>Recurrence</strong></td>
<td>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 <code>2H</code> if you want the remote directory to be scanned every 2 hours from the start time. The default is <code>1H</code>.</td>
</tr>
<tr>
<td><strong>Run On Save</strong></td>
<td>If you want the Log File protocol to run immediately after you click <strong>Save</strong>, select this check box. After the <strong>Run On Save</strong> completes, the Log File protocol follows your configured start time and recurrence schedule. Selecting <strong>Run On Save</strong> clears the list of previously processed files for the Ignore Previously Processed File parameter.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.</td>
</tr>
</tbody>
</table>
Table 313. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>From the list, select gzip. Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in zip, gzip, tar, or tar+gzip archive format.</td>
</tr>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>Select this check box to track and ignore files that are already processed by the Log File protocol. QRadar examines the log files in the remote directory to determine whether a file is 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 are not previously processed are downloaded. This option applies only to FTP and SFTP service types.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>Select this check box to define a local directory on your QRadar for storing downloaded files during processing. It is suggested that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which gives you the option to configure the local directory to use for storing files.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the Event Generator list, select LineByLine. The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.</td>
</tr>
</tbody>
</table>

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

The DSM configuration is complete. If your DSM requires custom event properties, see the IBM Security Custom Event Properties for IBM z/OS technical note. (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf)

IBM DataPower

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

IBM DataPower is formerly known as IBM WebSphere® DataPower.

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

Table 314. IBM DataPower DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM Name</td>
<td>DataPower</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMDataPower-QRadar_version-build_number.noarch.rpm</td>
</tr>
</tbody>
</table>
Table 314. IBM DataPower DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported versions</td>
<td>FirmwareV6 and V7</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>All Events</td>
</tr>
<tr>
<td>Log source type in QRadar UI</td>
<td>IBM DataPower</td>
</tr>
<tr>
<td>Auto discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>For more information</td>
<td>IBM web page (<a href="http://www.ibm.com/">http://www.ibm.com/</a>)</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>IBM DataPower</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks

Adding a DSM
Configuring IBM DataPower to communicate with QRadar

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

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.

Configuring IBM DataPower to communicate with QRadar

To collect IBM DataPower events, configure your third-party system to send events to IBM 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 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Category</td>
<td>all</td>
</tr>
<tr>
<td>Minimum Event Priority</td>
<td>warning</td>
</tr>
</tbody>
</table>

**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.

---

**IBM DB2**

The IBM DB2 DSM collects events from an IBM DB2 mainframe that uses IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.

To collect IBM DB2 events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about prerequisite requirements, see the [IBM Security zSecure Suite 2.2.1 Prerequisites](http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html).

2. Configure your IBM DB2 image to write events in LEEF format. For more information, see the [IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide](http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).

3. Create a log source in QRadar for IBM DB2.

4. If you want to create a custom event property for IBM DB2 in QRadar, for more information, see the [IBM Security Custom Event Properties for IBM z/OS technical note](http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf).

**Before you begin**

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and
parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)

• You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
• If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
• If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.


Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:
• IBM z/OS
• IBM CICS
• IBM RACF
• IBM DB2
• CA Top Secret
• CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Select your DSM name from the list.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>

Creating a log source for Log File protocol

The Log File protocol enables IBM QRadar to retrieve archived log files from a remote host for the IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, and CA ACF2 DSM's.

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 z/OS
with zSecure writes log files to a specified directory as gzip archives. 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 that uses the Log File protocol. QRadar requires credentials to log in to the system that hosts your LEEF formatted event files and a polling interval.

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. In the **Log Source Name** field, type a name for the log source.
6. In the **Log Source Description** field, type a description for the log source.
7. From the **Log Source Type** list, select your DSM name.
8. From the **Protocol Configuration** list, select **Log File**.
9. Configure the Log File protocol parameters.

The following table describes the parameters that require specific values for the DSM event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested 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 that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify.</td>
</tr>
</tbody>
</table>
| **Service Type**                    | From the **Service Type** list, select the protocol that 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 that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled. |
<p>| <strong>Remote IP or Hostname</strong>           | Type the IP address or host name of the device that stores your event log files.                                                                                                               |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Port</td>
<td>Type the TCP port on the remote host that is running the selected <strong>Service Type</strong>. The valid range is 1 - 65535. The options include ports: • 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.</td>
</tr>
<tr>
<td>Remote User</td>
<td>Type the user name or user ID necessary to log in to the system that contains your event files. • If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length. • If your log files are 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.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Type the password necessary to log in to the host.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password necessary to log in to the host.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>If you select SCP or SFTP as the <strong>Service Type</strong>, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the <strong>Remote Password</strong> field is ignored.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>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.</td>
</tr>
<tr>
<td>Recursive</td>
<td>If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear. If you configure SCP as the Service Type, the Recursive option is ignored.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>If you select SFTP or FTP as the <strong>Service Type</strong>, you can configure the regular expression (regex) needed to filter the list of files that are specified in the <strong>Remote Directory</strong>. All matching files are included in the processing. The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <code>&lt;product_name&gt;..&lt;timestamp&gt;.gz</code> The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with zOS and end with .gz, type the following code: <code>zOS.*\.gz</code> Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions. (<a href="http://download.oracle.com/javase/tutorial/essential/regex/">http://download.oracle.com/javase/tutorial/essential/regex/</a>)</td>
</tr>
</tbody>
</table>
### Table 316. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FTP Transfer Mode</strong></td>
<td>This option displays only if you select <strong>FTP</strong> as the <strong>Service Type</strong>. From the list, select <strong>Binary</strong>. The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as <code>zip</code>, <code>gzip</code>, <code>tar</code>, or <code>tar+gzip</code> archive files.</td>
</tr>
<tr>
<td><strong>SCP Remote File</strong></td>
<td>If you select <strong>SCP</strong> as the <strong>Service Type</strong> you must type the file name of the remote file.</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>Type the time of day you want the processing to begin. For example, type <code>00:00</code> 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.</td>
</tr>
<tr>
<td><strong>Recurrence</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Run On Save</strong></td>
<td>If you want the Log File protocol to run immediately after you click <strong>Save</strong>, select this check box. 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.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>From the list, select <code>gzip</code>. Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in <code>zip</code>, <code>gzip</code>, <code>tar</code>, or <code>tar+gzip</code> archive format.</td>
</tr>
<tr>
<td><strong>Ignore Previously Processed File(s)</strong></td>
<td>Select this check box to track and ignore files that are already processed by the Log File protocol. QRadar examines the log files in the remote directory to determine whether a file is 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 are not previously processed are downloaded. This option applies only to FTP and SFTP service types.</td>
</tr>
</tbody>
</table>
Table 316. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Local Directory?</td>
<td>Select this check box to define a local directory on your QRadar for storing downloaded files during processing. It is suggested that you leave this check box clear. When this check box is selected, the <strong>Local Directory</strong> field is displayed, which gives you the option to configure the local directory to use for storing files.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the <strong>Event Generator</strong> list, select <strong>LineByLine</strong>. The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.</td>
</tr>
</tbody>
</table>

10. Click **Save**.

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

The DSM configuration is complete. If your DSM requires custom event properties, see the IBM Security Custom Event Properties for IBM z/OS technical note. (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf)

**Integrating IBM DB2 Audit Events**

The IBM DB2 DSM allows you to integrate your DB2 audit logs into IBM QRadar for analysis.

The `db2audit` command creates a set of comma-delimited text files with a .del extension that defines the scope of audit data for QRadar when auditing is configured and enabled. Comma-delimited files created by the `db2audit` command include:

- audit.del
- checking.del
- context.del
- execute.del
- objmaint.del
- secmaint.del
- sysadmin.del
- validate.del

To integrate the IBM DB2 DSM with QRadar, you must:

1. Use the `db2audit` command to ensure the IBM DB2 records security events. See your IBM DB2 vendor documentation for more information.
2. Extract the DB2 audit data of events contained in the instance to a log file, depending on your version of IBM DB2.
3. Use the Log File protocol source to pull the output instance log file and send that information back to QRadar on a scheduled basis. QRadar then imports and processes this file.

**Related tasks**

- “Extracting audit data for DB2 v8.x to v9.4” on page 561
- You can extract audit data when you are using IBM DB2 v8.x to v9.4.
- “Extracting audit data for DB2 v9.5” on page 561
You can extract audit data when you are using IBM DB2 v9.5.

Extracting audit data for DB2 v8.x to v9.4
You can extract audit data when you are using IBM DB2 v8.x to v9.4.

Procedure
1. Log into a DB2 account with SYSADMIN privilege.
2. Type the following start command to audit a database instance:
   
   \texttt{db2audit start}
   
   For example, the start command response might resemble the following output:
   
   \texttt{AUD00001 Operation succeeded.}
3. Move the audit records from the instance to the audit log:
   
   \texttt{db2audit flush}
   
   For example, the flush command response might resemble the following output:
   
   \texttt{AUD00001 Operation succeeded.}
4. Extract the data from the archived audit log and write the data to \texttt{.del} files:
   
   \texttt{db2audit extract delasc}
   
   For example, an archive command response might resemble the following output:
   
   \texttt{AUD00001 Operation succeeded.}
   
   \textbf{Note}: Double-quotation marks (" ) are used as the default text delimiter in the ASCII files, do not change the delimiter.
5. Remove non-active records:
   
   \texttt{db2audit prune all}
6. Move the \texttt{.del} files to a storage location where IBM QRadar can pull the file. The movement of the comma-delimited (\texttt{.del}) files should be synchronized with the file pull interval in QRadar.

   You are now ready to create a log source in QRadar to collect DB2 log files.

Extracting audit data for DB2 v9.5
You can extract audit data when you are using IBM DB2 v9.5.

Procedure
1. Log into a DB2 account with SYSADMIN privilege.
2. Move the audit records from the database instance to the audit log:
   
   \texttt{db2audit flush}
   
   For example, the flush command response might resemble the following output:
   
   \texttt{AUD00001 Operation succeeded.}
3. Archive and move the active instance to a new location for future extraction:
   
   \texttt{db2audit archive}
   
   For example, an archive command response might resemble the following output:
   
   \begin{verbatim}
   Node AUD Archived or Interim Log File Message
   ----------------------------------------------------------
   - 0 AUD00001 dsaudit.instance.log.0.20091217125028 AUD00001 Operation succeeded.
   \end{verbatim}
   
   \textbf{Note}: In DB2 v9.5 and later, the archive command replaces the prune command.
The archive command moves the active audit log to a new location, effectively pruning all non-active records from the log. An archive command must be complete before an extract can be executed.

4. Extract the data from the archived audit log and write the data to .del files:
   
   ```
   db2audit extract delasc from files db2audit.instance.log.0.200912171528
   ```
   
   For example, an archive command response might resemble the following output:
   
   ```
   AUD00001 Operation succeeded.
   ```
   
   **Note:** Double-quotation marks ("”) are used as the default text delimiter in the ASCII files, do not change the delimiter.

5. Move the .del files to a storage location where IBM QRadar can pull the file. The movement of the comma-delimited (.del) files should be synchronized with the file pull interval in QRadar.

   You are now ready to create a log source in QRadar to collect DB2 log files.

---

**IBM Federated Directory Server**

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

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM Federated Directory Server</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMIBM-Federated DirectoryServer-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V7.2.0.2 and later</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>FDS Audit</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

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 318. IBM Federated Directory Serve log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>IBM Federated Directory Server</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The source IP or host name of the IBM Federated Directory Server.</td>
</tr>
</tbody>
</table>

**Related tasks**

**Adding a DSM**

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

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.

**IBM Fiberlink MaaS360**

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

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

Table 319. IBM Fiberlink MaaS360 DSM Specification

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM Fiberlink MaaS360</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMFiberlinkMaaS360</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Table 319. IBM Fiberlink MaaS360 DSM Specification (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Compliance rule events</td>
</tr>
<tr>
<td></td>
<td>Device enrollment events</td>
</tr>
<tr>
<td></td>
<td>Action history events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Included identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Fiberlink MaaS360 website (<a href="http://www.maas360.com/">http://www.maas360.com/</a>)</td>
</tr>
</tbody>
</table>

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. Add an IBM Fiberlink MaaS360 log source on the QRadar Console.

**Related tasks**
“Adding a DSM” on page 4
“Adding a log source” on page 4

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

**Before you begin**
To enable IBM Fiberlink MaaS360 to communicate with QRadar, you must enable the REST API. Contact Fiberlink customer service to enable the REST API for your Fiberlink MaaS360 account.

**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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>The Log Source Identifier</td>
<td>The <strong>Log Source Identifier</strong> can be set to any valid value and does not need to reference a specific server. You can set the <strong>Log Source Identifier</strong> to the same value as the Log Source Name. If you have more than one IBM Fiberlink MaaS360 log source that is configured, you might want to identify the first log source as <em>fiberlink1</em>, the second log source as <em>fiberlink2</em>, and the third log source as <em>fiberlink3</em>.</td>
</tr>
<tr>
<td>Login URL</td>
<td>The URL for the Fiberlink MaaS360 REST server.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name that is used to access the MaaS360 APIs. Users with the following administrator roles can access the APIs: • Service Administrator • Administrator • Administrator-Level 2</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is used to access your MaaS360 APIs.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>The secret key that is provided by Fiberlink Customer Service when you enabled the REST API.</td>
</tr>
<tr>
<td>App ID</td>
<td>The App ID that was provided by Fiberlink Customer Service when you enabled the REST API.</td>
</tr>
<tr>
<td>Billing ID</td>
<td>The Billing ID for your Fiberlink MaaS360 account.</td>
</tr>
<tr>
<td>Platform</td>
<td>The platform version of the Fiberlink MaaS360 console.</td>
</tr>
<tr>
<td>App Version</td>
<td>The App Version of the application that corresponds to your REST API account.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses the Fiberlink MaaS360 API by using a proxy, select the <strong>Use Proxy</strong> check box. If the proxy requires authentication, configure the <strong>Proxy Server</strong>, <strong>Proxy Port</strong>, <strong>Proxy Username</strong>, and <strong>Proxy Password</strong> fields. If the proxy does not require authentication, configure the <strong>Proxy Server</strong> and <strong>Proxy Port</strong> fields.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>QRadar automatically downloads the server certificate and begins trusting the target server when the <strong>Yes</strong> option is selected.</td>
</tr>
</tbody>
</table>

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

IBM Guardium® is a database activity and audit tracking tool for system administrators to retrieve detailed auditing events across database platforms.

These instructions require that you install the 8.2p45 fix for InfoSphere® Guardium. For more information about this fix, see the Fix Central website at http://www.ibm.com/support/fixcentral/.

IBM QRadar collects informational, error, alert, and warnings from IBM Guardium by using syslog. IBM QRadar receives IBM Guardium Policy Builder events in the Log Event Extended Format (LEEF).

QRadar can only automatically discover and map events of the default policies that ship with IBM Guardium. Any user configured events that are required are displayed as unknowns in QRadar and you must manually map the unknown events.

Configuration overview

The following list outlines the process that is required to integrate IBM Guardium with QRadar.

1. Create a syslog destination for policy violation events. For more information, see “Creating a syslog destination for events” on page 566.
2. Configure your existing policies to generate syslog events. For more information, see “Configuring policies to generate syslog events” on page 567.
3. Install the policy on IBM Guardium. For more information, see “Installing an IBM Guardium Policy” on page 568.
4. Configure the log source in QRadar. For more information, see “Configuring a log source” on page 568.
5. Identify and map unknown policy events in QRadar. For more information, see “Creating an event map for IBM Guardium events” on page 569.

Creating a syslog destination for events

To create a syslog destination for these events on IBM Guardium, you must log in to the command line interface (CLI) and define the IP address for IBM QRadar.

Procedure

1. Using SSH, log in to IBM Guardium as the default user.
   Username: <username>
   Password: <password>
2. Type the following command to configure the syslog destination for informational events:
   `store remote add daemon.info <IP address>:<port> <tcp|udp>`
   For example,
   `store remote add daemon.info <IP_address> tcp`
   Where:
   • `<IP address>` is the IP address of your QRadar Console or Event Collector.
   • `<port>` is the syslog port number that is used to communicate to the QRadar Console or Event Collector.
   • `<tcp|udp>` is the protocol that is used to communicate to the QRadar Console or Event Collector.
3. Type the following command to configure the syslog destination for warning events:
   `store remote add daemon.warning <IP address>:<port> <tcp|udp>`
   Where:
• `<IP address>` is the IP address of your QRadar Console or Event Collector.
• `<port>` is the syslog port number that is used to communicate to the QRadar Console or Event Collector.
• `<tcp|udp>` is the protocol that is used to communicate to the QRadar Console or Event Collector.

4. Type the following command to configure the syslog destination for error events:

   ```
   store remote add daemon.err `<IP address>`:<port> `<tcp|udp`
   ```

   Where:
   • `<IP address>` is the IP address of your QRadar Console or Event Collector.
   • `<port>` is the syslog port number that is used to communicate to the QRadar Console or Event Collector.
   • `<tcp|udp>` is the protocol that is used to communicate to the QRadar Console or Event Collector.

5. Type the following command to configure the syslog destination for alert events:

   ```
   store remote add daemon.alert `<IP address>`:<port> `<tcp|udp`
   ```

   Where:
   • `<IP address>` is the IP address of your QRadar Console or Event Collector.
   • `<port>` is the syslog port number that is used to communicate to the QRadar Console or Event Collector.
   • `<tcp|udp>` is the protocol that is used to communicate to the QRadar Console or Event Collector.

You are now ready to configure a policy for IBM InfoSphere Guardium.

### Configuring policies to generate syslog events

Policies in IBM Guardium are responsible for reacting to events and forwarding the event information to IBM QRadar.

**Procedure**

1. Click the **Tools** tab.
2. From the left navigation, select **Policy Builder**.
3. From the **Policy Finder** pane, select an existing policy and click **Edit Rules**.
4. Click **Edit this Rule individually**.
   
   The **Access Rule Definition** is displayed.
5. Click **Add Action**.
6. From the **Action** list, select one of the following alert types:
   • **Alert Per Match** - A notification is provided for every policy violation.
   • **Alert Daily** - A notification is provided the first time a policy violation occurs that day.
   • **Alert Once Per Session** - A notification is provided per policy violation for unique session.
   • **Alert Per Time Granularity** - A notification is provided per your selected time frame.
7. From the **Message Template** list, select QRadar.
8. From **Notification Type**, select **SYSLOG**.
9. Click **Add**, then click **Apply**.
10. Click **Save**.
11. Repeat “Configuring policies to generate syslog events” on page 567 for all rules within the policy that you want to forward to QRadar.

For more information on configuring a policy, see your *IBM InfoSphere Guardium* vendor documentation. After you have configured all of your policies, you are now ready to install the policy on your IBM Guardium system.
**Note:** Due to the configurable policies, QRadar can only automatically discover the default policy events. If you have customized policies that forward events to QRadar, you must manually create a log source to capture those events.

### Installing an IBM Guardium Policy

Any new or edited policy in IBM Guardium must be installed before the updated alert actions or rule changes can occur.

**Procedure**

1. Click the **Administration Console** tab.
2. From the left navigation, select **Configuration > Policy Installation**.
3. From the **Policy Installer** pane, select a policy that you modified in “Configuring policies to generate syslog events” on page 567.
4. From the drop-down list, select **Install and Override**.
   - A confirmation is displayed to install the policy to all Inspection Engines.
5. Click **OK**.

   For more information on installing a policy, see your *IBM InfoSphere Guardium* vendor documentation.

After you install all of your policies, you are ready to configure the log source in IBM QRadar.

### Configuring a log source

IBM QRadar only automatically discovers default policy events from IBM Guardium.

**About this task**

Because of the configurable nature of policies, it is suggested that you configure a log source manually for IBM Guardium.

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. In the **Log Source Name** field, type a name for the log source.
6. In the **Log Source Description** field, type a description for the log source.
7. From the **Log Source Type** list, select **IBM Guardium**.
8. From the **Protocol Configuration** list, select **Syslog**.
9. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the IBM InfoSphere Guardium appliance.</td>
</tr>
</tbody>
</table>

10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.
Creating an event map for IBM Guardium events

Event mapping is required for a number of IBM Guardium events. Due to the customizable nature of policy rules, most events, except the default policy events do not contain a predefined IBM QRadar Identifier (QID) map to categorize security events.

About this task

You can individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track recurring events from your network devices. Until you map an event, all events that are displayed in the Log Activity tab for IBM Guardium are categorized as unknown. Unknown events are easily identified as the Event Name column and Low Level Category columns display Unknown.

As your device forwards events to QRadar, it can take time to categorize all of the events for a device, as some events might not be generated immediately by the event source appliance or software. It is helpful to know how to quickly search for unknown events. When you know how to search for unknown events, we suggest that you repeat this search until you are satisfied that most of your events are identified.

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 the log source group or Other.
   
   Log sources that are not assigned to a group are categorized as Other.
6. From the Log Source list, select your IBM Guardium log source.
7. Click Add Filter.
   
   The Log Activity tab is displayed with a filter for your log source.
8. From the View list, select Last Hour.
   
   Any events that are generated by the IBM Guardium DSM in the last hour are displayed. Events that are displayed as unknown in the Event Name column or Low Level Category column require event mapping in QRadar.

   Note: You can save your existing search filter by clicking Save Criteria.

   You are now ready to modify the event map.

Modifying the event map

Modifying an event map allows for the manual categorization of events to a IBM QRadar Identifier (QID) map. Any event that is categorized to a log source can be remapped to a new QRadar Identifier (QID).

About this task

IBM Guardium event map events that do not have a defined log source cannot be mapped to an event. Events without a log source display SIM Generic Log in the Log Source column.

Procedure

1. On the Event Name column, double-click an unknown event for IBM Guardium.
   
   The detailed event information is displayed.
2. Click Map Event.
3. 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 categorization.
• For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the IBM QRadar Administration Guide.

• From the **Low-Level Category** list, select a low-level event categorization.

• From the **Log Source Type** list, select a log source type.

The **Log Source Type** list gives the option to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, IBM Guardium provides policy events, you might select another product that likely captures similar events.

4. To search for a QID by name, type a name in the **QID/Name** field.

The **QID/Name** field gives the option to filter the full list of QIDs for a specific word, for example, policy.

5. Click **Search**.

A list of QIDs are displayed.

6. Select the QID you want to associate to your unknown event.

7. Click **OK**.

QRadar maps any additional events that are forwarded from your device with the same QID that matches the event payload. The event count increases each time that the event is identified by QRadar.

If you update an event with a new QRadar Identifier (QID) map, past events that are stored in QRadar are not updated. Only new events are categorized with the new QID.

**IBM IMS**

The IBM Information Management System (IMS) DSM for IBM QRadar allows you to use an IBM mainframe to collect events and audit IMS database transactions.

To integrate IBM IMS events with QRadar, you must download scripts that allow IBM IMS events to be written to a log file.

**Overview of the event collection process:**

1. The IBM mainframe records all security events as Service Management Framework (SMF) records in a live repository.

2. The IBM IMS data is extracted from the live repository using the SMF dump utility. The SMF file contains all of the events and fields from the previous day in raw SMF format.

3. The `qeximsloadlib.trs` program pulls data from the SMF formatted file. The `qeximsloadlib.trs` program only pulls the relevant events and fields for QRadar and writes that information in a condensed format for compatibility. The information is saved in a location accessible by QRadar.

4. QRadar uses the log file protocol source to retrieve the output file information for QRadar on a scheduled basis. QRadar then imports and processes this file.

**Configuring IBM IMS**

You can integrate IBM IMS with QRadar:

**Procedure**

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

   QexIMS_bundled.tar.gz

2. On a Linux-based operating system, extract the file:

   `tar -zxvf qexims_bundled.tar.gz`
The following files are contained in the archive:

- qexims_jcl.txt - Job Control Language file
- qeximsloadlib.trs - Compressed program library (requires IBM TRSMAIN)
- qexims_trsmain_JCL.txt - Job Control Language for TRSMAIN to decompress the .trs file

3. Load the files onto the IBM mainframe by using the following methods:

   Upload the sample qexims_trsmain_JCL.txt and qexims_jcl.txt files by using the TEXT protocol.

4. Upload the qeximsloadlib.trs file by using BINARY mode transfer and append to a pre-allocated data set. The qeximsloadlib.trs file is a tersed file that contains the executable (the mainframe program QexIMS). 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.

   **Note:** QexIMS is a small C mainframe program that reads the output of the IMS log file (EARLOUT data) line by line. QexIMS adds a header to each record that contains event information, for example, record descriptor, the date, and time. The program places each field into the output record, suppresses trailing blank characters, and delimits each field with the pipe character. This output file is formatted for QRadar and the blank suppression reduces network traffic to QRadar. This program does not need much CPU or I/O disk resources.

5. Customize the qexims_trsmain_JCL.txt file according to your installation-specific information for parameters.

   For example, jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

   The qexims_trsmain_JCL.txt file uses the IBM utility TRSMAIN to extract the program that is stored in the qeximsloadlib.trs file.

   An example of the qexims_trsmain_JCL.txt file includes:

   ```
   //TRSMAIN JOB (yourvalidjobcard),Q11abs, // MSGCLASS=V //DEL EXEC PGM=IEFBR14 //D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXIMS.TRS // UNIT=SYSDA, // SPACE=(CYL,(10,10)) //TRSMAIN EXEC PGM=TRSMAIN, PARM='UNPACK' //SYSPRINT DD SYSOUT=* //DCB=(LRECL=133,RECFM=FBA) //INFILE DD DISP=SHR,DSN=<yourhlq>.QEXIMS.TRS //OUTFILE DD DISP=(NEW,CATLG,DELETE), // DSN=<yourhlq>.LOAD, // SPACE=(CYL,(1,1,5),RLSE),UNIT=SYSDA
   ```

   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 qexims program as a member.

6. You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in LINKLST. The program does not require authorization.

7. The qexims_jcl.txt file is a text file that contains a sample JCL. You must configure the job card to meet your configuration.

   The qexims_jcl.txt sample file includes:

   ```
   //QEXIMS JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK, // MSGCLASS=P, // REGION=6M // /*QEXIMS JCL VERSION 1.0 FEBRUARY 2011 */ //*************************************************************** // Change dataset names to site specific dataset names */ //*************************************************************** //*************************************************************** /********** SET IMSOUT='Q1JACK. QEXIMS.OUTPUT', // IMSIN='Q1JACK. QEXIMS. INPUT. DATA' //*************************************************************** //*************************************************************** /********** Delete old datasets */
   ```

Chapter 79. IBM 571
8. After the output file is created, you must make one of the following choices:

- Schedule a job to transfer the output file to an interim FTP server.
- Each time the job completes, the output file is forwarded to an interim FTP server. You must configure the following parameters in the sample JCL to successfully forward the output to an interim FTP server:

For example:

```sql
//*FTP EXEC PGM=FTP,REGION=3800K /*INPUT DD *
//<<target server>
//<<USER>
//<<PASSWORD>> //ASCII /*PUT '<IMSOUT>' /TARGET DIRECTORY>/IMSOUT
//QUIT /*OUTPUT DD SYSOUT=* /*SYSPRINT DD SYSOUT=* /*
```

Where:
- `<target server>` is the IP address or host name of the interim FTP server to receive the output file.
- `<USER>` is the user name required to access the interim FTP server.
- `<PASSWORD>` is the password required to access the interim FTP server.
- `<IMSOUT>` is the name of the output file saved to the interim FTP server.

For example:

PUT 'Q1JACK.QEXIMS.OUTPUT.C320' /192.0.2.1/IMS/QEXIMS.OUTPUT.C320

**Note:** You must remove commented lines that begin with `/*` for the script to properly forward the output file to the interim FTP server.

You are now ready to configure the log file protocol.

9. Schedule QRadar to retrieve the output file from IBM IMS.

If the mainframe is configured to serve files through FTP, SFTP, or allow SCP, then no interim FTP server is required and QRadar can pull the output file directly from the mainframe. The following text must be commented out using `/*` or deleted from the `qexims_jcl.txt` file:

```sql
//*FTP EXEC PGM=FTP,REGION=3800K /*INPUT DD *
//<<target server>
//<<USER> //<<PASSWORD>> //ASCII /*PUT '<IMSOUT>' /TARGET DIRECTORY>/IMSOUT
//QUIT /*OUTPUT DD SYSOUT=* /*SYSPRINT DD SYSOUT=* /*
```
You are now ready to configure the log file protocol.

**Configuring a log source**

A log file protocol source allows IBM QRadar to retrieve archived log files from a remote host.

**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 IBM IMS.
5. Using the **Protocol Configuration** list, select **Log File**.
6. Configure the following parameters:

<table>
<thead>
<tr>
<th>Table 321. Log file protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Service Type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
</tr>
<tr>
<td>Remote Port</td>
</tr>
<tr>
<td>Remote User</td>
</tr>
<tr>
<td>Remote Password</td>
</tr>
<tr>
<td>Confirm Password</td>
</tr>
<tr>
<td>SSH Key File</td>
</tr>
<tr>
<td>Remote Directory</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>Recursive</td>
</tr>
<tr>
<td>FTP File Pattern</td>
</tr>
<tr>
<td>FTP Transfer Mode</td>
</tr>
<tr>
<td>SCP Remote File</td>
</tr>
<tr>
<td>Start Time</td>
</tr>
<tr>
<td>Recurrence</td>
</tr>
<tr>
<td>Run On Save</td>
</tr>
<tr>
<td>EPS Throttle</td>
</tr>
</tbody>
</table>
### Table 321. Log file protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>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 the contents to be processed.</td>
</tr>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>Select this check box to track files that are processed and you do not want the files to be processed a second time. This applies only to FTP and SFTP Service Types.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>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 gives the option to configure the local directory to use for storing files.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the Event Generator list, select LineByLine.</td>
</tr>
</tbody>
</table>

7. Click Save.

The configuration is complete. Events that are retrieved by using the log file protocol are displayed on the Log Activity tab of QRadar.

## IBM Informix Audit

The IBM Informix® Audit DSM allows IBM QRadar to integrate IBM Informix audit logs into QRadar for analysis.

QRadar retrieves the IBM Informix archived audit log files from a remote host using the log file protocol configuration. QRadar records all configured IBM Informix Audit events.

When configuring your IBM Informix to use the log file protocol, make sure the host name or IP address configured in the IBM Informix is the same as configured in the Remote Host parameter in the log file protocol configuration.

You are now ready to configure the log source and protocol in QRadar:

- To configure QRadar to receive events from an IBM Informix device, you must select the IBM Informix Audit option from the Log Source Type list.
- To configure the log file protocol, you must select the Log File option from the Protocol Configuration list.

Use a secure protocol for transferring files, such as Secure File Transfer Protocol (SFTP).

**Related concepts**

“Log File protocol configuration options” on page 62

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

**Related tasks**

“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**IBM Lotus Domino**

You can integrate an IBM Lotus® Domino® device with IBM QRadar. An IBM Lotus Domino device accepts events by using SNMP.

**Setting Up SNMP Services**

To set up the SNMP services on the IBM Lotus Domino server:

**Procedure**

1. Install the Lotus Domino SNMP Agent as a service. From the command prompt, go to the Lotus \Domino directory and type the following command:
   
   Insnmp -SC

2. Confirm that the Microsoft SNMP service is installed.

3. Start the SNMP and LNSNMP services. From a command prompt, type the following commands:
   
   • net start snmp
   
   • net start lnsnmp

4. Select **Start > Program > Administrative Tools > Services** to open the **Services MMC**

5. Double-click on the **SNMP** service and select the **Traps** tab.

6. In the **Community name** field, type **public** and click **add to list**.

7. In the **Traps destinations** section, select **Add** and type the IP address of your IBM QRadar. Click **Add**.

8. Click **OK**.

9. Confirm that both SNMP agents are set to **Automatic** so they run when the server boots.

**Setting up SNMP in AIX**

**Before you begin**

Make sure TCP/IP and SNMP are properly installed and configured on the server.

You must log in as a root user.

**Procedure**

1. Stop the LNSNMP service with the following command:
   
   lnsnmp.sh stop

2. Stop the SNMP subsystem with the following command:
   
   stopsrc -s snmpd

3. Configure SNMP to accept LNSNMP as an SMUX peer. Add the following line to `/etc/snmpd.peers`
   
   "Lotus Notes Agent" 1.3.6.1.4.1.334.72 "NotesPasswd"

4. Configure SNMP to accept an SMUX association from LNSNMP. Add the following line to `/etc/` snmpd.conf or `/etc/snmpdv3.conf`
   
   smux 1.3.6.1.4.1.334.72 NotesPasswd

5. Start the SNMP subsystem with the following command:
   
   startsrc -s snmpd

6. Start the LNSNMP service with the following command:
   
   lnsnmp.sh start
7. Create a link to the LNSNMP script
   
   ```
   ln -f -s /opt/ibm/lotus/notes/latest/ibmpow/lnsnmp.sh /etc/lnsnmp.rc
   ```

8. Configure LNSNMP service to start during the system restart. Add the following line to the end of `/etc/rc.tcpip`
   
   ```
   /etc/lnsnmp.rc start
   ```

**Starting the Domino Server Add-in Tasks**

After you configure the SNMP services, you must start the Domino server add-in tasks.

**About this task**

Use the following procedure for each Domino partition.

**Procedure**

1. Log in to the Domino Server console.
2. To support SNMP traps for Domino events, type the following command to start the Event Interceptor add-in task:
   
   ```
   load intrcpt
   ```
3. To support Domino statistic threshold traps, type the following command to start the Statistic Collector add-in task:
   
   ```
   load collect
   ```
4. Arrange for the add-in tasks to be restarted automatically the next time that Domino is restarted. Add `intrcpt` and `collect` to the `ServerTasks` variable in Domino's `NOTES.INI` file.

**Configuring SNMP Services**

You can configure SNMP services:

**About this task**

Configurations might vary depending on your environment. See your vendor documentation for more information.

**Procedure**

1. Open the Domino Administrator utility and authenticate with administrative credentials.
2. Click the `Files` tab, and the `Monitoring Configuration` (`events4.nsf`) document.
3. Expand the `DDM Configuration` Tree and select `DDM Probes By Type`.
4. Select `Enable Probes`, and then select `Enable All Probes In View`.
   
   **Note:** You might receive a warning when you complete this action. This warning is a normal outcome, as some of the probes require more configuration.
5. Select `DDM Filter`.
   
   You can either create a new DDM Filter or edit the existing DDM Default Filter.
6. Apply the DDM Filter to enhanced and simple events. Choose to log all event types.
7. Depending on the environment, you can choose to apply the filter to all servers in a domain or only to specific servers.
8. Click `Save`. Close when finished.
9. Expand the `Event Handlers` tree and select `Event Handlers By Server`.
10. Select `New Event Handler`.
11. Configure the following parameters:
- **Basic - Servers to monitor**: Choose to monitor either all servers in the domain or only specific servers.
- **Basic - Notification trigger**: Any event that matches the criteria.
- **Event - Criteria to match**: Events can be any type.
- **Event - Criteria to match**: Events must be one of these priorities (Check all the boxes).
- **Event - Criteria to match**: Events can have any message.
- **Action - Notification method**: SNMP Trap.
- **Action - Enablement**: Enable this notification.

12. Click **Save**. Close when finished.

You are now ready to configure the log source in IBM QRadar.

**Configuring your IBM Lotus Domino device to communicate with QRadar**

IBM QRadar does not automatically discover incoming syslog events from your IBM Lotus Domino device.

**About this task**

You must manually create a log source from the **Admin** tab in QRadar.

**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 Lotus Domino.
6. From the **Protocol Configuration** list, select **SNMPv2**.
7. Configure the following values:

<table>
<thead>
<tr>
<th><strong>Table 322: SNMPv2 protocol parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Community</td>
</tr>
<tr>
<td>Include OIDs in Event Payload</td>
</tr>
</tbody>
</table>

8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.
IBM Privileged Session Recorder

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>Privileged Session Recorder</td>
</tr>
<tr>
<td>RPM filename</td>
<td>DSM-IBMPrivilegedSessionRecorder</td>
</tr>
<tr>
<td>Protocol</td>
<td>JDBC</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Command Execution Audit Events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>IBM website (<a href="http://www.ibm.com/">http://www.ibm.com/</a>)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>IBM Privileged Session Recorder</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>DATABASE@HOSTNAME</td>
</tr>
<tr>
<td>Database Type</td>
<td>DB2</td>
</tr>
<tr>
<td>Database Name</td>
<td>The Session Recorder data store name that you configured on the IBM Privileged Identity Manager dashboard.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The Session Recorder database server address.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that is specified on IBM Privileged Identity Manager dashboard.</td>
</tr>
<tr>
<td>Username</td>
<td>The DB2 database user name</td>
</tr>
<tr>
<td>Password</td>
<td>The DB2 database password</td>
</tr>
</tbody>
</table>
### Table 324. IBM Privileged Session Recorder log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined Query</td>
<td>IBM Privileged Session Recorder</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>This option must be selected.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>The initial date and time for the JDBC retrieval.</td>
</tr>
</tbody>
</table>

**Related tasks**

Adding a DSM  
Configuring IBM Privileged Session Recorder to communicate with QRadar  
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.

**Configuring IBM Privileged Session Recorder to communicate with QRadar**

Before you can configure a log source in IBM Privileged Session Recorder for IBM 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. Record the following parameters to use when you configure a log source in QRadar:

<table>
<thead>
<tr>
<th>IBM Privileged Session Recorder Field</th>
<th>QRadar Log Source Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>IP or Hostname</td>
</tr>
<tr>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td>Database name</td>
<td>Database Name</td>
</tr>
<tr>
<td>Database administrator ID</td>
<td>Username</td>
</tr>
</tbody>
</table>

**Configuring a log source for IBM Privileged Session Recorder**

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

**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 Name** field, type a name for your log source.
7. From the **Log Source Type** list, select **IBM Privileged Session Recorder**.
8. From the **Protocol Configuration** list, select **JDBC**.
9. Configure the parameters for the log source. These parameters are found in `c_logsource_JDBCprotocol.dita#concept_p1k_ln3_gn`.

10. Click **Save**.

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

**Related information**

`c_logsource_JDBCprotocol.dita#concept_p1k_ln3_gn`

---

**IBM Proventia**

IBM QRadar supports a number of IBM Proventia DSMs.

Several IBM Proventia DSMs are supported by QRadar:

**IBM Proventia Management SiteProtector**

The IBM Proventia® Management SiteProtector DSM for IBM QRadar accepts SiteProtector events by polling the SiteProtector database.

The DSM allows QRadar to record Intrusion Prevention System (IPS) events and audit events directly from the IBM SiteProtector database.

**Note:** The IBM Proventia Management SiteProtector DSM requires the latest JDBC Protocol to collect audit events.

The IBM Proventia Management SiteProtector DSM for IBM QRadar can accept detailed SiteProtector events by reading information from the primary SensorData1 table. The SensorData1 table is generated with information from several other tables in the IBM SiteProtector database. SensorData1 remains the primary table for collecting events.

IDP events include information from SensorData1, along with information from the following tables:

- SensorDataAVP1
- SensorDataReponse1

Audit events include information from the following tables:

- AuditInfo
- AuditTrail

Audit events are not collected by default and make a separate query to the AuditInfo and AuditTrail tables when you select the **Include Audit Events** check box. For more information about your SiteProtector database tables, see your vendor documentation.

Before you configure QRadar to integrate with SiteProtector, we suggest that you create a database user account and password in SiteProtector for QRadar.

Your QRadar user must have read permissions for the SensorData1 table, which stores SiteProtector events. The JDBC - SiteProtector protocol allows QRadar to log in and poll for events from the database. Creating a QRadar account is not required, but it is recommended for tracking and securing your event data.

**Note:** Ensure that no firewall rules are blocking the communication between the SiteProtector console and QRadar.

**Configuring a log source in QRadar to collect IBM Proventia Management SiteProtector events**

Configure IBM QRadar to collect IBM Proventia Management SiteProtector events by using the JDBC protocol.

**Procedure**

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Click **Add**.
4. Configure the parameters. The following table describes the parameters that require specific values to collect event from IBM Proventia Management SiteProtector:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>(Optional)</td>
<td></td>
</tr>
<tr>
<td>Log Source Type</td>
<td>IBM Proventia Management SiteProtector</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be</td>
</tr>
<tr>
<td></td>
<td>unique among all log sources of the log source type that is configured to</td>
</tr>
<tr>
<td></td>
<td>use the JDBC protocol.</td>
</tr>
<tr>
<td></td>
<td>If the log source collects events from a single appliance that has a</td>
</tr>
<tr>
<td></td>
<td>static IP address or host name, use the IP address or host name of the</td>
</tr>
<tr>
<td></td>
<td>appliance as all or part of the Log Source Identifier value; for example,</td>
</tr>
<tr>
<td></td>
<td>192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect</td>
</tr>
<tr>
<td></td>
<td>events from a single appliance that has a static IP address or host name,</td>
</tr>
<tr>
<td></td>
<td>you can use any unique name for the Log Source Identifier value; for</td>
</tr>
<tr>
<td></td>
<td>example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>From the list, select <strong>MSDE</strong> as the type of database to use for the event</td>
</tr>
<tr>
<td></td>
<td>source.</td>
</tr>
<tr>
<td>Database Name</td>
<td>The name of the database to which you want to connect.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>Type the IP address or host name of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number that is used by the database server. The default port</td>
</tr>
<tr>
<td></td>
<td>for MSDE is 1433. You must enable and verify that you can communicate by</td>
</tr>
<tr>
<td></td>
<td>using the port that you specified in the <strong>Port</strong> field.</td>
</tr>
<tr>
<td></td>
<td>The JDBC configuration port must match the listener port of the IBM</td>
</tr>
<tr>
<td></td>
<td>Proventia database. To be able to communicate with QRadar, the IBM</td>
</tr>
<tr>
<td></td>
<td>Proventia database must have incoming TCP connections enabled.</td>
</tr>
<tr>
<td></td>
<td>If you define a database instance that uses MSDE as the database type,</td>
</tr>
<tr>
<td></td>
<td>you must leave the <strong>Port</strong> parameter blank in your configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the database user name. The user name can be up to 255 alphanumeric</td>
</tr>
<tr>
<td></td>
<td>characters in length. The user name can also include underscores (_).</td>
</tr>
<tr>
<td>Password</td>
<td>Type the database password.</td>
</tr>
<tr>
<td></td>
<td>The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password to access the database.</td>
</tr>
</tbody>
</table>
### Table 325. IBM Proventia Management SiteProtector JDBC protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Authentication Domain**| If you did not select **Use Microsoft JDBC, Authentication Domain** is displayed.  
The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.  
The authentication domain must contain alphanumeric characters. The domain can include the following special characters: underscore (_), en dash (-), and period(.) |
| **Database Instance**    | The database instance, if required. MSDE databases can include multiple SQL server instances on one server.  
When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the **Database Instance** parameter must be blank in the log source configuration. |
| **Predefined Query**     | Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the **none** option. |
| **Table Name**           | Type the name of the view that includes the event records. The default table name is SensorData1. |
| **Select List**          | Type * to include all fields from the table or view.  
You can use a comma-separated list to define specific fields from tables or views, if needed for your configuration. The list must contain the field that is defined in the **Compare Field** parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.). |
| **Compare Field**        | Type SensorDataRowID to identify new events added between queries to the table. |
| **Use Prepared Statements** | Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements. |
| **Start Date and Time**  | Type the start date and time for database polling in the following format: 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. |
| **Polling Interval**     | Type the polling interval, which 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 without an H or M designator poll in seconds. |
| **EPS Throttle**         | The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000. |
Table 325. IBM Proventia Management SiteProtector JDBC protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Named Pipe Communication</td>
<td>If you did not select Use Microsoft JDBC, Use Named Pipe Communication is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>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 to ensure Named Pipe communication functions properly.</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select Use Microsoft JDBC, Use NTLMv2 is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable Use Microsoft JDBC.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option if your connection supports SSL. This option appears only for MSDE.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected Use Microsoft JDBC and Use SSL, the Microsoft SQL Server Hostname parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC parameters, see c_logsource_JDBCprotocol.dita

5. Click Save.
6. On the Admin tab, click Deploy Changes.

IBM ISS Proventia

The IBM Integrated Systems Solutions® (ISS) Proventia DSM for IBM QRadar records all relevant IBM Proventia® events by using SNMP.

Procedure

1. In the Proventia Manager user interface navigation pane, expand the System node.
2. Select System.
   The Service Configuration page is displayed.
4. Click the SNMP tab.
5. Select SNMP Traps Enabled.
6. In the Trap Receiver field, type the IP address of your QRadar you want to monitor incoming SNMP traps.
7. In the Trap Community field, type the appropriate community name.
8. From the Trap Version list, select the trap version.
9. Click Save Changes.

You are now ready to configure QRadar to receive SNMP traps.

10. To configure QRadar to receive events from an ISS Proventia device. From the Log Source Type list, select IBM Proventia Network Intrusion Prevention System (IPS).

For more information about your ISS Proventia device, see your vendor documentation.

Related concepts
“SNMPv2 protocol configuration options” on page 83
You can configure a log source to use the SNMPv2 protocol to receive SNMPv2 events.

“SNMPv3 protocol configuration options” on page 83
You can configure a log source to use the SNMPv3 protocol to receive SNMPv3 events.

IBM QRadar Packet Capture

The IBM QRadar DSM for IBM QRadar Packet Capture collects events from an IBM Security Packet Capture device.

The following table describes the specifications for the IBM QRadar Packet Capture DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM QRadar Packet Capture</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMQRadarPacketCapture-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>IBM QRadar Packet Capture V7.2.3 to V7.2.7</td>
</tr>
<tr>
<td></td>
<td>IBM QRadar Network Packet Capture V7.3.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>IBM QRadar Network Packet Capture knowledge center (<a href="https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/kc_gen/toc-gen43.html">https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/kc_gen/toc-gen43.html</a>)</td>
</tr>
</tbody>
</table>

To integrate IBM QRadar Packet Capture 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
2. Configure your IBM QRadar Packet Capture device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add an IBM QRadar Packet Capture log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from IBM QRadar Packet Capture:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>IBM QRadar Packet Capture</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

4. To verify that QRadar is configured correctly, review the following tables to see examples of parsed event messages.

The following table shows a sample event message from IBM QRadar Packet Capture:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Added</td>
<td>User Account Added</td>
<td>May 10 00:01:04 &lt;Server&gt; LEEF: 2.0</td>
</tr>
</tbody>
</table>

The following table shows a sample event message from IBM QRadar Network Packet Capture:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Capture Statistics</td>
<td>Information</td>
<td>&lt;14&gt;Mar 1 20:39:41 &lt;Server&gt; LEEF: 2.0</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 QRadar Packet Capture to communicate with QRadar
To collect IBM QRadar Packet Capture events, you must configure event forwarding to a remote syslog server.

Procedure
1. Using SSH, log in to your IBM QRadar Packet Capture device as the root user.
2. Choose one of the following options to enable syslog.
a) Option 1: Open the `/etc/rsyslog.conf` file in a text editor such as `vi`:

```
vi /etc/rsyslog.conf
```

Then add the following line at the end of the file:

```
*.* @@<QRadar Event collector IP>:514
```

b) Option 2: Create the `<filename>.conf` file in the `/etc/rsyslog.d/` directory, and then add the following line to the file that you created:

```
*.* @@<QRadar Event collector IP>:514
```

3. Restart the Syslog service by typing the following command:

```
service rsyslog restart
```

The message logs are sent to the QRadar Event Collector and local copies are saved.

**Note:** QRadar parses only LEEF events for IBM QRadar Packet Capture. On the Log Activity tab in QRadar, the Event Name displays as IBM QRadar Packet Capture Message and the Low Level Category displays as Stored for all other events.

**What to do next**
To verify that LEEF events are being logged on your IBM QRadar Packet Capture device, inspect `/var/log/messages`.

```
tail /var/log/messages
```

**Configuring IBM QRadar Network Packet Capture to communicate with QRadar**

To collect IBM QRadar Network Packet Capture events, you must configure a remote Syslog server for your IBM QRadar Network Packet Capture appliance.

**Procedure**
1. Log in to your IBM QRadar Network Packet Capture appliance as administrator.
2. Click **Admin**.
3. In the REMOTE SYSLOG SETUP pane, enable system logging.
4. Enable the UPD or TCP protocol, depending on your transfer settings.
5. In the Remote Syslog Server Port field, type the port number that you want to use to send remote syslog events. The default port number for remote syslog is 514.
6. In the Remote Syslog Server field, type the IP address for your QRadar Event Collector to which you want to send events.
7. Click **Apply**.

**Note:** QRadar parses only LEEF events for IBM QRadar Network Packet Capture. On the Log Activity tab in QRadar, the Event Name displays as IBM QRadar Packet Capture Message and the Low Level Category displays as Stored for all other events.

**IBM RACF**

The IBM RACF DSM collects events from an IBM z/OS mainframe by using IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.
To collect IBM RACF events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html).

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 (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).

3. Create a log source in QRadar for IBM RACF.


Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.


Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 log source for Log File protocol

The Log File protocol enables IBM QRadar to retrieve archived log files from a remote host for the IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, and CA ACF2 DSM's.

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 z/OS
with zSecure writes log files to a specified directory as gzip archives. 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 that uses the Log File protocol. QRadar requires credentials to log in to the system that hosts your LEEF formatted event files and a polling interval.

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. In the **Log Source Name** field, type a name for the log source.
6. In the **Log Source Description** field, type a description for the log source.
7. From the **Log Source Type** list, select your DSM name.
8. From the **Protocol Configuration** list, select **Log File**.
9. Configure the Log File protocol parameters.

The following table describes the parameters that require specific values for the DSM event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested 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 that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify.</td>
</tr>
<tr>
<td><strong>Service Type</strong></td>
<td>From the <strong>Service Type</strong> list, select the protocol that 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 that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the <strong>Remote IP or Hostname</strong> field has the SFTP subsystem enabled.</td>
</tr>
<tr>
<td><strong>Remote IP or Hostname</strong></td>
<td>Type the IP address or host name of the device that stores your event log files.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Remote Port       | Type the TCP port on the remote host that is running the selected **Service Type**. The valid range is 1 - 65535. The options include ports:  
• 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. |
| Remote User       | Type the user name or user ID necessary to log in to the system that contains your event files.  
• If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length.  
• If your log files are 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 gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.              |
| 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.                                                            |
| Recursive         | If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear.  
If you configure SCP as the Service Type, the Recursive option is ignored. |
| FTP File Pattern  | If you select SFTP or FTP as the **Service Type**, you can configure the regular expression (regex) needed to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing.  
The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: `<product_name>.<timestamp>.gz`  
The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with zOS and end with .gz, type the following code:  
zOS.*\.*gz  
Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions. (http://download.oracle.com/javase/tutorial/essential/regex/) |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FTP Transfer Mode</strong></td>
<td>This option displays only if you select <strong>FTP</strong> as the <strong>Service Type</strong>. From the list, select <strong>Binary</strong>.</td>
</tr>
<tr>
<td></td>
<td>The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as <strong>zip</strong>, <strong>gzip</strong>, <strong>tar</strong>, or <strong>tar+gzip</strong> archive files.</td>
</tr>
<tr>
<td><strong>SCP Remote File</strong></td>
<td>If you select SCP as the <strong>Service Type</strong> you must type the file name of the remote file.</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>Type the time of day you want the processing to begin. For example, type <strong>00:00</strong> to schedule the Log File protocol to collect event files at midnight.</td>
</tr>
<tr>
<td></td>
<td>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: <strong>HH: MM</strong>.</td>
</tr>
<tr>
<td><strong>Recurrence</strong></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>For example, type <strong>2H</strong> if you want the remote directory to be scanned every 2 hours from the start time. The default is <strong>1H</strong>.</td>
</tr>
<tr>
<td><strong>Run On Save</strong></td>
<td>If you want the Log File protocol to run immediately after you click <strong>Save</strong>, select this check box.</td>
</tr>
<tr>
<td></td>
<td>After the <strong>Run On Save</strong> completes, the Log File protocol follows your configured start time and recurrence schedule.</td>
</tr>
<tr>
<td></td>
<td>Selecting <strong>Run On Save</strong> clears the list of previously processed files for the Ignore Previously Processed File parameter.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of <strong>Events Per Second</strong> (EPS) that you do not want this protocol to exceed. The valid range is <strong>100 - 5000</strong>.</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>From the list, select <strong>gzip</strong>.</td>
</tr>
<tr>
<td></td>
<td>Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in <strong>zip</strong>, <strong>gzip</strong>, <strong>tar</strong>, or <strong>tar+gzip</strong> archive format.</td>
</tr>
<tr>
<td><strong>Ignore Previously Processed File(s)</strong></td>
<td>Select this check box to track and ignore files that are already processed by the Log File protocol.</td>
</tr>
<tr>
<td></td>
<td>QRadar examines the log files in the remote directory to determine whether a file is 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 are not previously processed are downloaded.</td>
</tr>
<tr>
<td></td>
<td>This option applies only to FTP and SFTP service types.</td>
</tr>
</tbody>
</table>
Table 330. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change Local Directory?</strong></td>
<td>Select this check box to define a local directory on your QRadar for storing downloaded files during processing. It is suggested that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which gives you the option to configure the local directory to use for storing files.</td>
</tr>
<tr>
<td><strong>Event Generator</strong></td>
<td>From the Event Generator list, select <strong>LineByLine</strong>. The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.</td>
</tr>
</tbody>
</table>

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

The DSM configuration is complete. If your DSM requires custom event properties, see the IBM Security Custom Event Properties for IBM z/OS technical note. (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf)

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:
- IBM z/OS
- IBM CICS
- IBM RACF
- IBM DB2
- CA Top Secret
- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

Table 331. Log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Select your DSM name from the list.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>

Integrate IBM RACF with IBM QRadar by using audit scripts

The IBM RACF DSM collects events and audit transactions on the IBM mainframe with the Log File protocol.

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 can be displayed even when you collect events by using the Native QEXRACF integration.

Use the following procedure 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 by using the SMF dump utility. The RACFICE utility IRRADU00 (an IBM utility) creates a log file that contains all of the events and fields from the previous day in an SMF record format.
3. The QEXRACF program pulls data from the SMF formatted file. The program pulls only 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.

Configuring IBM RACF that uses audit scripts to integrate with IBM QRadar

IBM QRadar uses scripts to audit events from IBM RACF installations, which are collected by using the Log File protocol.

Procedure

1. Download the qexracf_bundled.tar.gz from the IBM support website.
2. On a Linux-based operating system, use the following command to extract the file:
   ```bash
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 by using any terminal emulator file transfer method.

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

Upload the QexRACF loadlib.trs file by using binary mode and append to a preallocated data set. The QexRACF loadlib.trs file is a tersed file that contains the executable (the mainframe program QEXRACF).

When you upload the .trs file from a workstation, preallocate 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 decompress the program that is stored in the QexRACF loadlib.trs file.

The following is an example of the qexracf_trsmain_JCL.txt file includes the following code:

```bash
//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 needs.
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. When the upload is complete, copy the program to an existing link listed library or add a STEPLIB DD statement that has the correct dataset name of the library that will contain the program.

7. The qexracf_jcl.txt file is a text file that contains 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 has the following code.

```plaintext
//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 output 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=40960),
// UNIT=SYSALDA
//SMFDATA DD DISP=SHR,DSN=&SMFIN
//SMFOUT DD DUMMY
//SYSDATE DD DSN=SMFOUT
//OUTDD DD DISP=SHR,DSN=&QRACFOUT
//**************************************************************
// FTP Output file from C program (Qexracf) to an FTP server *
//**************************************************************
// Note you need to replace <user>, <password>, <serveripaddr> *
//**************************************************************
//FTP EXEC PGM=FTP,REGION=3800K //*INPUT DD *
//<FTPSERVERIPADDR> <USER> <PASSWORD> //SYSPRINT DD SYSOUT=* //SYSTSPRT DD SYSOUT=* //QUIT //OUTDD DD DSN=QRACFOUDSN
```

8. After the output file is created, you must send this file to an FTP server.
This action 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 script. If the z/OS platform is configured to serve files through FTP or SFTP, or allow SCP, then no interim server is needed 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 are joined as one system.

### IBM SAN Volume Controller

The IBM QRadar DSM for IBM SAN Volume Controller collects events from IBM SAN Volume Controller. The following table describes the specifications for the IBM SAN Volume Controller DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM SAN Volume Controller</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMSANVolumeController-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>CADF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Activity, Control, and Monitor audit events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>IBM SAN Volume Controller website (<a href="http://www-03.ibm.com/systems/storage/software/virtualization/svc/">http://www-03.ibm.com/systems/storage/software/virtualization/svc/</a>)</td>
</tr>
</tbody>
</table>

To integrate IBM SAN Volume Controller with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs, in the order that they are listed, on your QRadar Console:
   - DSMCommon RPM
   - IBM SAN Volume Controller DSM RPM

2. Configure your IBM SAN Volume Controller server to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add an IBM SAN Volume Controller log source on the QRadar Console. The following table describes the parameters that require specific values for IBM SAN Volume Controller event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>IBM SAN Volume Controller</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the IBM SAN Volume Controller server.</td>
</tr>
</tbody>
</table>
4. To verify that QRadar is configured correctly, review the following table to see an example of a parsed
event message.
The following table shows a sample event message for IBM SAN Volume Controller:
Table 334. IBM SAN Volume Controller sample message
Event name

Low level category

Backup Successful

Backup Activity Succeeded

Sample log message
Oct 12 20:02:33
Cluster_<IP_address> IBM2145:
{"typeURI": "http://example.
com/cloud/audit/1.0/event"
,"eventTime": "2016-10-12T20:02
:30.000000+0000","target":
{"typeURI": "service/storage/
object","id": "0","name":
"username"},"observer": {"typeURI"
: "service/network/cluster/logger",
"id": "10032004394","name":
"username"},"tags": ["Backup"],
"eventType": "activity",
"measurements": [{"metric":
{"metricId": "www.example.com/svc/
Cloud
/Backup_Time/0000000000/000/0",
"name": "Time of backup being
copied or restored","unit":
"YYMMDDHHMMSS"},"result": "2016/
10/12/20/02/30"},{"metric":
{"metricId": "www.example.com/svc/
Cloud/Backup_Generation_Number/
0000000000/000/0","name":
"Volume backup generation number",
"unit": "Natural Number"},"result"
: "1"}],"initiator": {"typeURI":
"service/network/node","host":
{"address": "<IP_address>"},
"attachments": [{"content":
"6005076400C8010E5000000000000
000","typeURI": "text/plain",
"name": "volume_uuid"}],"name":
"username","id": "1"},"reason":
{"reasonCode": "200","reasonType"
: "http://www.example.com/assignments
/http-status-codes/http-status
-codes.xml"},"action": "backup"
,"outcome": "success","id":
"xxxxxxxxxxx-xxxxxxxxxx-xxx"}

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 SAN Volume Controller to communicate with QRadar
To collect events from IBM SAN Volume Controller, you must configure IBM SAN Volume Controller (SVC)
cluster to send events to QRadar from a syslog server.
SVC cluster uses rsyslogd 5.8.10 on a Linux 6.4 based host.
Procedure
1. Use SSH to log in to the SVC cluster command-line interface (CLI).
2. Type the following command to configure a remote syslog server to send CADF events to QRadar:
svctask mksyslogserver -ip <QRadar_Event_Collector_IP_Address> error
<on_or_off> -warning <on_or_off> -info <on_or_off> -cadf on

596 IBM QRadar : QRadar DSM Configuration Guide


The following example shows a command that is used to configure a remote syslog server to send CADF events:

```
svctask mksyslogserver -ip 192.0.2.1 -error on -warning on -info on -cadf o
```

**Note:** The error and warning flags are CADF event types that SVC sends to syslog servers.

---

**IBM Security Access Manager for Enterprise Single Sign-On**

You can use the IBM® Security Access Manager for Enterprise Single Sign-On DSM for IBM QRadar to receive events that are forwarded by using syslog.

QRadar can collect events from IBM Security Access Manager for Enterprise Single Sign-On version 8.1 or 8.2.

Events that are forwarded by the IBM Security Access Manager for Enterprise Single Sign-On include audit, system, and authentication events.

Events are read from the following database tables and forwarded by using syslog:

- IMSLOGUserService
- IMSLOGUserAdminActivity
- IMSLOGUserActivity

All events that are forwarded to QRadar from IBM Security Access Manager for Enterprise Single Sign-On use ### as a syslog field-separator. IBM Security Access Manager for Enterprise Single Sign-On forwards events to QRadar by using UDP on port 514.

**Before you begin**

To configure syslog forwarding for events, you must be an administrator or your user account must include credentials to access the IMS Configuration Utility.

Any firewalls that are configured between your IBM Security Access Manager for Enterprise Single Sign-On and QRadar are ideally configured to allow UDP communication on port 514. This configuration requires you to restart your IBM Security Access Manager for Enterprise Single Sign-On appliance.

**Configuring a log server type**

IBM Security Access Manager for Enterprise Single Sign-On appliance requires you to configure a log server type to forward syslog formatted events:

**Procedure**

   - For example, https://localhost:9043/webconf
2. From the navigation menu, select **Advanced Settings** > **IMS Server** > **Logging** > **Log Server Information**.
3. From the **Log server types** list, select **syslog**.
4. Click **Add**.
5. Click **Update** to save the configuration.

**Configuring syslog forwarding**

**About this task**

To forward events to QRadar, you must configure a syslog destination on your IBM Security Access Manager for Enterprise Single Sign-On appliance.
Procedure

1. From the navigation menu, select **Advanced Settings > IMS ServerLoggingSyslog**.

2. Configure the following options:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
   | Enable syslog      | From the **Available Tables** list, you must select the following tables, and click **Add**.  
   |                    | • logUserService  
   |                    | • logUserActivity  
   |                    | • logUserAdminActivity  
   | Syslog server port | Type 514 as the port number used for forwarding events to QRadar.  
   | Syslog server hostname | Type the IP address or host name of your QRadar Console or Event Collector.  
   | Syslog logging facility | Type an integer value to specify the facility of the events that are forwarded to QRadar. The default value is 20.  
   | Syslog field-separator | Type ### as the characters used to separate name-value pair entries in the syslog payload.  

3. Click **Update** to save the configuration.


   The syslog configuration is complete. The log source is added to QRadar as IBM Security Access Manager for Enterprise Single Sign-On syslog events are automatically discovered. Events that are forwarded to QRadar are displayed on the **Log Activity** tab.

Configuring a log source in IBM QRadar

QRadar automatically discovers and creates a log source for syslog events from IBM Security Access Manager for Enterprise Single Sign-On.

About this task

The following procedure is optional.

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 Access Manager for Enterprise Single Sign-On**.
6. Using the **Protocol Configuration** list, select **Syslog**.
7. Configure the following values:
### Table 336. Syslog parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your IBM Security Access Manager for Enterprise Single Sign-On appliance.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the log source. By default, the check box is selected.</td>
</tr>
<tr>
<td>Credibility</td>
<td>Select the <strong>Credibility</strong> of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>Select the <strong>Event Collector</strong> to use as the target for the log source.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the <strong>Coalescing Events</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td>Incoming Event Payload</td>
<td>From the <strong>Incoming Event Payload</strong> list, select the incoming payload encoder for parsing and storing the logs.</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the <strong>Store Event Payload</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

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

---

**IBM Security Access Manager for Mobile**

The IBM QRadar DSM for IBM Security Access Manager for Mobile collects logs from an IBM Security Access Manager for Mobile device, and an IBM Identity as a Service (IDaaS) device.

The following table identifies the specifications for the IBM Security Access Manager for Mobile DSM:

### Table 337. IBM Security Access Manager for Mobile DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM Security Access Manager for Mobile</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMSecurityAccessManagerForMobile-7.x - QRadar_version-Buildbuild_number.noarch.rpm</td>
</tr>
</tbody>
</table>
Table 337. IBM Security Access Manager for Mobile DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported versions</td>
<td>IBM Security Access Manager for Mobile v8.0.0 IBM IDaaS v2.0</td>
</tr>
<tr>
<td>Event Format</td>
<td>Common Base Event Format Log Event Extended Format (LEEF)</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>IBM_SECURITY_AUTHN IBM_SECURITY_TRUST IBM_SECURITY_RUNTIME IBM_SECURITY_CBA_AUDIT_MGMT IBM_SECURITY_CBA_AUDIT_RTE IBM_SECURITY_RTSS_AUDIT_AUTHZ IBM_SECURITY_SIGNING CloudOE Operations Usage IDaaS Appliance Audit IDaaS Platform Audit</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate IBM Security Access Manager for Mobile with 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:
   - TLS Syslog Protocol RPM
   - IBM Security Access Manager for Mobile DSM RPM
2. Configure your IBM Security Access Manager for Mobile device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an IBM Security Access Manager for Mobile log source on the QRadar console. The following table describes the parameters that require specific values for IBM Security Access Manager for Mobile and IBM Identity as a Service event collection:

<p>| Table 338. IBM Security Access Manager for Mobile log source parameters |
|--------------------------|----------------------|
| Parameter                | Value                |
| Log Source type          | IBM Security Access Manager for Mobile or IBM Identity as a Service |
| Protocol Configuration   | TLS Syslog           |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name in the Syslog header. Use the packet IP address, if the Syslog header does not contain an IP address or host name.</td>
</tr>
<tr>
<td>TLS Listen Port</td>
<td>Type the port number to accept incoming TLS Syslog Event.</td>
</tr>
</tbody>
</table>

4. Saving the log source creates a listen port for incoming TLS Syslog events and generates a certificate for the network devices. The certificate must be copied to any device on your network that can forward encrypted syslog. Additional network devices with a syslog-tls certificate file and the TLS listen port number can be automatically discovered as a TLS syslog log source in QRadar.

**Configuring IBM Security Access Manager for Mobile to communicate with QRadar**

Configure IBM Security Access Manager for Mobile to send audit logs to IBM QRadar through TLS syslog.

**Before you begin**

Ensure that IBM Security Access Manager for Mobile has access to QRadar for TLS syslog communication.

**Procedure**

1. Select **Monitor Analysis and Diagnosis > Logs > Audit Configuration**.
2. Click the **Syslog** tab and enter the information in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable audit log</td>
<td>Click <strong>Enable audit log</strong>.</td>
</tr>
<tr>
<td>Enable verbose audit events</td>
<td>Click <strong>Enable verbose audit events</strong>.</td>
</tr>
<tr>
<td></td>
<td>Audit events that are not verbose do not contain the JSON payload, which contains details of user activity.</td>
</tr>
<tr>
<td>Location of syslog server</td>
<td>Select <strong>On a remote server</strong>.</td>
</tr>
<tr>
<td>Host</td>
<td>The QRadar server host name or IP.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number that you want to use for QRadar to accept incoming TLS syslog events.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select <strong>TLS</strong></td>
</tr>
<tr>
<td>Certificate database (truststore)</td>
<td>The truststore that validates the syslog server certificate.</td>
</tr>
<tr>
<td>Enable client certificate authentication</td>
<td>Click <strong>Enable client certificate authentication</strong>.</td>
</tr>
<tr>
<td></td>
<td>The client can do client certificate authentication during the SSL handshake upon server request.</td>
</tr>
<tr>
<td>Certificate database (keystore)</td>
<td>The keystore for client certificate authentication.</td>
</tr>
<tr>
<td>Certificate label</td>
<td>The personal certificate for client certificate authentication</td>
</tr>
<tr>
<td>Enable disk failover</td>
<td>Clear <strong>Enable disk failover</strong>.</td>
</tr>
</tbody>
</table>
3. Click **Save**.
4. Click **Click here to review the changes or apply them to the system** to review pending changes.
5. Click **Deploy Changes**.

The runtime server restarts automatically if any of the new changes require a restart.

**Configuring IBM IDaaS Platform to communicate with QRadar**

You can enable IBM IDaaS Platform audit events to be generated in LEEF format on your IBM IDaaS console.

**Before you begin**

Ensure that IBM IDaaS Platform is installed and configured on your WAS console.

**Procedure**

1. Access the IDaaS Platform configuration file on your WAS console. `<WAS_home>/profiles/<profile_name>/config/idaas/platform.config.properties`
2. If the `platform.config.properties` file does not contain a set of audit properties, configure the following options:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>audit.enabled=true</code></td>
<td>Audit property is enabled.</td>
</tr>
<tr>
<td><code>audit.syslog.message.format=leef</code></td>
<td>Valid type is LEEF.</td>
</tr>
<tr>
<td><code>audit.syslog.server=&lt;IP_address&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>audit.syslog.transport=TRANSPORT_UDP</code></td>
<td>Transport values are TRANSPORT_UDP and TRANSPORT_TLS.</td>
</tr>
<tr>
<td><code>audit.syslog.server.port=514</code></td>
<td></td>
</tr>
</tbody>
</table>

3. Restart the IBM IDaaS Platform application on your WAS console.

**Configuring an IBM IDaaS console to communicate with QRadar**

You can enable audit events to be generated in LEEF Syslog format on your IBM IDaaS console.

**Before you begin**

Ensure that your IBM IDaaS console is installed and configured.

**Procedure**

1. Select **Secure Access Control > Advanced Configuration**.
2. Type `idaas.audit.event` in the **Filter** text box. The default format is Syslog.
3. Click **Edit**.
4. Select **LEEFSyslog**
5. Click **Save**.
6. Click **Deploy Changes**.

**IBM Security Directory Server**


The following table identifies the specifications for the IBM Security Directory Server DSM:
### IBM Security Directory Server Integration Process

You can integrate IBM Security Directory Server with IBM QRadar.

Use the following procedure:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - IBM Security Directory Server DSM RPM

2. Configure each IBM Security Directory Server system in your network to enable communication with QRadar.

   For more information about enabling communication between QRadar and IBM Security Directory Server, see [IBM website](https://www.ibm.com).

1. If QRadar does not automatically discover the log source, for each IBM Security Directory Server on your network, create a log source on the QRadar Console.

---

### Configuring IBM Security Directory Server to Communicate with QRadar

IBM QRadar can collect LEEF formatted audit events from your IBM Security Directory Server.

---

### About This Task

To configure IBM Security Directory Server to send logs to IBM QRadar, you must use the IBM Security Directory Server command line to add an auxiliary object class and then set values for the QRadar log management attributes.

### Procedure

1. Create a file (file_name) on the IBM Security Director Server with the following contents:

```yaml
dn: cn=Audit, cn=Log Management, cn=Configuration
changetype: modify
add: objectclass
objectclass: ibm-slapdQRadarConfig
```
2. To add the auxiliary object class `ibm-slapdQRadarConfig` for QRadar configuration attributes to `cn=Audit,cn=Log Management,cn=Configuration`, run the following command:

```
# idsldapmodify -h host_name -p portnumber -D cn=RDN_value -w password -f file_name
```

3. Create a new file (new_file) with the following contents:

```
dn: cn= specific_log_name, cn=Log Management, cn=configuration
changetype: modify
add:ibm-slapdLogEventQRadarEnabled
ibm-slapdLogEventQRadarEnabled: true
-
add:ibm-slapdLogEventQRadarHostName
ibm-slapdLogEventQRadarHostName: host_name_of_qradar_instance
-
add: ibm-slapdLogEventQRadarPort
ibm-slapdLogEventQRadarPort: port_of_qradar_instance
-
add: ibm-slapdLogEventQRadarMapFilesLocation
ibm-slapdLogEventQRadarMapFilesLocation: directory_location_of_qradar_mapfiles
```

4. Replace the following values in the new_file contents:
   
   - Replace `host_name_of_qradar_instance` with the destination QRadar Event Collector hostname or IP address.
   - Replace `port_of_qradar_instance` with 514.
   - If you have IBM Security Directory Server V6.3.1 installed, replace `directory_location_of_qradar_mapfiles` with `/opt/ibm/ldap/V6.3.1/idstools/idslogmgmt/`.

For example:

```
dn: cn= specific_log_name, cn=Log Management, cn=configuration
changetype: modify
add:ibm-slapdLogEventQRadarEnabled
ibm-slapdLogEventQRadarEnabled: true
-
add:ibm-slapdLogEventQRadarHostName
ibm-slapdLogEventQRadarHostName: qradar-collector.example.com
-
add: ibm-slapdLogEventQRadarPort
ibm-slapdLogEventQRadarPort: 514
-
add: ibm-slapdLogEventQRadarMapFilesLocation
ibm-slapdLogEventQRadarMapFilesLocation: /opt/ibm/ldap/V6.3.1/idstools/idslogmgmt/
```

5. To set the attribute values for QRadar integration, run the following command:

```
# idsldapmodify -h host_name -p portnumber -D cn=RDN_value -w password -f new_file
```

6. To start an instance, run the following command:

```
# ibmslapd -I <instance_name> -n
```

7. Optional: To start log management locally, run the following command:

```
# idslogmgmt -I <instance_name>
```

To start, get status, and stop log management remotely, run the following commands:

```
# ibmdirctl -D <adminDN> -w <password> -h <host_name> -p <administration server port number> startlogmgmt
# ibmdirctl -D <adminDN> -w <password> -h <host_name> -p <administration server port number> statuslogmgmt
# ibmdirctl -D <adminDN> -w <password> -h <host_name> -p <administration server port number> stoplogmgmt
```
Configuring an IBM Security Directory Server log source in IBM QRadar
You can collect IBM Security Directory Server events, configure a log source in QRadar.

About this task
Ensure that the DSM-IBMSecurityDirectoryServer-build_number.noarch.rpm file is installed and deployed on your QRadar host.

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 Security Directory Server.
7. From the Protocol Configuration list, select Syslog.
8. Configure the remaining parameters.
9. Click Save.
10. On the Admin tab, click Deploy Changes.

IBM Security Identity Governance
The IBM QRadar DSM for IBM Security Identity Governance collects audit events from IBM Security Governance servers.

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM Security Identity Governance</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMSecurityIdentityGovernance-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>IBM Security Identity Governance V5.1.1</td>
</tr>
<tr>
<td>Protocol</td>
<td>JDBC</td>
</tr>
<tr>
<td>Event format</td>
<td>NVP</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>IBM website (<a href="https://www.ibm.com">https://www.ibm.com</a>)</td>
</tr>
</tbody>
</table>

To integrate IBM Security Identity Governance 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. If multiple DSM RPMs are required, the integration sequence must reflect the DSM RPM dependency.
   - IBM Security Identity Governance (ISIG) DSM RPM
2. Configure a JDBC log source to poll for events from your IBM Security Identity Governance database.

3. Ensure that no firewall rules block communication between QRadar and the database that is associated with IBM Security Identity Governance.

4. If QRadar does not automatically detect the log source, add an IBM Security Identity Governance log source on the QRadar Console. The following table describes the parameters that require specific values for IBM Security Identity Governance event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>IBM Security Identity Governance</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>Select Oracle or DB2 for the database that you want to use as the event source.</td>
</tr>
<tr>
<td>Database Name</td>
<td>The name of the database to which you want to connect.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name of the IBM Security Governance database server.</td>
</tr>
</tbody>
</table>
Table 341. IBM Security Identity Governance DSM log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • MSDE - 1433   • Postgres - 5432   • MySQL - 3306   • Sybase - 1521   • Oracle - 1521   • Informix - 9088   • DB2 - 50000 If a database instance is used with the MSDE database type, you must leave the Port field blank.</td>
</tr>
<tr>
<td>Username</td>
<td>A user account for QRadar in the database.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is required to connect to the database.</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the none option.</td>
</tr>
<tr>
<td>Table Name</td>
<td>AUDIT_LOG</td>
</tr>
<tr>
<td>Select List</td>
<td>*</td>
</tr>
<tr>
<td>Compare Field</td>
<td>ID</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Enable the check box.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>The initial date and time for database polling.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>The amount of time, in seconds, between queries to the database table. The default polling interval is 10 seconds.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The number of events per second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
</tbody>
</table>
### Table 341. IBM Security Identity Governance DSM log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Mechanism</td>
<td>From the list, select the security mechanism that is supported by your DB2 server. If you don’t want to select a security mechanism, select None. The default is None. For more information about security mechanisms that are supported by DB2 environments, see the IBM Support website (<a href="https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvjcsec.html">https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvjcsec.html</a>)</td>
</tr>
<tr>
<td>Use Oracle Encryption</td>
<td>Oracle Encryption and Data Integrity settings is also known as Oracle Advanced Security. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC parameters, see c_logsource_JDBCprotocol.dita

**Related tasks**
- “Adding a DSM” on page 4
- “Adding a log source” on page 4
  
  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 communicate with your IBM Security Identity Governance database**

To forward audit logs from your IBM Security Identity Governance database to IBM QRadar, you must add a log source. Log sources are not automatically detected.

**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 Security Identity Governance.
7. From the Protocol Configuration list, select JDBC.
8. Configure the parameters.
9. Click Save.
IBM Security Identity Manager

The IBM Security Identity Manager DSM for IBM QRadar accepts audit, recertification, and system events from IBM Security Identity Manager appliances.

About this task

To collect events with QRadar, you must have the IBM Security Identity Manager JDBC protocol that is installed, which allows QRadar to poll for event information in the ITIMDB database. IBM Security Identity Manager events are generated from the audit table along with several other tables from the database.

Before you configure QRadar to integrate with IBM Security Identity Manager, create a database user account and password in IBM Security Identity Manager for QRadar. Your QRadar user needs read permission for the ITIMDB database, which stores IBM Security Identity Manager events.

The IBM Security Identity Manager protocol allows QRadar to log in and poll for events from the database. Creating a QRadar account is not required, but it is suggested for tracking and securing your event data.

**Note:** Ensure that no firewall rules are blocking the communication between your IBM Security Identity Manager appliance and QRadar.

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. In the **Log Source Description** field, type a description for the log source.
6. From the **Log Source Type** list, select IBM **Security Identity Manager**.
7. Using the **Protocol Configuration** list, select IBM **Security Identity Manager JDBC**.
8. Configure the following values:

| **Table 342. IBM Security Identity Manager JDBC parameters** |
|---|---|
| **Parameter** | **Description** |
| Log Source Type | IBM Security Identity Manager |
| Protocol Configuration | IBM Security Identity Manager JDBC |
| Log Source Identifier | Type a name for the log source. The name can’t contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol.  
If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn’t collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Database Type** | From the **Database Type** list, select a database to use for the event source.  
The options include the following databases:  
• **DB2** - Select this option if DB2 is the database type on your IBM Security Identity Manager appliance. DB2 is the default database type.  
• **MSDE** - Select this option if MSDE is the database type on your IBM Security Identity Manager appliance.  
• **Oracle** - Select this option if Oracle is the database type on your IBM Security Identity Manager appliance. |
| **Database Name** | The name of the database to which you want to connect.                                                                                      |
| **IP or Hostname** | Type the IP address or host name of the IBM Security Identity Manager appliance.                                                                |
| **Port**      | Type the port number that is used by the database server. The default that is displayed depends on the selected **Database Type**. The valid range is 0 - 65536. The default for DB2 is port 50000.  
The JDBC configuration port must match the listener port of the database. The database must have incoming TCP connections that are enabled to communicate with QRadar.  
The default port number for all options include:  
• **DB2** - 50000  
• **MSDE** - 1433  
• **Oracle** - 1521  
If you define a database Instance when you use MSDE as the database type, you must leave the **Port** parameter blank in your configuration. |
| **Username**  | Type the database user name. The user name can be up to 255 alphanumeric characters in length. The user name can also include underscores (_). |
| **Password** | Type the database password. The password can be up to 255 characters in length.                                                 |
| **Schema Name** | Type ISIMUSER in the **Schema Name** field.                                                                                               |
| **Table Name** | Type AUDIT_EVENT as the name of the table or view that includes the event records. If you change the value of this field from the default, events cannot be properly collected by the IBM Security Identity Manager JDBC protocol.  
The table name can be up to 255 alphanumeric characters in length. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (–), and period(.) |
Table 342. IBM Security Identity Manager JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select List</strong></td>
<td>Type ★ to include all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if needed for your configuration. The list must contain the field that is defined in the <strong>Compare Field</strong> parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td><strong>Compare Field</strong></td>
<td>Type TIMESTAMP to identify new events added between queries to the table by their time stamp. The compare field can be up to 255 alphanumeric characters in length. The list can include the special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td><strong>Start Date and Time</strong></td>
<td>Configure the start date and time for database polling. The <strong>Start Date and Time</strong> 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.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Type the polling interval in seconds, which is the amount of time between queries to the database table. The default polling interval is 30 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 without an H or M designator poll in seconds.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td><strong>Authentication Domain</strong></td>
<td>If you select MSDE as the <strong>Database Type</strong>, the <strong>Authentication Domain</strong> field is displayed. If your network is configured to validate users with domain credentials, you must define a Windows Authentication Domain. Otherwise, leave this field blank. The authentication domain must contain alphanumeric characters. The domain can include the following special characters: underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td><strong>Database Instance</strong></td>
<td>If you select MSDE as the <strong>Database Type</strong>, the <strong>Database Instance</strong> field is displayed. Type the instance to which you want to connect, if you have multiple SQL server instances on one server. If you use a non-standard port in your database configuration, or access to port 1434 for SQL database resolution is blocked, you must leave the <strong>Database Instance</strong> parameter blank in your configuration.</td>
</tr>
</tbody>
</table>
IBM Security Identity Manager JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Named Pipe Communication</strong></td>
<td>If you select MSDE as the <strong>Database Type</strong>, the <strong>Use Named Pipe Communication</strong> check box is displayed. By default, this check box is clear. Select this check box to use an alternative method to a TCP/IP port connection. When you use 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.</td>
</tr>
<tr>
<td><strong>Use NTLMv2</strong></td>
<td>If you select MSDE as the <strong>Database Type</strong>, the <strong>Use NTLMv2</strong> check box is displayed. Select the <strong>Use NTLMv2</strong> check box to force MSDE connections to use the NTLMv2 protocol when they communicate with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the <strong>Use NTLMv2</strong> check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td><strong>Database Cluster Name</strong></td>
<td>If you select the <strong>Use Named Pipe Communication</strong> check box, the <strong>Database Cluster Name</strong> parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.</td>
</tr>
</tbody>
</table>

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

   The configuration is complete.

**IBM Security Network IPS (GX)**

The IBM Security Network IPS (GX) 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 (GX) DSM:

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

To integrate the IBM Security Network IPS (GX) 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 (GX) RPMs on your QRadar Console.
2. For each instance of IBM Security Network IPS (GX), configure your IBM Security Network IPS (GX) 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 (GX) on your network.

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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 (GX) appliance for communication with QRadar**

To collect events with QRadar, you must configure your IBM Security Network IPS (GX) 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 (GX) 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 (GX) log source in QRadar

QRadar automatically discovers and creates a log source for syslog events from IBM Security Network IPS (GX) 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name for the log source as an identifier for events from your IBM Security Network IPS (GX) appliance.</td>
</tr>
<tr>
<td>Credibility</td>
<td>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.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>Enables the log source to coalesce (bundle) events.</td>
</tr>
<tr>
<td>Incoming Event Payload</td>
<td>The incoming payload encoder for parsing and storing the logs.</td>
</tr>
</tbody>
</table>

8. Click Save.

IBM QRadar Network Security XGS

The IBM QRadar Network Security XGS DSM accepts events by using the Log Enhanced Event Protocol (LEEF), which enables IBM QRadar to record all relevant events.

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM</td>
<td>QRadar Network Security XGS</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMQRadarNetworkSecurityXGS-QRadar_version-build_number.noarch,rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>v5.0 with fixpack 7 to v5.4</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
</tbody>
</table>
Before you configure a Network Security XGS appliance in QRadar, you must configure remote syslog alerts for your IBM QRadar Network Security XGS rules or policies to forward events to QRadar.

### Configuring IBM QRadar Network Security XGS Alerts

All event types are sent to IBM QRadar by using a remote syslog alert object that is LEEF enabled.

#### About this task

Remote syslog alert objects can be created, edited, and deleted from each context in which an event is generated. Log in to the IBM QRadar Network Security XGS local management interface as admin to configure a remote syslog alert object, and go to one of the following menus:

- Manage > System Settings > System Alerts (System events)
- Secure > Network Access Policy (Access events)
- Secure > IPS Event Filter Policy (Security events)
- Secure > Intrusion Prevention Policy (Security events)
- Secure > Network Access Policy > Inspection > Intrusion Prevention Policy

In the IPS Objects, the Network Objects pane, or the System Alerts page, complete the following steps.

#### Procedure

2. Select an existing remote syslog alert object, and then click Edit.
3. Configure the following options:

<table>
<thead>
<tr>
<th>Table 344. Syslog configuration parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Remote Syslog Collector</td>
</tr>
<tr>
<td>Remote Syslog Collector Port</td>
</tr>
</tbody>
</table>
Table 344. Syslog configuration parameters (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote LEEF Enabled</td>
<td>Select this check box to enable LEEF formatted events. This is a required field.</td>
</tr>
<tr>
<td></td>
<td>If you do not see this option, verify that you have software version 5.0 with fixpack 7 to v5.4 installed on your IBM QRadar Security Network appliance.</td>
</tr>
<tr>
<td>Comment</td>
<td>Typing a comment for the syslog configuration is optional.</td>
</tr>
</tbody>
</table>

4. Click **Save Configuration**.

   The alert is added to the **Available Objects** list.

5. To update your IBM QRadar Network Security XGS appliance, click **Deploy**.

6. Add the LEEF alert object for QRadar to the following locations:
   - One or more rules in a policy
   - **Added Objects** pane on the **System Alerts** page

7. Click **Deploy**

   For more information about the Network Security XGS device, click **Help** in the QRadar Network Security XGS local management interface browser client window or access the online *IBM QRadar Network Security XGS documentation*.

### Configuring a Log Source in IBM QRadar

QRadar automatically discovers and creates a log source for LEEF-enabled syslog events from IBM QRadar Network Security XGS. The following configuration steps are optional.

**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 QRadar Network Security XGS.
6. Using the **Protocol Configuration** list, select **Syslog**.
7. Configure the following values:

   Table 345. Syslog parameters
   
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your IBM QRadar Network Security XGS.</td>
</tr>
</tbody>
</table>

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

### IBM Security Privileged Identity Manager

The IBM QRadar DSM for IBM Security Privileged Identity Manager collects events by using the JDBC protocol.

The following table identifies the specifications for the IBM Security Privileged Identity Manager DSM:
Table 346. IBM Security Privileged Identity Manager DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM Security Privileged Identity Manager</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMSecurityPrivilegedIdentityManager-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V1.0.0 to V2.1.1</td>
</tr>
<tr>
<td>Protocol</td>
<td>JDBC</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit, Authentication, System</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

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 Rational® Portfolio Manager
   - IBM Security Privileged Identity Manager DSM RPM
2. Configure IBM Security Privileged Identity Manager to communicate with QRadar.
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 event collection:

Table 347. IBM Security Privileged Identity Manager JDBC log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source type</td>
<td>IBM Security Privileged Identity Manager</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
</tbody>
</table>
### Table 347. IBM Security Privileged Identity Manager JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| **Log Source Identifier**  | Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol.  
If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2. |
| **Database Type**          | MSDE                                                                                                                                 |
| **Database Name**          | The database name must match the database name that is specified in the **Log Source Identifier** field.                               |
| **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.                       |
| **Password**               | The password that is used to connect to the database.                                                                                 |
| **Authentication Domain**  | If you did not select **Use Microsoft JDBC, Authentication Domain** is displayed.                                                      
The domain for MSDE databases that are a Windows domain. If your network does not use a domain, leave this field blank. |
| **Database Instance**      | The database instance, if required. MSDE databases can include multiple SQL server instances on one server.                          
When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the **Database Instance** parameter must be blank in the log source configuration. |
<p>| <strong>Predefined Query</strong>       | Select <strong>None</strong>.                                                                                                                     |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table Name</td>
<td><code>&lt;DB2ADMIN&gt;.V_PIM_AUDIT_EVENT</code></td>
</tr>
<tr>
<td></td>
<td>Replace <code>DB2ADMIN</code> with the actual database schema name as identified in the Database Administrator ID parameter in IBM Security Privileged Identity Manager.</td>
</tr>
<tr>
<td>Select List</td>
<td>Type an asterisk (*) to select all fields from the table or view.</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Identifies new events that are added to the table between queries. Type <code>TIMESTAMP</code>.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Prepared statements enable the JDBC protocol source to set up the SQL statement, and run the SQL statement numerous times with different parameters. Select this check box.</td>
</tr>
<tr>
<td>Start Date and Time (Optional)</td>
<td>Type the start date and time for database polling in the following format: <code>yyyy-MM-dd HH:mm</code> with <code>HH</code> 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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>The amount of time between queries to the event table. Use the default <code>Polling Interval</code> value of <code>10</code>.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed. Use the default <code>EPS Throttle</code> value of <code>20000</code>.</td>
</tr>
<tr>
<td>Use Named Pipe Communication</td>
<td>If you did not select <code>Use Microsoft JDBC</code>, <code>Use Named Pipe Communication</code> is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>If you selected <code>Use Named Pipe Communication</code>, the <code>Database</code> parameter displays. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select Use Microsoft JDBC, Use NTLMv2 is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option if your connection supports SSL.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected Use Microsoft JDBC and Use SSL, the Microsoft SQL Server Hostname parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 Privileged Identity Manager to communicate with QRadar**

To communicate with IBM 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. You need these values when you configure a log source in QRadar.
   - Host name
   - Port
   - Database name
   - Database Administrator ID
6. **Important:** If you are using ISPIM 2.0.2 FP 6 and later, do not complete this step.

Create a view in IBM Security Privileged Identity Manager DB2 database in the same schema as identified in the Database Administrator ID parameter, by running the following SQL statement:

```sql
CREATE view V_PIM_AUDIT_EVENT AS
SELECT
```
Sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when using the JDBC protocol for the IBM Security Privileged Identity Manager DSM:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>

IBM Security Trusteer Apex Advanced Malware Protection

The IBM Security Trusteer Apex™ Advanced Malware Protection DSM collects and forwards event data from a Trusteer Apex Advanced Malware Protection system to IBM QRadar.

QRadar collects the following items from the Trusteer Apex Advanced Malware Protection system:

- Syslog events
- Log files (from an intermediary server that hosts flat feed files from the system.)
- Syslog events through SSL/TLS authentication

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM Security Trusteer Apex Advanced Malware Protection</td>
</tr>
<tr>
<td>Specification</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-TrusteerApex-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>Syslog/LEEF event collection: Apex Local Manager 2.0.45</td>
</tr>
<tr>
<td></td>
<td>LEEF: ver_1303.1</td>
</tr>
<tr>
<td></td>
<td>Flat File Feed: v1, v3, and v4</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>Log File</td>
</tr>
<tr>
<td></td>
<td>TLS Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Malware Detection</td>
</tr>
<tr>
<td></td>
<td>Exploit Detection</td>
</tr>
<tr>
<td></td>
<td>Data Exfiltration Detection</td>
</tr>
<tr>
<td></td>
<td>Lockdown for Java Event</td>
</tr>
<tr>
<td></td>
<td>File Inspection Event</td>
</tr>
<tr>
<td></td>
<td>Apex Stopped Event</td>
</tr>
<tr>
<td></td>
<td>Apex Uninstalled Event</td>
</tr>
<tr>
<td></td>
<td>Policy Changed Event</td>
</tr>
<tr>
<td></td>
<td>ASLR Violation Event</td>
</tr>
<tr>
<td></td>
<td>ASLR Enforcement Event</td>
</tr>
<tr>
<td></td>
<td>Password Protection Event</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

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
   - TLS Syslog 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 625.
• To send syslog events by using TLS Syslog Protocol to QRadar, see “Configuring IBM Security Trusteer Apex Advanced Malware Protection to send TLS Syslog events to QRadar” on page 626.

• 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 628.

3. If QRadar doesn’t 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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>IBM Security Trusteer Apex Advanced Malware Protection</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name from the syslog header. If the syslog header does not contain an IP address or a host name, use the packet IP address.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>IBM Security Trusteer Apex Advanced Malware Protection</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>TLS Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name from the syslog header. If the syslog header doesn't contain an IP address or a host name, use the packet IP address.</td>
</tr>
<tr>
<td>TLS Listen Port</td>
<td>The default port is 6514.</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>TLS</td>
</tr>
<tr>
<td>Certificate Type</td>
<td>Select the Provide Certificate option from the list.</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>The Maximum Connections parameter controls how many simultaneous connections the TLS Syslog protocol can accept for each Event Collector. For each Event Collector, there is a limit of 1000 connections across all TLS syslog log source configurations. The default for each device connection is 50. <strong>Note:</strong> Automatically discovered log sources that share a listener with another log source count only one time towards the limit. For example, the same port on the same event collector.</td>
</tr>
</tbody>
</table>
Table 351. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for TLS Syslog protocol (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS Protocols</td>
<td>Select the version of TLS installed on the client from the drop down list.</td>
</tr>
<tr>
<td>Provided Server Certificate Path</td>
<td>Absolute path of server certificate. For example, /opt/qradar/conf/trusted_certificates/apex-alm-tls.cert</td>
</tr>
<tr>
<td>Provided Private Key Path</td>
<td>Absolute path of PKCS#8 private key. For example, /etc/pki/tls/private/apex-alm-tls.pk8</td>
</tr>
</tbody>
</table>

**Important:** When you use the TLS syslog, and you want to use an FQDN to access the system, you must generate your own certificate for the listener, and then specify it in the TLS syslog configuration.

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

Table 352. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Log File Protocol

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>IBM Security Trusteer Apex Advanced Malware Protection</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Log File</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the server that hosts the Flat File Feed.</td>
</tr>
<tr>
<td>Service Type</td>
<td>SFTP</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>The IP address or host name of the server that hosts the Flat File Feed.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>22</td>
</tr>
<tr>
<td>Remote User</td>
<td>The user name that you created for QRadar on the server that hosts the Flat File Feed.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>If you use a password, leave this field blank.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>The log file directory where the Flat File Feed is stored.</td>
</tr>
<tr>
<td>Recursive</td>
<td>To avoid pulling the same file repeatedly to QRadar, do not select this option.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>&quot;trusteer_feeds_.<em>?<em>[0-9]{8}</em></em>[0-9]*?.csv&quot;</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time that you want your log file protocol to start collecting log files.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The polling interval for log file retrieval.</td>
</tr>
<tr>
<td>Run On Save</td>
<td>Must be enabled.</td>
</tr>
<tr>
<td>Processor</td>
<td>None</td>
</tr>
</tbody>
</table>
Table 352. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Log File Protocol (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore Previously Processed Files</td>
<td>Must be enabled.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>LINEBYLINE</td>
</tr>
<tr>
<td>File Encoding</td>
<td>UTF-8</td>
</tr>
</tbody>
</table>

Related concepts
Configuring IBM Security Trusteer Apex Advanced Malware Protection to send TLS Syslog events to QRadar
You can configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events through secure socket layer (SSL) or transport layer security (TLS) to IBM QRadar.

Related tasks
Adding a DSM
Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar
You can configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to IBM QRadar.

Configuring a Flat File Feed service
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.

Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar
You can configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to IBM 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, see:
• IBM Security Trusteer Apex Advanced Malware Protection Local Manager - Hybrid Solution Reference Guide
• IBM Security Trusteer Apex Advanced Malware Protection Feeds Reference Guide

Note: 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 doesn't automatically display, click Add.
4. Type the name of the Apex Local Manager.
5. Select the Enable check 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 IBM Security Trusteer Apex Advanced Malware Protection to send TLS Syslog events to QRadar

You can configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events through secure socket layer (SSL) or transport layer security (TLS) to IBM QRadar.

Complete the following steps to establish a secure channel for transmitting logs between Apex Trusteer and QRadar:
1. Create TLS/SSL Server Certificates and private key.
2. Create Client Authentication certificates in a PKCS#12 container for Apex Local Manager.
3. Configure the QRadar log source for IBM Security Trusteer Apex Advanced Malware Protection.
4. Configure the Apex Local Manager(ALM).

Creating a TLS/SSL server certificate and private key
To establish a communication between QRadar and Apex Local Manager (ALM) by using TLS encryption, you must create a self-signed certificate with public and private key pairs.

Procedure
1. Log in to QRadar as a root user by using SSH.
2. Create a self-signed certificate. For example:

   ```bash
   openssl req -new -x509 -newkey rsa:2048 -days 3650 -sha512 -nodes -x509 -subj 
   
   
   
   
   "C=US/ST=<State>/L=<City>/O=IBM/OU=IBM Security/CN=qradar FQDN or ip address"
   -keyout apex-alm-tls.key -out apex-alm-tls.cert
   
   
   
   
   
   -keyout apex-alm-tls.key -out apex-alm-tls.cert
   
   
   
   
   
   -keyout apex-alm-tls.key -out apex-alm-tls.cert
   ```

3. Convert the private key to the required DER encode PKCS#8 format:

   ```bash
   openssl pkcs8 -topk8 -inform PEM -outform DER -in apex-alm-tls.key -out apex-alm-tls.pk8 -nocrypt
   ```

   **Note:**
   - Use a unique filename if a certificate needs to be changed or updated.
   - Put the certificate file in /opt/qradar/conf/trusted_certificates.
   - Do not place the PKCS#8 formatted key file in /opt/qradar/conf/trusted_certificates.

   **Warning:** Make sure that you complete this step so that the connection works between ALM and QRadar.

Creating Client Authentication certificates and keys for Apex Local Manager
Configuring an ALM for TLS Syslog authentication requires a PKCS#12 file that contains the certificate and private key.

Procedure
1. Create a self-signed certificate and private key. For example,

   ```bash
   openssl req -new -x509 -newkey rsa:2048 -days 3650 -sha512 -nodes -x509 -subj 
   "C=US/ST=<State>/L=<City>/O=IBM/OU=IBM Security/CN=ALM FQDN or IP Address"
   -keyout alm-client-syslog-tls.key -out alm-client-syslog-tls.cert
   ```

2. Create the PKCS#12 container:

   ```bash
   openssl pkcs12 -export -inkey alm-client-syslog-tls.key -in alm-client-syslog-tls.cert -out alm-client-syslog-tls.p12 -name 
   "alm-client-syslog-tls"
   ```

   **Attention:** Make note of the password that you entered. The password is required when you configure the Apex Local Manager.
Configuring the Apex Local Manager

Configure the Apex Local Manager through a customer-assigned Apex Trusteer Management Application (TMA) original server.

**Procedure**

1. Log in to the Apex TMA.
2. From the left navigation menu, click the **Administration** accordion to expand the options available.
3. Click the **Apex Local Manager & SIEM Settings**.
4. Click **Add** and complete the following steps:
   a) Select the option to enable this Apex Local Manager.
   b) Enter a unique name.
5. Click **Next**.
6. From the **SIEM/Syslog Server Settings** page, provide a value for the following parameters:

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>IBM Security Q-Radar SIEM (LEEF)</td>
</tr>
<tr>
<td>Hostname</td>
<td><code>&lt;fqdn of the Qradar appliance&gt;</code></td>
</tr>
<tr>
<td>Port</td>
<td>Default is 6514.</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP with SSL/TLS</td>
</tr>
<tr>
<td>PKCS#12 Upload File</td>
<td>Upload the local PKCS#12 file</td>
</tr>
<tr>
<td>Encryption Password</td>
<td>The password that was entered during the creation of the client authentication certificates for Apex Local Manager.</td>
</tr>
<tr>
<td>CA Certificate Upload File</td>
<td>Upload local certificate file. For example, apex-alm-tls.cert</td>
</tr>
</tbody>
</table>
7. Click **Next**.
8. From the **System Events Setting** page, provide a value for the following parameters:

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td><code>&lt;QRadar FQDN or IP Address&gt;</code></td>
</tr>
<tr>
<td>Port</td>
<td>Default is 6514</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog with SSL/TLS</td>
</tr>
<tr>
<td>PKCS#12 Upload File</td>
<td>Upload the local PKCS#12 file. For example, alm-client-syslog.tls.p12</td>
</tr>
<tr>
<td>Encryption Password</td>
<td>The password that was entered during the creation of the client authentication certificates for Apex Local Manager.</td>
</tr>
<tr>
<td>CA Certificate Upload File</td>
<td>Upload local certificate file. For example, apex-alm-tls.cert</td>
</tr>
</tbody>
</table>
9. Click **Finish** to save the configuration.
10. Select the new entry.
11. Copy the **Provisioning key**.
What to do next
See “Configuring the ALM instance” on page 628

Configuring the ALM instance
Configure the ALM instance by using the provisioning key copied from the Apex Local Manager.

Procedure
1. Log in to the Apex Local Manager at:
   https://ipaddress:8443
2. From the General Settings page, paste the provisioning key into the field and click the Synchronize Settings.
   Note: A message will be displayed that states that the settings synchronized successfully.
3. Click the Test Connection to send test event to QRadar and validate the connection.

Configuring a Flat File Feed service
For IBM QRadar to retrieve log files from IBM Security Trusteer Apex 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 Trusteer Apex Advanced Malware Protection and allows for connections from external devices so that QRadar can retrieve the log files.

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

About this task
Flat file feed 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 in 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 Trusteer Apex Advanced Malware Protection to send flat file feed.
IBM Security Trusteer Apex Local Event Aggregator

IBM QRadar can collect and categorize malware, exploit, and data exfiltration detection events from Trusteer Apex Local Event Aggregator.

To collect syslog events, you must configure your Trusteer Apex Local Event Aggregator to forward syslog events to QRadar. Administrators can use the Apex L.E.A. management console interface to configure a syslog target for events. QRadar automatically discovers and creates log sources for syslog events that are forwarded from Trusteer Apex Local Event Aggregator appliances. QRadar supports syslog events from Trusteer Apex Local Event Aggregator V1304.x and later.

To integrate events with QRadar, administrators can complete the following tasks:

1. On your Trusteer Apex Local Event Aggregator appliance, configure syslog server.
2. On your QRadar system, verify that the forwarded events are automatically discovered.

Configuring syslog for Trusteer Apex Local Event Aggregator

To collect events, you must configure a syslog server on your Trusteer Apex Local Event Aggregator to forward syslog events.

Procedure

1. Log in to the Trusteer Apex L.E.A. management console.
2. From the navigation menu, select Configuration.
3. To export the current Trusteer Apex Local Event Aggregator configuration, click Export and save the file.
4. Open the configuration file with a text editor.
5. From the syslog.event_targets section, add the following information:

   ```json
   {   
     "host": "<QRadar IP address>", "port": "514", "proto": "tcp"   
   }
   ``

6. Save the configuration file.
7. From the navigation menu, select Configuration.
8. Click Choose file and select the new configuration file that contains the event target IP address.
9. Click Import.

As syslog events are generated by the Trusteer Apex Local Event Aggregator, they are forwarded to the target specified in the configuration file. The log source is automatically discovered after enough events are forwarded to QRadar. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created. The Log Activity tab displays events from Trusteer Apex Local Event Aggregator.

IBM Sense

The IBM QRadar DSM for IBM Sense collects notable events from a local or external system that generates Sense events.

The following table describes the specifications for the IBM Sense DSM:
Table 355. IBM Sense DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM Sense</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMSense-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>1</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
</tbody>
</table>
| Recorded event types| User Behavior
User Geography
User Time
User Access
User Privilege
User Risk
Sense Offense
Resource Risk |
| Automatically discovered? | Yes                                    |
| Includes identity?  | No                                                                   |
| Includes custom properties? | No                              |
| More information    | IBM website (http://www.ibm.com)                                    |

To integrate IBM Sense 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 Sense DSM RPM
   - DSMCommon RPM

The following table shows a sample event message for IBM Sense:

Table 356. IBM Sense sample message.

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| Behavior Change | User Behavior      | LEEF:2.0|IBM|Sense|1.0|Behavior Change|cat=User Behavior
description= score= scoreType= confidence= primaryEntity= primaryEntityType= additionalEntity= additionalEntityType= beginningTimestamp= endTimestamp= sensorDomain= referenceId1= referenceId2= referenceId3= referenceId4= referenceURL= originalSenseEventName= |
Configuring IBM Sense to communicate with QRadar

The User Behavior Analytics (UBA) app uses the IBM Sense DSM to add user risk scores and offenses into QRadar. When the app is installed, an IBM Sense log source is automatically created and configured by the app. No user input or configuration is required.

IBM SmartCloud Orchestrator

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>SmartCloud Orchestrator</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMSmartCloudOrchestrator-Qradar_version_build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V2.3 FP1 and later</td>
</tr>
<tr>
<td>Protocol type</td>
<td>IBM SmartCloud Orchestrator REST API</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Audit Records</td>
</tr>
<tr>
<td>Log source type in the QRadar UI</td>
<td>IBM SmartCloud Orchestrator</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td><a href="http://ibm.com">http://ibm.com</a></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>IBM SmartCloud Orchestrator.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>IBM SmartCloud Orchestrator REST API</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or server name of the SmartCloud Orchestrator.</td>
</tr>
</tbody>
</table>

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 DSM” on page 4
“Adding a log source” on page 4

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 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 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:

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

IBM Tivoli Access Manager for e-business
The IBM Tivoli Access Manager for e-business DSM for IBM QRadar accepts access, audit, and HTTP events forwarded from IBM Tivoli Access Manager.

QRadar collects audit, access, and HTTP events from IBM Tivoli Access Manager for e-business by using syslog. Before you can configure QRadar, you must configure Tivoli Access Manager for e-business to forward events to a syslog destination.

Tivoli Access Manager for e-business supports WebSEAL, a server that applies fine-grained security policy to the Tivoli Access Manager protected Web object space. For more information about WebSEAL, see IBM
Configure Tivoli Access Manager for e-business

Procedure

1. Log in to Tivoli Access Manager's IBM Security Web Gateway.
2. From the navigation menu, select Secure Reverse Proxy Settings > Manage > Reverse Proxy.
   The Reverse Proxy pane is displayed.
3. From the Instance column, select an instance.
4. Click the Manage list and select Configuration > Advanced.
   The text of the WebSEAL configuration file is displayed.
5. Locate the Authorization API Logging configuration.
   The remote syslog configuration begins with `logcfg`.
   For example, to send authorization events to a remote syslog server:
   ```
   # logcfg = audit.azn:rsyslog server=<IP address>,port=514,log_id=<log name>
   ```
6. Copy the remote syslog configuration (`logcfg`) to a new line without the comment (#) marker.
7. Edit the remote syslog configuration.
   For example,
   ```
   logcfg = audit.azn:rsyslog server=<IP address>,port=514,log_id=<log name>
   logcfg = audit.authn:rsyslog server=<IP address>,port=514,log_id=<log name>
   logcfg = http:rsyslog server=<IP address>,port=514,log_id=<log name>
   ```
   Where:
   - `<IP address>` is the IP address of your QRadar Console or Event Collector.
   - `<Log name>` is the name assigned to the log that is forwarded to QRadar. For example, `log_id=WebSEAL-log`.
8. Customize the `request.log` file.
   For example,
   ```
   request-log-format = isam-http-request-log|client-ip=%a|server-ip=%A|client-logname=%l|remote-user=%u|time=%t|port=%p|protocol=%H|request-method=%m|response-status=%s|url=%U|bytes=%b|remote-host=%h|request=%r
   ```
9. Click Submit.
   The Deploy button is displayed in the navigation menu.
10. From the navigation menu, click Deploy.
11. Click Deploy.
   You must restart the reverse proxy instance to continue.
12. From the Instance column, select your instance configuration.
13. Click the Manage list and select Control > Restart.
   A status message is displayed after the restart completes. For more information on configuring a syslog destination, see your IBM Tivoli Access Manager for e-business vendor documentation. You are now ready to configure a log source in QRadar.
Configuring a log source

IBM QRadar automatically discovers syslog audit and access events, but does not automatically discover HTTP events that are forwarded from IBM Tivoli Access Manager for e-business.

About this task

Since QRadar automatically discovers audit and access events, you are not required to create a log source. However, you can manually create a log source for QRadar to receive IBM Tivoli Access Manager for e-business syslog events. The following configuration steps for creating a log source are optional.

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.
5. In the Log Source Name field, type a name for the log source.
6. In the Log Source Description field, type a description for the log source.
7. From the Log Source Type list, select IBM Tivoli Access Manager for e-business.
8. From the Protocol Configuration list, select Syslog.
9. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for your IBM Tivoli Access Manager for e-business appliance. The IP address or host name identifies your IBM Tivoli Access Manager for e-business as a unique event source in QRadar.</td>
</tr>
</tbody>
</table>

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

IBM Tivoli Endpoint Manager

IBM Tivoli Endpoint Manager is now known as IBM BigFix.

Related concepts

"IBM BigFix" on page 541

IBM WebSphere Application Server

The IBM WebSphere Application Server DSM for IBM QRadar accepts events using the log file protocol source.

QRadar records all relevant application and security events from the WebSphere Application Server log files.

Configuring IBM WebSphere

You can configure IBM WebSphere Application Server events for IBM QRadar.

Procedure

1. Using a web browser, log in to the IBM WebSphere administrative console.
2. Click **Environment > WebSphere Variables.**
3. Define Cell as the Scope level for the variable.
4. Click **New.**
5. Configure the following values:
   - **Name** - Type a name for the cell variable.
   - **Description** - Type a description for the variable (optional).
   - **Value** - Type a directory path for the log files.

   For example:
   ```
   {QRADAR_LOG_ROOT} = /opt/IBM/WebSphere/AppServer/profiles/Custom01/logs/QRadar
   ```

   You must create the target directory that is specified in “Configuring IBM WebSphere” on page 634 before proceeding.
6. Click **OK.**
7. Click **Save.**
8. You must restart the WebSphere Application Server to save the configuration changes.

   **Note:** If the variable you created affects a cell, you must restart all WebSphere Application Servers in the cell before you continue.

**What to do next**

You are now ready to customize the logging option for the IBM WebSphere Application Server DSM.

**Customizing the Logging Option**

You must customize the logging option for each application server WebSphere uses and change the settings for the JVM Logs (Java Virtual Machine logs).

**Procedure**

1. **Select Servers > Application Servers.**
2. Select your WebSphere Application Server to load the server properties.
3. Select **Logging and Tracing > JVM Logs.**
4. Configure a name for the JVM log files.

   For example:
   ```
   System.Out log file name:
   ${QRADAR_LOG_ROOT}/${WAS_SERVER_NAME}-SystemOut.log
   System.Err log file name:
   ${QRADAR_LOG_ROOT}/${WAS_SERVER_NAME}-SystemErr.log
   ```
5. Select a time of day to save the log files to the target directory.
6. Click **OK.**
7. You must restart the WebSphere Application Server to save the configuration changes.

   **Note:** If the JVM Logs changes affect the cell, you must restart all of the WebSphere Application Servers in the cell before you continue.

You are now ready to import the file into IBM QRadar using the log file protocol.
Creating a log source

The log file protocol allows IBM QRadar to retrieve archived log files from a remote host. The IBM WebSphere Application Server DSM supports the bulk loading of log files by using the log file protocol source.

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.
5. In the Log Source Name field, type a name for the log source.
6. In the Log Source Description field, type a description for the log source.
7. From the Log Source Type list, select IBM WebSphere Application Server.
8. Using the Protocol Configuration list, select Log File.
9. Configure the following values:

Table 359. Log file parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type an IP address, host name, or name to identify your IBM WebSphere Application Server as an event source in QRadar. 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 IBM WebSphere Application Servers that provides logs to a file repository, specify the IP address or host name of the device that created the event log. This allows events to be identified at the device level in your network, instead of identifying the file repository.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP.</td>
</tr>
<tr>
<td></td>
<td>• SFTP - SSH File Transfer Protocol</td>
</tr>
<tr>
<td></td>
<td>• FTP - File Transfer Protocol</td>
</tr>
<tr>
<td></td>
<td>• SCP - Secure Copy</td>
</tr>
<tr>
<td></td>
<td>The underlying protocol that is 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.</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>Type the IP address or host name of your IBM WebSphere Application Server storing your event log files.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535.</td>
</tr>
<tr>
<td></td>
<td>The options include FTP ports:</td>
</tr>
<tr>
<td></td>
<td>• FTP - TCP Port 21</td>
</tr>
<tr>
<td></td>
<td>• SFTP - TCP Port 22</td>
</tr>
<tr>
<td></td>
<td>• SCP - TCP Port 22</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 359. Log file parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote User</td>
<td>Type the user name necessary to log in to the host that contains your event files. The user name can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Type the password necessary to log in to the host.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password necessary to log in to the host.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>If you select SCP or SFTP as the Service Type, this parameter allows for the definition of an SSH private key file. The Remote Password field is ignored when you provide an SSH Key File.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>Type the directory location on the remote host to the cell and file path you specified in “Configuring IBM WebSphere” on page 634. This is the directory that you created containing your IBM WebSphere Application Server event files. For FTP only. If your log files are located 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.</td>
</tr>
<tr>
<td>Recursive</td>
<td>Select this check box if you want the file pattern to search sub folders. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>If you select SFTP or FTP as the Service Type, this option allows for the configuration of the regular expression (regex) to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing. The FTP file pattern that you specify must match the name that you assigned to your JVM logs in “Customizing the Logging Option” on page 635. For example, to collect system logs, type the following code: System.*..log Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: <a href="http://download.oracle.com/javase/tutorial/essential/regex/">http://download.oracle.com/javase/tutorial/essential/regex/</a></td>
</tr>
</tbody>
</table>
### Table 359. Log file parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| FTP Transfer Mode     | This option appears only if you select FTP as the Service Type. The FTP Transfer Mode parameter allows for the definition of the file transfer mode when log files are retrieved 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 parameter and LINEBYLINE the Event Generator parameter when you use ASCII as the FTP 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. |
| 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. When you schedule a log file protocol, select a recurrence time for the log file protocol shorter than the scheduled write interval of the WebSphere Application Server log files. This ensures that WebSphere events are collected by the log file protocol before the new log file overwrites the old event log. |
| 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 - 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 the contents to be processed. |
| Ignore Previously Processed File(s) | Select this check box to track files that are processed. Files that are previously processed are not processed a second time. This check box applies only to FTP and SFTP Service Types. |
Table 359. Log file parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Local Directory?</td>
<td>Select this check box to define the local directory on your QRadar 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 gives the option of configuring the local directory to use for storing files.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the Event Generator list, select WebSphere Application Server. The Event Generator applies more processing, which is specific to retrieved event files for IBM WebSphere Application Server events.</td>
</tr>
</tbody>
</table>

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

The configuration is complete. For more information about IBM WebServer Application Server, see your vendor documentation.

**IBM WebSphere DataPower**

IBM WebSphere DataPower is now known as IBM Datapower.

**Related concepts**

IBM DataPower

**IBM z/OS**

The IBM z/OS DSM collects events from an IBM z/OS® mainframe that uses IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can collect the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to collect events on a polling interval, which enables QRadar to collect the events on the schedule that you define.

To collect IBM z/OS events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html).

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 (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).

3. Create a log source in QRadar for IBM z/OS.

4. If you want to create a custom event property for IBM z/OS in QRadar, for more information, see the IBM Security Custom Event Properties for IBM z/OS technical note (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf).
Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.


Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:

- IBM z/OS
- IBM CICS
- IBM RACF
- IBM DB2
- CA Top Secret
- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

<table>
<thead>
<tr>
<th>Table 360. Log source parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Select your DSM name from the list.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>
Creating a log source for Log File protocol

The Log File protocol enables IBM QRadar to retrieve archived log files from a remote host for the IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, and CA ACF2 DSM's.

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 z/OS with zSecure writes log files to a specified directory as gzipped archives. 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 that uses the Log File protocol. QRadar requires credentials to log in to the system that hosts your LEAF formatted event files and a polling interval.

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.
5. In the Log Source Name field, type a name for the log source.
6. In the Log Source Description field, type a description for the log source.
7. From the Log Source Type list, select your DSM name.
8. From the Protocol Configuration list, select Log File.
9. Configure the Log File protocol parameters.

The following table describes the parameters that require specific values for the DSM event collection:

<table>
<thead>
<tr>
<th>Table 361. Log File protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Service Type</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>----------------------------</td>
</tr>
<tr>
<td><strong>Remote IP or Hostname</strong></td>
</tr>
</tbody>
</table>
| **Remote Port**            | Type the TCP port on the remote host that is running the selected **Service Type**. The valid range is 1 - 65535.  
The options include ports:  
  • 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. |
| **Remote User**            | Type the user name or user ID necessary to log in to the system that contains your event files.  
  • If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length.  
  • If your log files are 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 gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored. |
| **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. |
| **Recursive**              | If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear.  
  If you configure SCP as the Service Type, the Recursive option is ignored. |
### Table 361. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>
| **FTP File Pattern**    | If you select **SFTP** or **FTP** as the **Service Type**, you can configure the regular expression (regex) needed to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing.  
  The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: `<product_name>.<timestamp>.gz`  
  The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with `zOS` and end with `.gz`, type the following code:  
  `zOS.*\.gz`  
  Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions. (http://download.oracle.com/javase/tutorial/essential/regex/) |
| **FTP Transfer Mode**   | This option displays only if you select **FTP** as the **Service Type**. From the list, select **Binary**.  
  The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as `zip`, `gzip`, `tar`, or `tar+gzip` archive files. |
| **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. 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**         | If you want the Log File protocol to run immediately after you click **Save**, select this check box.  
  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 - 5000. |
Table 361. Log File protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>From the list, select gzip.</td>
</tr>
<tr>
<td></td>
<td>Processors enable event file archives to be expanded and contents are</td>
</tr>
<tr>
<td></td>
<td>processed for events. Files are processed after they are downloaded to</td>
</tr>
<tr>
<td></td>
<td>QRadar. QRadar can process files in zip, gzip, tar, or tar+gzip</td>
</tr>
<tr>
<td></td>
<td>archive format.</td>
</tr>
<tr>
<td>Ignore Previously Processed</td>
<td>Select this check box to track and ignore files that are already</td>
</tr>
<tr>
<td>File(s)</td>
<td>processed by the Log File protocol.</td>
</tr>
<tr>
<td></td>
<td>QRadar examines the log files in the remote directory to determine</td>
</tr>
<tr>
<td></td>
<td>whether a file is previously processed by the Log File protocol.</td>
</tr>
<tr>
<td></td>
<td>If a previously processed file is detected, the Log File protocol</td>
</tr>
<tr>
<td></td>
<td>does not download the file for processing. All files that are not</td>
</tr>
<tr>
<td></td>
<td>previously processed are downloaded.</td>
</tr>
<tr>
<td></td>
<td>This option applies only to FTP and SFTP service types.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>Select this check box to define a local directory on your QRadar for</td>
</tr>
<tr>
<td></td>
<td>storing downloaded files during processing.</td>
</tr>
<tr>
<td></td>
<td>It is suggested that you leave this check box clear. When this check</td>
</tr>
<tr>
<td></td>
<td>box is selected, the Local Directory field is displayed, which gives</td>
</tr>
<tr>
<td></td>
<td>you the option to configure the local directory to use for storing</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the Event Generator list, select LineByLine.</td>
</tr>
<tr>
<td></td>
<td>The Event Generator applies more processing to the retrieved event</td>
</tr>
<tr>
<td></td>
<td>files. Each line is a single event. For example, if a file has 10</td>
</tr>
<tr>
<td></td>
<td>lines of text, 10 separate events are created.</td>
</tr>
</tbody>
</table>

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

The DSM configuration is complete. If your DSM requires custom event properties, see the IBM Security Custom Event Properties for IBM z/OS technical note. (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf)

**IBM zSecure Alert**

The IBM zSecure Alert DSM for IBM QRadar accepts alert events by using syslog, allowing QRadar to receive alert events in real time.

**About this task**

The alert configuration on your IBM zSecure Alert appliance determines which alert conditions you want to monitor and forward to QRadar. To collect events in QRadar, you must configure your IBM zSecure Alert appliance to forward events in a UNIX syslog event format by using the QRadar IP address as the destination. For information on configuring UNIX syslog alerts and destinations, see the IBM Security zSecure Alert User Reference Manual.

QRadar automatically discovers and creates a log source for syslog events from IBM zSecure Alert. However, you can manually create a log source for QRadar to receive syslog events. The following configuration steps are optional.
Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.
5. In the Log Source Name field, type a name for your log source.
6. In the Log Source Description field, type a description for the log source.
7. From the Log Source Type list, select IBM zSecure Alert.
8. Using the Protocol Configuration list, select Syslog.
9. Configure the following values:

<table>
<thead>
<tr>
<th>Table 362. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

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

The configuration is complete.
Chapter 80. ISC Bind

You can integrate an Internet System Consortium (ISC) BIND device with IBM QRadar. An ISC BIND device accepts events using syslog.

About this task
You can configure syslog on your ISC BIND device to forward events to QRadar.

Procedure
1. Log in to the ISC BIND device.
2. Open the following file to add a logging clause:
   
   named.conf
   logging {
     channel <channel_name> {
       syslog <syslog_facility>;
       severity <critical | error | warning | notice | info | debug [level ] | dynamic >;
       print-category yes;
       print-severity yes;
       print-time yes;
     };
     category queries {
       <channel_name>;
     };
     category notify {
       <channel_name>;
     };
     category network {
       <channel_name>;
     };
     category client {
       <channel_name>;
     };
   }

   For Example:
   logging {
     channel QRadar {
       syslog local3;
       severity info;
3. Save and exit the file.

4. Edit the syslog configuration to log to your QRadar using the facility you selected in Chapter 80, “ISC Bind,” on page 647:

   `<syslog_facility>.* @<IP_address>`

   Where `<IP Address>` is the IP address of your QRadar.

   For example:

   `local3.* @<IP_address>`

   **Note**: QRadar only parses logs with a severity level of info or higher.

5. Restart the following services.

   service syslog restart
   service named restart

**What to do next**

You can now configure the log source in QRadar.

---

**Configuring a log source**

IBM QRadar automatically discovers and creates a log source for syslog events from ISC BIND.

**About this task**

The following configuration steps are optional.

**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 **ISC BIND**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 363. Syslog protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

   The configuration is complete.
Chapter 81. Illumio Adaptive Security Platform

The IBM QRadar DSM for Illumio Adaptive Security Platform collects events from the Illumio Policy Compute Engine (PCE).

The following table describes the specifications for the Illumio Adaptive Security Platform DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Illumio</td>
</tr>
<tr>
<td>DSM name</td>
<td>Illumio Adaptive Security Platform</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IllumioAdaptiveSecurityPlatform-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Log Event Extended Format (LEEF)</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit, Traffic</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Illumio website (<a href="https://www.illumio.com">https://www.illumio.com</a>)</td>
</tr>
</tbody>
</table>

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

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs, in the order that they are listed, on your QRadar Console:
   - DSMCommon RPM
   - Illumio Adaptive Security Platform DSM RPM

2. Configure your Illumio PCE to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add an Illumio Adaptive Security Platform log source on the QRadar Console. The following table describes the parameters that require specific values for Illumio Adaptive Security Platform event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Illumio Adaptive Security Platform</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>A unique identifier for the log source.</td>
</tr>
</tbody>
</table>

4. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

The following table shows a sample event message from Illumio Adaptive Security Platform:

© Copyright IBM Corp. 2005, 2019
Table 366. Illumio Adaptive Security Platform sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow_allowed</td>
<td>Firewall Permit</td>
<td>`&lt;14&gt;1 2016-08-08T22:18:24.000+00:00 hostname1 illumio_pce/collector 5458 - -</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sec=694704.253 sev=INFO pid=5458 tid=145454040 rid=0 LEEF:2.0</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 4

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 Illumio Adaptive Security Platform to communicate with QRadar

To forward events to IBM QRadar, you must configure Exporting Events to Syslog and Syslog Forwarding for your Illumio PCE.

Related tasks

“Configuring Exporting Events to Syslog for Illumio PCE” on page 652

All audit and traffic summaries are sent to syslog in JSON format by default. The default configuration must be updated so that the events are exported in LEEF format.

“Configuring Syslog Forwarding for Illumio PCE” on page 653

Because the PCE software exports logs to a local syslog, you must configure either rsyslog or syslog-ng service on each node in your PCE cluster to forward these logs to QRadar.

Configuring Exporting Events to Syslog for Illumio PCE

All audit and traffic summaries are sent to syslog in JSON format by default. The default configuration must be updated so that the events are exported in LEEF format.

Procedure

1. Stop the PCE software so that changes to the PCE `runtime_env.yml` file can be made.
2. Enable LEEF formatting by configuring the PCE `runtime_env.yml` parameter `syslog_event_export_format`.

syslog_event_export_format:leef

3. Export traffic summaries to Syslog by configuring the PCE `runtime_env.yml` parameter `export_flow_summaries_to_syslog`:

   export_flow_summaries_to_syslog:
   accepted
   potentially_blocked
   blocked
**Note:** By default, the PCE exports all audit events to Syslog. Therefore, no configuration is required to enable exporting audit events.

**Note:** The `export_flow_summaries_to_syslog` parameter should be considered experimental and the mechanism for configuring this feature might change in a future release.

4. Type the `/illumio-pce-env check` command to validate the syntax of the configuration file.
5. Start the PCE software.
6. Configure Syslog Forwarding.

**Configuring Syslog Forwarding for Illumio PCE**
Because the PCE software exports logs to a local syslog, you must configure either rsyslog or syslog-ng service on each node in your PCE cluster to forward these logs to QRadar.

**Procedure**
1. If you want to configure rsyslog, complete the following steps.
   a) Edit the `/etc/rsyslog.conf` file by adding the following entries or uncomment if they are already present. Replace `<QRadar Event Collector IP>` with the IP address of the QRadar event collector:

   ```
   ### LEEF (flow data, audit events) ###
   if $syslogseverity <= 6 \n   and $syslogtag startswith 'illumio_pce/collector[\' \n   and $msg contains 'LEEF:\' \n   and $msg contains '|Illumio|PCE|' \n   and $msg contains 'cat=flow_summary' \n   then @@<QRadar Event Collector IP>:514
   
   if $syslogseverity <= 6 \n   and $syslogtag startswith 'illumio_pce/' \n   and $msg contains 'LEEF:\' \n   and $msg contains '|Illumio|PCE|' \n   and $msg contains 'audit_events' \n   then @@<QRadar Event Collector IP>:514
   ```

   b) Restart the rsyslog service.

   `service rsyslog restart`

2. If you want to configure syslog-ng, complete the following steps.
   a) Edit the `/etc/syslog-ng/syslog-ng.conf` file by adding the following entries or uncomment if they are already present. Replace `<QRadar Event Collector IP>` with the IP address of the QRadar event collector:

   ```
   #destination d_net { tcp("<QRadar Event Collector IP>") port(514) flush_lines(1)); };
   #log { source(s_src); filter(flow_events);
   destination(d_net); };
   #log { source(s_src);
   filter(audit_events); destination(d_net); };
   
   ### LEEF (flow data, audit events) ###
   filter flow_events {
   level(info..emerg)
   and program("illumio_pce/collector")
   and message('LEEF:[^\]\]+|Illumio|PCE\])' and message('cat=flow_summary');
   }
   
   filter audit_events {
   level(info..emerg)
   and program("illumio_pce/")
   and message('LEEF:[^\]\]+|Illumio|PCE\])' and message('cat=[^ #]+audit_events');
   }
   ```

   b) Restart the syslog-ng service.

   `service syslog-ng restart`
Chapter 82. Imperva Incapsula

The IBM QRadar DSM for Imperva Incapsula collects logs from an Imperva Incapsula service. The following table describes the specifications for the Imperva Incapsula DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Imperva</td>
</tr>
<tr>
<td>DSM name</td>
<td>Imperva Incapsula</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-ImpervaIncapsula-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Access events and Security alerts</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate Imperva Incapsula 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
   - Imperva Incapsula DSM RPM

2. Configure the Log download utility to collect logs and then forward the logs to QRadar.

3. If QRadar does not automatically detect the log source, add an Imperva Incapsula log source on the QRadar Console. The following table describes the parameters that require specific values to collect event from Imperva Incapsula:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Imperva Incapsula</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

4. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Imperva Incapsula:
### Table 369. Imperva Incapsula sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>REQ_PASSED</td>
<td>Information</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>

### Related tasks

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 Imperva Incapsula to communicate with QRadar

To collect events from Imperva Incapsula, a Python script is required.

The script, configuration files, and instructions, can be obtained from the GitHub website (https://github.com/Incapsula/logs-downloader).

### Procedure

1. Install the script dependencies by using a package manager such as apt-get or pip. The script dependencies must be installed on an intermediary server that is not QRadar. The following dependencies might require additional modules, depending on your operating system:
   - M2Crypto
   - loggerglue
   - crypto.cipher
2. To collect log events, run the script.
a) Create a new local directory or use the default directory to store the script configuration file. The Settings.Config file is stored in this local directory. The default directory is /etc/incapsula/logs/config. To get the Settings.Config file, go to the GitHub website (https://github.com/Incapsula/logs-downloader/tree/master/config).

b) Configure the parameter values for the Settings.Config configuration file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIID</td>
<td>Your API ID.</td>
</tr>
<tr>
<td>APIKEY</td>
<td>Your API key.</td>
</tr>
<tr>
<td>SAVE_LOCALLY</td>
<td>A Yes or No value that instructs Incapsula whether to maintain the log files after they are processed. When set to No, the files are deleted. The default is YES.</td>
</tr>
<tr>
<td>PROCESS_DIR</td>
<td>The directory where Incapsula automatically saves the logs after extracting them. The default is /tmp/processed/</td>
</tr>
<tr>
<td>BASEURL</td>
<td>The URL of your logs repository in the Incapsula cloud. This URL is displayed in the Incapsula Administration Console Settings window as the Log Server URL field.</td>
</tr>
<tr>
<td>USEPROXY</td>
<td>Specify YES to use a proxy to download the files. The default is NO.</td>
</tr>
<tr>
<td>PROXYSERVER</td>
<td>If you choose to use a proxy server, when you type the proxy URL, use the <a href="https://1.1.1.1:8080">https://1.1.1.1:8080</a> format.</td>
</tr>
<tr>
<td>SYSLOG_ENABLE</td>
<td>Type YES. A Yes or No value that instructs Incapsula about whether to send the files by using syslog. The default is YES.</td>
</tr>
<tr>
<td>SYSLOG_ADDRESS</td>
<td>The IP address for QRadar</td>
</tr>
<tr>
<td>SYSLOG_PORT</td>
<td>514</td>
</tr>
<tr>
<td>USE_CUSTOM_CA_FILE</td>
<td>In case the service's certificate is not in the bundle, the default is NO.</td>
</tr>
<tr>
<td>CUSTOM_CA_FILE</td>
<td>The file path for the custom certificate file.</td>
</tr>
</tbody>
</table>

3. Run the following command to start the LogsDownloader script and retrieve logs:

```
python LogsDownloader.py -c <path_to_config_folder> -l <path_to_system_logs_folder> -v <system_logs_level>
```

The -c, -l, and -v parameters are optional. If the parameter values are not specified, the following table describes the default values that are used:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;path_to_config_folder&gt;</td>
<td>The default is /etc/incapsula/logs/config</td>
</tr>
<tr>
<td>&lt;path_to_system_logs_folder&gt;</td>
<td>The &lt;path_to_system_logs_folder&gt; is the folder where the LogsDownloader.py script output log file is stored. This parameter does not refer to your Incapsula logs. The default is /var/log/incapsula/logsDownloader/</td>
</tr>
<tr>
<td>&lt;system_logs_level&gt;</td>
<td>The logging level for the script output log. Supported values are info, debug, and error. The default value is info.</td>
</tr>
</tbody>
</table>

**Note:**

- If the **SAVE_LOCALLY** parameter is set to YES, the downloaded log files can be found in the PROCESS_DIR directory.
- After the files are downloaded, the script saves the name of the last file it collects as LastKnownDownloadedFileId.txt in the <path_to_config_folder> directory. If you want to collect all of the historical logs, you must delete this file.
- For more information about setting up an intermediary server, see Imperva Incapsula's Web Protection - Log Integration (https://docs.incapsula.com/Content/management-console-and-settings/log-integration.htm).
Chapter 83. Imperva SecureSphere

The IBM QRadar DSM for Imperva SecureSphere collects all relevant syslog events from your Imperva SecureSphere devices.

The following table lists the specifications for the Imperva SecureSphere DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Imperva</td>
</tr>
<tr>
<td>DSM name</td>
<td>SecureSphere</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-ImpervaSecureSphere-QRadar-version-Build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>v6.2 and v7.x to v13 Release Enterprise Edition (Syslog)</td>
</tr>
<tr>
<td></td>
<td>v9.5 to v13 (LEEF)</td>
</tr>
<tr>
<td>Event format</td>
<td>syslog</td>
</tr>
<tr>
<td></td>
<td>LEEF</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Firewall policy events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Imperva website (<a href="http://www.imperva.com">http://www.imperva.com</a>)</td>
</tr>
</tbody>
</table>

To send events from Imperva SecureSphere devices to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Imperva SecureSphere DSM RPM on your QRadar Console.
2. For each instance of Imperva SecureSphere, configure the Imperva SecureSphere appliance to communicate with QRadar. On your Imperva SecureSphere appliance, complete the following steps:
   a. Configure an alert action.
   b. Configure a system event action.
3. If QRadar does not automatically discover the Imperva SecureSphere log source, create a log source for each instance of Imperva SecureSphere on your network. Use the following table to define the Imperva SecureSphere-specific parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Imperva SecureSphere</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks
Adding a DSM
Configuring an alert action for Imperva SecureSphere
Configure your Imperva SecureSphere appliance to forward syslog events for firewall policy alerts to QRadar.

**Configuring a system event action for Imperva SecureSphere**

Configure your Imperva SecureSphere appliance to forward syslog system policy events to QRadar.

**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.

“Configuring an alert action for Imperva SecureSphere” on page 660

Configure your Imperva SecureSphere appliance to forward syslog events for firewall policy alerts to QRadar.

“Configuring a system event action for Imperva SecureSphere” on page 661

Configure your Imperva SecureSphere appliance to forward syslog system policy events to QRadar.

“Configuring Imperva SecureSphere V11.0 to V13 to send database audit records to QRadar” on page 663

To send database audit records from Imperva SecureSphere V11.0 to V13 IBM QRadar, create a custom action set, add an action interface, and then configure an audit policy.

---

**Configuring an alert action for Imperva SecureSphere**

Configure your Imperva SecureSphere appliance to forward syslog events for firewall policy alerts to QRadar.

**About this task**

Use the following list to define a message string in the `Message` field for each event type you want to forward:

**Attention:** The line breaks in the code examples might cause this configuration to fail. For each alert, copy the code blocks into a text editor, remove the line breaks, and paste as a single line in the `Custom Format` column.

**Database alerts (V9.5 and V10 to V13)**

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|
|${Alert.alertType}|${Alert.immediateAction}|Alert ID=${Alert.dn}
|devTimeFormat=[see note]|devTime=${Alert.createTime}
|Alert type=${Alert.alertType}|src=${Alert.sourceIp}|usrName=${Event.struct.user.user}|Application name=${Alert.applicationName}
|dst=${Event.destInfo.serverIp}|Alert ID=${Alert.dn}
|Severity=${Alert.severity}|Immediate Action=${Alert.immediateAction}
|SecureSphere Version=${SecureSphereVersion}
```

**File server alerts (V9.5 and V10 to V13)**

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|
|${Alert.alertType}|${Alert.immediateAction}|Alert ID=${Alert.dn}
|devTimeFormat=[see note]|devTime=${Alert.createTime}
|Alert type=${Alert.alertType}|src=${Alert.sourceIp}|usrName=${Event.struct.user.username}|Domain=${Event.struct.user.domain}
|Application name=${Alert.applicationName}|dst=${Event.destInfo.serverIp}
|Severity=${Alert.severity}|Immediate Action=${Alert.immediateAction}
|SecureSphere Version=${SecureSphereVersion}
```

**Web application firewall alerts (V9.5 and V10 to V13)**

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|
|${Alert.alertType}|${Alert.immediateAction}|Alert ID=${Alert.dn}
|devTimeFormat=[see note]|devTime=${Alert.createTime}
|Alert type=${Alert.alertType}|src=${Alert.sourceIp}
|usrName=${Alert.username}|Application name=${Alert.applicationName}
|Service name=${Alert.serviceName}|Alert Description=${Alert.description}
```
All alerts (V6.2 and V7 to V13 Release Enterprise Edition)

DeviceType=ImpervaSecuresphere Alert|an=${Alert.alertMetadata.alertName}|at=SecuresphereAlert|sp=${Event.sourceInfo.sourcePort}|s=${Event.sourceInfo.sourceIp}|d=${Event.destInfo.serverIp}|dp=${Event.destInfo.serverPort}|u=${Alert.username}|g=${Alert.serverGroupName}|ad=${Alert.description}

**Note:** The `devTimeFormat` parameter does not include a value because you can configure the time format on the SecureSphere appliance. Review the time format of your SecureSphere appliance and specify the appropriate time format.

**Procedure**

1. Log in to SecureSphere by using administrative privileges.
2. Click the **Policies** tab.
3. Click the **Action Sets** tab.
4. Generate events for each alert that the SecureSphere device generates:
   a) Click **New** to create a new action set for an alert.
   b) Move the action to the **Selected Actions** list.
   c) Expand the **System Log** action group.
   d) In the **Action Name** field, type a name for your alert action.
   e) From the **Apply to event type** list, select **Any event type**.
   f) Configure the following parameters:
      • In the **Syslog host** field, type the IP address of the QRadar appliance to which you want to send events.
      • In the **Syslog log level** list, select **INFO**.
      • In the **Message** field, define a message string for your event type.
   g) In the **Facility** field, type syslog.
   h) Select the **Run on Every Event** check box.
   i) Click **Save**.
5. To trigger syslog events, associate each of your firewall policies to an alert action:
   a) From the navigation menu, click **Policies > Security > Firewall Policy**.
   b) Select the policy that you want to use for the alert action.
   c) Click the **Policy** tab.
   d) From the **Followed Action** list, select your new action and configure the parameters.
      **Tip:** Configure established connections as either blocked, inbound, or outbound. Always allow applicable service ports.
   e) Ensure that your policy is configured as enabled and is applied to the appropriate server groups.
   f) Click **Save**.

### Configuring a system event action for Imperva SecureSphere

Configure your Imperva SecureSphere appliance to forward syslog system policy events to QRadar.

**About this task**

Use the following list to define a message string in the **Message** field for each event type you want to forward:
Attention: The line breaks in the code examples might cause this configuration to fail. For each alert, copy the code blocks into a text editor, remove the line breaks, and paste as a single line in the Custom Format column.

System events (V9.5 and V10 to V13)

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion} |${Event.eventType}
|Event ID=${Event.dn}|devTimeFormat=[see note]|devTime=${Event.createTime}
|Event Type=${Event.eventType}|Message=${Event.message}
|Severity=${Event.severity.displayName}|usrName=${Event.username}
|SecureSphere Version=${SecureSphereVersion}
```

Database audit records (V9.5 and V10 to V13)

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}
|${Event.struct.eventType}|Server Group=${Event.serverGroup}
|Service Name=${Event.serviceName}|Application Name=${Event.applicationName}
|Source Type=${Event.sourceInfo.eventSourceType}
|User Type=${Event.struct.user.userType}|usrName=${Event.struct.userGroup}
|Authenticated=${Event.struct.user.authenticated}|App User=${Event.struct.applicationUser}
|Server Group=${Event.serverGroup}
|Service Name=${Event.serviceName}|Application Name=${Event.applicationName}
|Source Type=${Event.sourceInfo.eventSourceType}
|User Type=${Event.struct.user.userType}|usrName=${Event.struct.userGroup}
|Authenticated=${Event.struct.user.authenticated}|App User=${Event.struct.applicationUser}
|Server Group=${Event.serverGroup}
|Service Name=${Event.serviceName}
```

All events (V6.2 and V7.x to V13 Release Enterprise Edition)

```
DeviceType=ImpervaSecuresphere Event|et=${Event.eventType}
|dc=Securesphere System Event|sp=${Event.sourceInfo.sourcePort}
|s=${Event.sourceInfo.sourceIp}|dp=${Event.destInfo.serverIp}
|u=${Event.username}|t=${Event.createTime}
```

Note: The devTimeFormat parameter does not include a value because you can configure the time format on the SecureSphere appliance. Review the time format of your SecureSphere appliance and specify the appropriate time format.

Procedure

1. Log in to SecureSphere by using administrative privileges.
2. Click the Policies tab.
3. Click the Action Sets tab.
4. Generate events for each alert that the SecureSphere device generates:
   a) Click New to create a new action set for an alert.
   b) Type a name for the new action set.
   c) Move the action to the Selected Actions list.
   d) Expand the System Log action group.
e) In the **Action Name** field, type a name for your alert action.

f) From the **Apply to event type** list, select **Any event type**.

g) Configure the following parameters:

- In the **Syslog host** field, type the IP address of the QRadar appliance to which you want to send events.
- In the **Syslog log level** list, select **INFO**.
- In the **Message** field, define a message string for your event type.

h) In the **Facility** field, type **syslog**.

i) Select the **Run on Every Event** check box.

j) Click **Save**.

5. To trigger syslog events, associate each of your system event policies to an alert action:

   a) From the navigation menu, click **Policies > System Events**.

   b) Select or create the system event policy that you want to use for the alert action.

   c) Click the **Followed Action** tab.

   d) From the **Followed Action** list, select your new action and configure the parameters.

   
   **Tip:** Configure established connections as either blocked, inbound, or outbound. Always allow applicable service ports.

   e) Click **Save**.

---

**Configuring Imperva SecureSphere V11.0 to V13 to send database audit records to QRadar**

To send database audit records from Imperva SecureSphere V11.0 to V13 IBM QRadar, create a custom action set, add an action interface, and then configure an audit policy.

**Procedure**

1. Create a custom action set:

   a) Log in to your Imperva SecureSphere system.

   b) In the **Main** workspace, select **Policies > Action Sets**.

   c) In the **Action Sets** pane, click the green plus sign icon.

   d) In the **Action Set** text box, type a name for the action set. For example, **QRadar SIEM**.

   e) From the **Apply to event type** list, select **Audit**.

   f) Click **Create**.

2. Add the action interface that you want to be part of the action set to the **Selected Actions** pane:

   a) Click the green up arrow icon, and then select **Gateway System Log > log audit event to System Log (Gateway System Log)**.

   b) Configure the following action interface parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type the name that you created for the action set. For example, QRadar SIEM.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select <strong>UDP</strong>.</td>
</tr>
<tr>
<td>Host</td>
<td>Type the IP address or the host name of the QRadar appliance for which you want to send events.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
<tr>
<td>Syslog Log Level</td>
<td>Info</td>
</tr>
<tr>
<td>Facility</td>
<td>syslog</td>
</tr>
</tbody>
</table>

**Message**

```
LEEF:1.0|Imperva|Secure
Sphere|${SecureSphereVersion}|${Alert.alertType}|${Alert.immediate
Action}|Alert ID=${Alert.dn}|devTime
Format=devTimeFormat=yyyy-MM-dd
HH:mm:ss.S|devTime=${Alert.createTime}
|Alert type=${Alert.alertType}|src=${Alert.sourceIp}|
usrName=${Event.
struct.user.user}|Application name=
${Alert.applicationName}|dst=${Event.
destInfo.serverIp}|Alert Description=
${Alert.description}|Severity=${Alert.
severity}|Immediate Action=${Alert.
immediateAction}|SecureSphere Version=${SecureSphereVersion}
```

**Attention:** The line breaks in the code example might cause this configuration to fail. For each alert, copy the code block below into a text editor, remove the line breaks, and paste as a single line in the **Message** field.

3. Configure an audit policy for the events that you want to send to QRadar:
   a) In the Main workspace, click **Policies > Audit**.
   b) Click **Create DB Service**.
   c) Type a name for the policy.
   d) Select **Use Existing**, and then select a policy from the list.
   e) Click the **Match Criteria** tab, and then enter the criteria for the policy.
   f) Click the **Apply To** tab, and then select the server group.
   g) Click the **External Logger** tab.
   h) From the **Syslog** list, select the **QRadar SIEM** that you configured.
   i) Optional: If you select a pre-defined policy from the **Syslog** list, configure the **Apply to** and **External Logger** fields.
   j) Click **Save**.

**What to do next**

You must define an audit policy or configure a pre-defined policy for each type of audit event that you want to send to QRadar.
Chapter 84. Infoblox NIOS

The IBM QRadar DSM for Infoblox NIOS collects Syslog events from an Infoblox NIOS device. To integrate Infoblox NIOS with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - Infoblox DSM RPM
2. Configure your Infoblox device to send syslog events to QRadar. For more information about sending syslog events from Infoblox, see your Infoblox NIOS documentation (https://docs.infoblox.com/display/ILP/NIOS).
3. Add an Infoblox log source on the QRadar Console. The following table describes the parameters that require specific values to collect Syslog events from Infoblox NIOS:

<table>
<thead>
<tr>
<th>Table 374. Infoblox NIOS Syslog log source parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Name</td>
</tr>
<tr>
<td>Log Source Type (Optional)</td>
</tr>
<tr>
<td>Log Source type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a log source” on page 4

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

Infoblox NIOS DSM specifications

The following table describes the specifications for the Infoblox NIOS DSM.

<table>
<thead>
<tr>
<th>Table 375. Infoblox NIOS DSM specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Specification</strong></td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>DSM name</td>
</tr>
<tr>
<td>RPM file name</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Supported versions</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>Event format</td>
</tr>
<tr>
<td>Specification</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
</tbody>
</table>
| Recorded event types          | • ISC Bind events  
                              • Linux DHCP events  
                              • Linux Server events  
                              • Apache events        |
| Automatically discovered?     | No                                                                   |
| Includes identity?            | Yes                                                                  |
| Includes custom properties?   | No                                                                   |
| More information              | For information about configuring your Infoblox NIOS device to send Syslog events to QRadar, see your Infoblox NIOS documentation (https://docs.infoblox.com/display/ILP/NIOS). |
Chapter 85. iT-CUBE agileSI

The iT-CUBE agileSI DSM for IBM QRadar can accept security-based and audit SAP events from agileSI installations that are integrated with your SAP system.

QRadar uses the event data that is defined as security risks in your SAP environment to generate offenses and correlate event data for your security team. SAP security events are written in Log Event Extended Format (LEEF) to a log file produced by agileSI. QRadar retrieves the new events by using the SMB Tail protocol. To retrieve events from agileSI, you must create a log source by using the SMB Tail protocol and provide QRadar credentials to log in and poll the LEEF formatted agileSI event file. QRadar is updated with new events each time the SMB Tail protocol polls the event file for new SAP events.

Configuring agileSI to forward events

To configure agileSI, you must create a logical file name for your events and configure the connector settings with the path to your agileSI event log.

About this task

The location of the LEEF formatted event file must be in a location viewable by Samba and accessible with the credentials you configure for the log source in IBM QRadar.

Procedure

1. In agileSI core system installation, define a logical file name for the output file that contains your SAP security events.

   SAP provides a concept that gives you the option to use platform-independent logical file names in your application programs. Create a logical file name and path by using transaction “FILE” (Logical File Path Definition) according to your organization’s requirements.

2. Log in to agileSI.


   Where:
   * `<sap-system-url>` is the IP address and port number of your SAP system, such as `<IP_address>:50041`.
   * `<client>` is the agent in your agileSI deployment.

3. From the menu, click Display/Change to enable change mode for agileSI.

4. From the toolbar, select Tools > Core Consumer Connector Settings.

   The Core Consumer Connector Settings are displayed.

5. Configure the following values:

   From the Consumer Connector list, select Q1 Labs.

6. Select the Active check box.

7. From the Connector Type list, select File.

8. From the Logical File Name field, type the path to your logical file name you configured in “Configuring agileSI to forward events ” on page 667.

   For example, /ITCUBE/LOG_FILES.

   The file that is created for the agileSI events is labeled LEEFYYYYDDMM.TXT where YYYYDDMM is the year, day, and month. The event file for the current day is appended with new events every time the extractor runs. iT-CUBE agileSI creates a new LEEF file for SAP events daily.
9. Click **Save**.

   The configuration for your connector is saved. Before you can complete the agileSI configuration, you must deploy the changes for agileSI by using extractors.

10. From the toolbar, select **Tools > Extractor Management**.

    The Extractor Management settings are displayed.

11. Click **Deploy all**.

    The configuration for agileSI events is complete. You are now ready to configure a log source in QRadar.

### Configuring an agileSI log source

IBM QRadar must be configured to log in and poll the event file by using the SMB Tail protocol.

**About this task**

The SMB Tail protocol logs in and retrieves events that are logged by agileSI in the LEEFYYYYDDMM.txt file.

**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 **iT-CUBE agileSI**.
9. Using the **Protocol Configuration** list, select **SMB Tail**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 376. SMB Tail protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Server Address</td>
</tr>
<tr>
<td>Domain</td>
</tr>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Confirm Password</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td>Log Folder Path</td>
</tr>
<tr>
<td>File Pattern</td>
</tr>
<tr>
<td>Force File Read</td>
</tr>
<tr>
<td>Recursive</td>
</tr>
<tr>
<td>Polling Interval (in seconds)</td>
</tr>
<tr>
<td>Throttle Events/Sec</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The configuration is complete. As your IT-CUBE agileSI log source retrieves new events, the Log Activity tab in QRadar is updated.
Chapter 86. Itron Smart Meter

The Itron Smart Meter DSM for IBM QRadar collects events from an Itron Openway Smart Meter by using syslog.

About this task
The Itron Openway Smart Meter sends syslog events to QRadar by using Port 514. For details of configuring your meter for syslog, see your Itron Openway Smart Meter documentation.

QRadar automatically discovers and creates a log source for syslog events from Itron Openway Smart Meters. However, you can manually create a log source for QRadar to receive syslog events. The following configuration steps are optional.

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 Itron Smart Meter.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Itron Openway Smart Meter installation.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The configuration is complete.
IBM QRadar supports a range of Juniper Networks DSMs.

### Juniper Networks AVT

The Juniper Networks Application Volume Tracking (AVT) DSM for IBM QRadar accepts events by using Java Database Connectivity (JDBC) protocol.

#### About this task

QRadar records all relevant events. To integrate with Juniper Networks NSM AVT data, you must create a view in the database on the Juniper Networks NSM server. You must also configure the Postgres database configuration on the Juniper Networks NSM server to allow connections to the database since, by default, only local connections are allowed.

**Note:** This procedure is provided as a guideline. For specific instructions, see your vendor documentation.

#### Procedure

1. Log in to your Juniper Networks AVT device command-line interface (CLI).
2. Open the following file:
   ```bash
   /var/netscreen/DevSvr/pgsql/data/pg_hba.conf
   ```
3. Add the following line to the end of the file:
   ```bash
   host all all <IP address>/32 trust
   ```
   Where: `<IP address>` is the IP address of your QRadar Console or Event Collector that you want to connect to the database.
4. Reload the Postgres service:
   ```bash
   su - nsm -c "pg_ctl reload -D /var/netscreen/DevSvr/pgsql/data"
   ```
5. As the Juniper Networks NSM user, create the view by using the following input:
   ```sql
   ```
   The view is created.
   You are now ready to configure the log source in QRadar.

### Configuring QRadar to receive events from a Juniper Networks AVT device

Administrators who do not have permission to create a database view because of policy restrictions can collect Juniper Networks AVT events with a log source that uses predefined queries.

#### About this task

Predefined queries are customized statements that can join data from separate tables when the database is polled by the JDBC protocol.

#### Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Click Add.
4. Configure the JDBC protocol for the log source. The following table describes the parameters that require specific values to collect events from Juniper Networks AVT by using the JDBC protocol:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Juniper Networks AVT</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>Postgres</td>
</tr>
<tr>
<td>Database Name</td>
<td>profilerDb</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name of the SQL server that hosts the Juniper Networks AVT database.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: MSDE - 1433, Postgres - 5432, MySQL - 3306, Sybase - 1521, Oracle - 1521, Informix - 9088, DB2 - 50000. If a database instance is used with the MSDE database type, you must leave the Port field blank.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name the log source can use to access the Juniper Networks AVT database.</td>
</tr>
</tbody>
</table>
Table 378. Juniper Networks AVT JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Type the password the log source can use to access the Juniper Networks AVT database. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>From the list, select Juniper Networks AVT.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>The Use Prepared Statements check box must be clear. The Juniper Networks AVT DSM does not support prepared statements.</td>
</tr>
<tr>
<td>Start Date and Time (Optional)</td>
<td>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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Type the polling interval, which is the amount of time between queries to the view you created. 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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
</tbody>
</table>

Note: Selecting a parameter value greater than 5 for the Credibility parameter weights your Juniper Networks AVT log source with a higher importance that is compared to other log sources in QRadar.

For more information about configuring the JDBC protocol, see c_logsource_JDBCprotocol.dita.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Juniper Networks DDoS Secure

Juniper Networks DDoS Secure is now known as NCC Group DDoS Secure.

Related concepts
“NCC Group DDoS Secure” on page 829
The IBM QRadar DSM for NCC Group DDoS Secure collects events from NCC Group DDoS Secure devices.

### Juniper Networks DX Application Acceleration Platform

The Juniper DX Application Acceleration Platform DSM for IBM QRadar uses syslog to receive events. QRadar records all relevant status and network condition events. Before you configure QRadar, you must configure your Juniper device to forward syslog events.

**Procedure**

1. Log in to the Juniper DX user interface.
2. Browse to the wanted cluster configuration (Services - Cluster Name), Logging section.
3. Select the **Enable Logging** check box.
4. Select your log format.
   - QRadar supports Juniper DX logs by using the common and perf2 formats only.
5. Select the log delimiter format.
   - QRadar supports comma delimited logs only.
6. In the **Log Host** section, type the IP address of your QRadar system.
7. In the **Log Port** section, type the UDP port on which you want to export logs.
8. You are now ready to configure the log source in QRadar.

### Configuring IBM QRadar to receive events from a Juniper DX Application Acceleration Platform

**About this task**

You can configure QRadar to receive events from a Juniper DX Application Acceleration Platform.

**Procedure**

From the **Log Source Type** list, select the **Juniper DX Application Acceleration Platform** option.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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

### Juniper Networks EX Series Ethernet Switch

The Juniper EX Series Ethernet Switch DSM for IBM QRadar accepts events by using syslog.

**About this task**

The Juniper EX Series Ethernet Switch DSM supports Juniper EX Series Ethernet Switches running Junos OS. Before you can integrate QRadar with a Juniper EX Series Ethernet Switch, you must configure your Juniper EX Series Switch to forward syslog events.

**Procedure**

1. Log in to the Juniper EX Series Ethernet Switch command line interface (CLI).
2. Type the following command:
   ```bash
   configure
   ```
3. Type the following command:

```
set system syslog host <IP address> <option> <level>
```

Where:

- `<IP address>` is the IP address of your QRadar.
- `<level>` is info, error, warning, or any.
- `<option>` is one of the following options from Table 379 on page 677.

### Table 379. Juniper Networks EX Series switch options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>All facilities</td>
</tr>
<tr>
<td>authorization</td>
<td>Authorization system</td>
</tr>
<tr>
<td>change-log</td>
<td>Configuration change log</td>
</tr>
<tr>
<td>conflict-log</td>
<td>Configuration conflict log</td>
</tr>
<tr>
<td>daemon</td>
<td>Various system processes</td>
</tr>
<tr>
<td>dfc</td>
<td>Dynamic flow capture</td>
</tr>
<tr>
<td>explicit-priority</td>
<td>Include priority and facility in messages</td>
</tr>
<tr>
<td>external</td>
<td>Local external applications</td>
</tr>
<tr>
<td>facility-override</td>
<td>Alternative facility for logging to remote host</td>
</tr>
<tr>
<td>firewall</td>
<td>Firewall filtering system</td>
</tr>
<tr>
<td>ftp</td>
<td>FTP process</td>
</tr>
<tr>
<td>interactive-commands</td>
<td>Commands run by the UI</td>
</tr>
<tr>
<td>kernel</td>
<td>Kernel</td>
</tr>
<tr>
<td>log-prefix</td>
<td>Prefix for all logging to this host</td>
</tr>
<tr>
<td>match</td>
<td>Regular expression for lines to be logged</td>
</tr>
<tr>
<td>pfe</td>
<td>Packet Forwarding Engine</td>
</tr>
<tr>
<td>user</td>
<td>User processes</td>
</tr>
</tbody>
</table>

For example:

```
set system syslog host <IP_address> firewall info
```

This command example configures the Juniper EX Series Ethernet Switch to send info messages from firewall filter systems to your QRadar.

4. Repeat steps 1-3 to configure any additional syslog destinations and options. Each additional option must be identified by using a separate syslog destination configuration.

5. You are now ready to configure the Juniper EX Series Ethernet Switch in QRadar.
Configuring IBM QRadar to receive events from a Juniper EX Series Ethernet Switch

You can configure QRadar to receive events from a Juniper EX Series Ethernet Switch:

**Procedure**

From the Log Source Type list, select Juniper EX-Series Ethernet Switch option.

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4

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

---

**Juniper Networks IDP**

The Juniper IDP DSM for IBM QRadar accepts events using syslog. QRadar records all relevant Juniper IDP events.

**About this task**

You can configure a sensor on your Juniper IDP to send logs to a syslog server:

**Procedure**

1. Log in to the Juniper NSM user interface.
2. In NSM, double-click the Sensor in Device Manager.
3. Select Global Settings.
4. Select Enable Syslog.
5. Type the Syslog Server IP address to forward events to QRadar.
6. Click OK.
7. Use Update Device to load the new settings onto the IDP Sensor.

The format of the syslog message that is sent by the IDP Sensor is as follows:

```
<day id>, <record id>, <timeReceived>,
<timeGenerated>, <domain>, <domainVersion>,
<deviceName>, <deviceIpAddress>, <category>,
<subcategory>, <src zone>, <src interface>,
<src addr>, <src port>, <nat src addr>,
<nat src port>, <dst zone>, <dst interface>,
<nat dst port>, <protocol>, <rule domain>,
<rule domainVersion>, <policyName>, <ruleBase>,
<ruleNumber>, <action>, <severity>,
<is alert>, <elapsed>, <bytes in>,
<bytes out>, <byteTotal>, <packet in>,
<packet out>, <packetTotal>, <repeatCount>,
<hasPacketData>, <varData Enum>, <misc-str>,
<user-str>, <app-str>, <uri-str>
```

See the following syslog example:

```
[syslog@juniper.net dayId="20060412" recordId="0"
timeRec="2006/04/12 21:52:21"
timeGen="2006/04/12 21:52:21" domain="" devDomVer="0" device_ip="IP_address"
cat="Predefined" attack="TROJAN:SUBSEVEN:SCAN" srczn="NULL" srcIntf="NULL"
srcAddr="Source_IP_address" srcPort="63396" natSrcAddr="NULL" natSrcPort="0"
dstzn="NULL" dstIntf="NULL" dstAddr=<Destination_IP_address" dstPort="27374"
natDstAddr="NULL" natDstPort="0" protocol="TCP" ruleDomain="" ruleVer="5"
policy="Policy2" rulebase="IDS" ruleNo="4" action="NONE" severity="LOW"
alert="no" elaspedTime="0" inbytes="0" outbytes="0" totBytes="0" inPak="0"
outPak="0" totPak="0" repCount="0" packetData="no" varEnum="31"
misc="<017>interface=eth2 user="NULL" app="NULL" uri="NULL""]
```
Configure a log source

Juniper NSM is a central management server for Juniper IDP. You can configure IBM QRadar to collect and represent the Juniper IDP alerts as coming from a central NSM, or QRadar can collect syslog from the individual Juniper IDP device.

To configure QRadar to receive events from Juniper Networks Secure Access device:

From the Log Source Type list, select Juniper Networks Intrusion Detection and Prevention (IDP).

For more information about Juniper IDP, see your Network and Security Manager documentation.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Juniper Networks Infranet Controller

The Juniper Networks Infranet Controller DSM for IBM QRadar accepts DHCP events by using syslog. QRadar records all relevant events from a Juniper Networks Infranet Controller.

About this task
Before you configure QRadar to integrate with a Juniper Networks Infranet Controller, you must configure syslog in the server. For more information on configuring your Juniper Networks Infranet Controller, consult your vendor documentation.

After you configure syslog for your Juniper Infranet Controller, you are now ready to configure the log source in QRadar.

To configure QRadar to receive events from your Juniper Networks Infranet Controller:

Procedure
From the Log Source Type list, select Juniper Networks Infranet Controller option.

For more information on configuring devices, see the IBM QRadar Managing Log Sources Guide.

Juniper Networks Firewall and VPN

The Juniper Networks Firewall and VPN DSM for IBM QRadar accepts Juniper Firewall and VPN events by using UDP syslog.

About this task
QRadar records all relevant firewall and VPN events.

Note: TCP syslog is not supported. You must use UDP syslog.

You can configure your Juniper Networks Firewall and VPN device to export events to QRadar.

Procedure
1. Log in to your Juniper Networks Firewall and VPN user interface.
3. Select the Enable Syslog Messages check box.
4. Type the IP address of your QRadar Console or Event Collector.
5. Click Apply.
You are now ready to configure the log source in QRadar.

**Related tasks**
- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 QRadar to receive events

**About this task**

You can configure QRadar to receive events from a Juniper Networks Firewall and VPN device.

**Procedure**

From the **Log Source Type** list, select **Juniper Networks Firewall and VPN** option.

For more information about your Juniper Networks Firewall and VPN device, see your Juniper documentation.

### Juniper Networks Junos OS

The Juniper Junos OS Platform DSM for IBM QRadar accepts events that use syslog, structured-data syslog, or PCAP (SRX Series only). QRadar records all valid syslog or structured-data syslog events.

**About this task**

The Juniper Junos OS Platform DSM supports the following Juniper devices that are running Junos OS:

- Juniper M Series Multiservice Edge Routing
- Juniper MX Series Ethernet Services Router
- Juniper T Series Core Platform
- Juniper SRX Series Services Gateway

For information on configuring PCAP data that uses a Juniper Networks SRX Series appliance, see “Configure the PCAP Protocol” on page 682.

**Note:** For more information about structured-data syslog, see RFC 5424 at the Internet Engineering Task Force: [http://www.ietf.org/](http://www.ietf.org/)

Before you configure QRadar to integrate with a Juniper device, you must forward data to QRadar using syslog or structured-data syslog.

**Procedure**

1. Log in to your Juniper platform command-line interface (CLI).
2. Include the following syslog statements at the set system hierarchy level:

   ```
   [set system] syslog {host (hostname) {facility <severity>; explicit-priority; any any; authorization any; firewall any; } source-address source-address; structured-data {brief;}}
   ```

   The following table lists and describes the configuration setting variables to be entered in the syslog statement.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Type the IP address or the fully qualified host name of your QRadar.</td>
</tr>
<tr>
<td>Facility</td>
<td>Define the severity of the messages that belong to the named facility with which it is paired. Valid severity levels are:</td>
</tr>
<tr>
<td></td>
<td>• Any</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Emergency</td>
</tr>
<tr>
<td></td>
<td>• Alert</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Error</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Notice</td>
</tr>
<tr>
<td></td>
<td>• Info</td>
</tr>
<tr>
<td></td>
<td>Messages with the specified severity level and higher are logged. The levels from emergency through info are in order from highest severity to lowest.</td>
</tr>
<tr>
<td>Source-address</td>
<td>Type a valid IP address configured on one of the router interfaces for system logging purposes.</td>
</tr>
<tr>
<td></td>
<td>The source-address is recorded as the source of the syslog message send to QRadar. This IP address is specified in the host host name statement set system syslog hierarchy level; however, this is not for messages directed to the other routing engine, or to the TX Matrix platform in a routing matrix.</td>
</tr>
<tr>
<td>structured-data</td>
<td>Inserts structured-data syslog into the data.</td>
</tr>
</tbody>
</table>

You can now configure the log source in QRadar.

The following devices are auto discovered by QRadar as a Juniper Junos OS Platform devices:

- Juniper M Series Multiservice Edge Routing
- Juniper MX Series Ethernet Services Router
- Juniper SRX Series
- Juniper EX Series Ethernet Switch
- Juniper T Series Core Platform

**Note:** Due to logging similarities for various devices in the JunOS family, expected events might not be received by the correct log source type when your device is automatically discovered. Review the automatically created log source for your device and then adjust the configuration manually. You can add any missed log source type or remove any incorrectly added log source type.

**Related concepts**

“TLS syslog protocol configuration options” on page 93
Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

**Related tasks**

“Adding a DSM” on page 4
Configuring QRadar to receive events from a Juniper Junos OS Platform device

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

You can manually configure IBM QRadar to receive events from a Juniper Junos OS Platform device.

Procedure

From the Log Source Type list, select one of the following options:

- Juniper JunOS Platform
- Juniper M-Series Multiservice Edge Routing
- Juniper MX-Series Ethernet Services Router
- Juniper SRX-series
- Juniper T-Series Core Platform

For more information about your Juniper device, see your vendor documentation.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4

Configure the PCAP Protocol

The Juniper SRX Series appliance supports forwarding of packet capture (PCAP) and syslog data to IBM QRadar.

Syslog data is forwarded to QRadar on port 514. The IP address and outgoing PCAP port number are configured on the Juniper Networks SRX Series appliance interface. The Juniper Networks SRX Series appliance must be configured in the following format to forward PCAP data:

<IP Address>:<Port>

Where,

- <IP Address> is the IP address of QRadar.
- <Port> is the outgoing port address for the PCAP data.

Note:

QRadar supports receiving PCAP data only from a single Juniper Networks SRX Series appliance for each event collector.

For more information about Configuring Packet Capture, see your Juniper Networks Junos OS documentation.

You are now ready to configure the new Juniper Networks SRX Log Source with PCAP protocol in QRadar.

Related tasks

“Configuring a New Juniper Networks SRX Log Source with PCAP” on page 683
The Juniper Networks SRX Series appliance is automatically discovered by IBM QRadar as a Juniper Junos OS Platform.

**Configuring a New Juniper Networks SRX Log Source with PCAP**

The Juniper Networks SRX Series appliance is automatically discovered by IBM QRadar as a Juniper Junos OS Platform.

**Before you begin**

Depending on your operating system, expected events might not be received when the log source is automatically detected. You can manually configure the log source.

**About this task**

QRadar detects the syslog data and adds the log source automatically. The PCAP data can be added to QRadar as Juniper SRX Series Services Gateway log source by using the PCAP Syslog combination protocol. Adding the **PCAP Syslog Combination** protocol after QRadar auto discovers the Junos OS syslog data adds a log source to your existing log source limit. Deleting the existing syslog entry, then adding the **PCAP Syslog Combination** protocol adds both syslog and PCAP data as single log source.

**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 **Juniper SRX-series Services Gateway**.
7. From the **Protocol Configuration** list, select **PCAP Syslog Combination**.
8. Type the **Log Source Identifier**.
9. Type the **Incoming PCAP Port**.
   
   To configure the **Incoming PCAP Port** parameter in the log source, enter the outgoing port address for the PCAP data as configured on the Juniper Networks SRX Series appliance interface. .
10. Click **Save**.
11. Select the auto discovered syslog-only Junos OS log source for your Juniper Networks SRX Series appliance.
12. Click **Delete**.
   
   A delete log source confirmation window is displayed.
13. Click **Yes**.
   
   The Junos OS syslog log source is deleted from the **Log Source** list. The **PCAP Syslog Combination** protocol is now visible in your log source list.
14. On the **Admin** tab, click **Deploy Changes**.

**Related tasks**

“Adding a DSM” on page 4  
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Juniper Networks Network and Security Manager**

The Juniper Networks Network and Security Manager (NSM) DSM for IBM QRadar accepts Juniper Networks NSM and Juniper Networks Secure Service Gateway (SSG) logs. All Juniper SSG logs must be forwarded through Juniper NSM to QRadar. All other Juniper devices logs can be forwarded directly to QRadar.

For more information on advanced filtering of Juniper Networks NSM logs, see your *Juniper Networks* vendor documentation.

To integrate a Juniper Networks NSM device with QRadar, you must complete the following tasks:

- “Configuring Juniper Networks NSM to export logs to syslog” on page 684
- “Configuring a log source for Juniper Networks NSM” on page 684

**Configuring Juniper Networks NSM to export logs to syslog**

Juniper Networks NSM uses the syslog server to export qualified log entries to syslog.

**About this task**

Configuring the syslog settings for the management system defines only the syslog settings for the management system. It does not export logs from the individual devices. You can enable the management system to export logs to syslog.

**Procedure**

1. Log in to the Juniper Networks NSM user interface.
2. From the Action Manager menu, select Action Parameters.
3. Type the IP address for the syslog server that you want to send qualified logs.
4. Type the syslog server facility for the syslog server to which you want to send qualified logs.
5. From the Device Log Action Criteria node, select the Actions tab.
   
   You are now ready to configure the log source in IBM QRadar.

**Configuring a log source for Juniper Networks NSM**

You can configure a log source in IBM QRadar for Juniper Networks NSM.

**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 Juniper Networks Network and Security Manager.
7. From the Protocol Configuration list, select Juniper NSM.
8. Configure the following values for the Juniper NSM protocol:
Table 380. Juniper NSM protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source.</td>
</tr>
<tr>
<td></td>
<td>The Log Source Identifier must be unique for the log source type.</td>
</tr>
<tr>
<td>IP</td>
<td>Type the IP address or host name of the Juniper Networks NSM server.</td>
</tr>
<tr>
<td>Inbound Port</td>
<td>Type the Inbound Port to which the Juniper Networks NSM sends communications.</td>
</tr>
<tr>
<td></td>
<td>The valid range is 0 - 65536. The default is 514.</td>
</tr>
<tr>
<td>Redirection Listen Port</td>
<td>Type the port to which traffic is forwarded.</td>
</tr>
<tr>
<td></td>
<td>The valid range is 0 - 65,536. The default is 516.</td>
</tr>
<tr>
<td>Use NSM Address for Log Source</td>
<td>Select this check box to use the Juniper NSM management server IP address instead of the log source IP address. By default, the check box is selected.</td>
</tr>
</tbody>
</table>

**Note:** In the QRadar interface, the Juniper NSM protocol configuration provides the option to use the Juniper Networks NSM IP address by selecting the **Use NSM Address for Log Source** check box. If you wish to change the configuration to use the originating IP address (clear the check box), you must log in to your QRadar Console, as a root user, and restart the Console (for an all-in-one system) or the Event Collector hosting the log sources (in a distributed environment) by using the `shutdown -r now` command.

**Juniper Networks Secure Access**

Juniper Networks Secure Access is now known as Pulse Secure Pulse Connect Secure.

**Related concepts**

“Pulse Secure Pulse Connect Secure” on page 951


**Juniper Networks Security Binary Log Collector**

The Juniper Security Binary Log Collector DSM for IBM QRadar can accept audit, system, firewall, and intrusion prevention system (IPS) events in binary format from Juniper SRX or Juniper Networks J Series appliances.

The Juniper Networks binary log file format is intended to increase performance when large amounts of data are sent to an event log. To integrate your device with QRadar, you must configure your Juniper appliance to stream binary formatted events, then configure a log source in QRadar.

See the following topics:

- “Configuring the Juniper Networks Binary Log Format” on page 686
- “Configuring a log source” on page 687
Configuring the Juniper Networks Binary Log Format

The binary log format from Juniper SRX or J Series appliances are streamed to IBM QRadar by using the UDP protocol. You must specify a unique port for streaming binary formatted events, because the standard syslog port for QRadar cannot understand binary formatted events.

About this task

The default port that is assigned to QRadar for receiving streaming binary events from Juniper appliances is port 40798.

Note: The Juniper Binary Log Collector DSM supports only events that are forwarded in Streaming mode. The Event mode is not supported.

Procedure

1. Log in to your Juniper SRX or J Series by using the command-line interface (CLI).
2. Type the following command to edit your device configuration:
   
   ```
   configure
   ```

3. Type the following command to configure the IP address and port number for streaming binary formatted events:
   
   ```
   set security log stream <Name> host <IP address> port <Port>
   ```
   
   Where:
   - `<Name>` is the name that is assigned to the stream.
   - `<IP address>` is the IP address of your QRadar Console or Event Collector.
   - `<Port>` is a unique port number that is assigned for streaming binary formatted events to QRadar. By default, QRadar listens for binary streaming data on port 40798. For a list of ports that are used by QRadar, see the IBM QRadar Common Ports List technical note.

4. Type the following command to set the security log format to binary:
   
   ```
   set security log stream <Name> format binary
   ```
   
   Where: `<Name>` is the name that you specified for your binary format stream in “Configuring the Juniper Networks Binary Log Format” on page 686.

5. Type the following command to enable security log streaming:
   
   ```
   set security log mode stream
   ```

6. Type the following command to set the source IP address for the event stream:
   
   ```
   set security log source-address <IP address>
   ```
   
   Where: `<IP address>` is the IP address of your Juniper SRX Series or Juniper J Series appliance.

7. Type the following command to save the configuration changes:
   
   ```
   commit
   ```

8. Type the following command to exit the configuration mode:
   
   ```
   exit
   ```

What to do next

The configuration of your Juniper SRX or J Series appliance is complete. You can now configure a log source in QRadar.
Configuring a log source

IBM QRadar does not automatically discover incoming Juniper Security Binary Log Collector events from Juniper SRX or Juniper J Series appliances.

About this task

If your events are not automatically discovered, you must manually create a log source by using the Admin tab in QRadar.

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 Juniper Security Binary Log Collector.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type an IP address or host name to identify the log source. The identifier address is the Juniper SRX or J Series appliance that generates the binary event stream.</td>
</tr>
<tr>
<td>Binary Collector Port</td>
<td>Specify the port number that is used by the Juniper Networks SRX or J Series appliance to forward incoming binary data to QRadar. The UDP port number for binary data is the same port that is configured in &quot;Configuring the Juniper Networks Binary Log Format&quot; on page 686, &quot;Configuring the Juniper Networks Binary Log Format&quot; on page 686. If you edit the outgoing port number for the binary event stream from your Juniper Networks SRX or J Series appliance, you must also edit your Juniper log source and update the Binary Collector Port parameter in QRadar. To edit the port: a. In the Binary Collector Port field, type the new port number for receiving binary event data. b. Click Save. The port update is complete and event collection starts on the new port number.</td>
</tr>
<tr>
<td>XML Template File Location</td>
<td>Type the path to the XML file used to decode the binary stream from your Juniper SRX or Juniper J Series appliance. By default, QRadar includes an XML template file for decoding the binary stream in the following directory: /opt/qradar/conf/security_log.xml</td>
</tr>
</tbody>
</table>
11. Click **Save**.
12. On the Admin tab, click **Deploy Changes**.

The configuration is complete. You can verify events that are forwarded to QRadar by viewing events in the **Log Activity** tab.

### Juniper Networks Steel-Belted Radius

The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

QRadar records all successful and unsuccessful login attempts. You can integrate Juniper Networks Steel-Belted Radius with QRadar by using one of the following methods:

- Configure Juniper Steel Belted-Radius to use WinCollect on Microsoft Windows operating systems. For more information, go to [Configuring Juniper Networks Steel-Belted Radius to forward Windows events to QRadar](#).
- Configure Juniper Steel-Belted Radius on Linux-based operating systems.
  - [Configuring Juniper Steel-Belted Radius by using the Syslog protocol](#).
  - [Configuring Juniper Steel-Belted Radius by using the TLS syslog protocol](#).
  - [Configuring Juniper Steel-Belted Radius by using the Log file protocol](#).

**Related concepts**

- [Configure Juniper Networks Steel-Belted Radius to forward Windows events to QRadar](#) You can forward Windows events to IBM QRadar by using WinCollect.

**Related tasks**

- [Configuring Juniper Networks Steel-Belted Radius to forward Syslog events to QRadar](#) Before you can add a log source in QRadar, configure your Juniper Networks Steel-Belted Radius device to send Syslog events to QRadar.

**Related reference**

- [Juniper Networks Steel-Belted Radius DSM specifications](#) The following table describes the specifications for the Juniper Steel-Belted Radius DSM.

### Juniper Networks Steel-Belted Radius DSM specifications

The following table describes the specifications for the Juniper Steel-Belted Radius DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Juniper Networks</td>
</tr>
</tbody>
</table>
Table 382. Juniper Networks Steel-Belted Radius DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSM name</td>
<td>Juniper Steel-Belted Radius</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-JuniperSteelBeltedRadius-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>5.x</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog, TLS Syslog, Log File, and WinCollect Juniper SBR</td>
</tr>
<tr>
<td>Event format</td>
<td></td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Related concepts
Juniper Networks Steel-Belted Radius
The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

Configure Juniper Networks Steel-Belted Radius to forward Windows events to QRadar
You can forward Windows events to IBM QRadar by using WinCollect.

To forward Windows events by using WinCollect, install WinCollect agent on a Windows host. Download the WinCollect agent setup file from the IBM Support website (https://www.ibm.com/support). Add a Juniper Steel-Belted Radius log source and assign it to the WinCollect agent.

The following table describes the parameters that require specific values for the WinCollect log source parameters.

Table 383. Juniper Steel-Belted Radius WinCollect Juniper SBR log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Juniper Steel-Belted Radius</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>WinCollect Juniper SBR</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the Windows device from which you want to collect Windows events. The log source identifier must be unique for the log source type.</td>
</tr>
<tr>
<td>Local System</td>
<td>Select the Local System check box to disable the remote collection of events for the log source. The log source uses local system credentials to collect and forward logs to QRadar. You need to configure the Domain, Username, and Password parameters if remote collection is required.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>The interval, in milliseconds, between times when WinCollect polls for new events.</td>
</tr>
</tbody>
</table>
Table 383. Juniper Steel-Belted Radius WinCollect Juniper SBR log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Active Directory Lookups</td>
<td>Do not select the check box.</td>
</tr>
<tr>
<td>WinCollect Agent</td>
<td>Select your WinCollect agent from the list.</td>
</tr>
<tr>
<td>Target Internal Destination</td>
<td>Use any managed host with an event processor component as an internal destination.</td>
</tr>
</tbody>
</table>


Related concepts
Juniper Networks Steel-Belted Radius
The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Juniper Networks Steel-Belted Radius to forward Syslog events to QRadar
Before you can add a log source in QRadar, configure your Juniper Networks Steel-Belted Radius device to send Syslog events to QRadar.

Procedure
1. Use SSH to log in to your Juniper Steel-Belted Radius device, as a root user.
2. Edit the following file:
   `/etc/syslog.conf`
3. Add the following information:
   `<facility>.<priority>@<IP address>`
   Where:
   • `<facility>` is the syslog facility, for example, local3.
   • `<priority>` is the syslog priority, for example, info.
   • `<IP address>` is the IP address of QRadar.
4. Save the file.
5. From the command-line, type the following command to restart syslog:
   `service syslog restart`

What to do next
You are now ready to add a log source in QRadar.

Related concepts
Juniper Networks Steel-Belted Radius
The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

**Related tasks**

“Configuring a Juniper Steel-Belted Radius log source by using the Syslog protocol” on page 691

If you want to collect Juniper Steel-Belted Radius logs from a Juniper Steel-Belted Radius device, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the Syslog protocol.

### Configuring a Juniper Steel-Belted Radius log source by using the Syslog protocol

If you want to collect Juniper Steel-Belted Radius logs from a Juniper Steel-Belted Radius device, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the Syslog protocol.

**Procedure**

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - DSMCommon RPM
   - Juniper Steel Belt Radius DSM RPM
   - 
   - 
2. Configure your Juniper Steel-Belted Radius device to send syslog events to QRadar.
3. Add a Syslog log source on the QRadar Console.

   The following table describes the parameters that require specific values to collect Syslog events from Juniper Steel-Belted Radius by using the Syslog protocol:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Juniper Steel-Belted Radius</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Related concepts**

Juniper Networks Steel-Belted Radius
The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 a Juniper Networks Steel-Belted Radius log source by using the TLS syslog protocol

If you want to collect Juniper Steel Belted-Radius logs from a Juniper Steel Belted-Radius device, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the TLS syslog protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - TLS Syslog protocol RPM
   - JuniperSteelBeltedRadius DSM RPM
2. Add a TLS Syslog log source on the QRadar Console.

The following table describes the parameters that require specific values to collect events from Juniper Steel-Belted Radius by using the TLS syslog protocol:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Juniper Steel-Belted Radius</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>TLS Syslog</td>
</tr>
</tbody>
</table>

Related concepts

Juniper Networks Steel-Belted Radius
The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

“TLS syslog protocol configuration options” on page 93
Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 a Juniper Steel-Belted Radius log source by using the Log File protocol

If you want to collect Juniper Steel-Belted Radius logs from Juniper Steel-Belted Radius, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the Log File protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - Log File protocol RPM
   - JuniperSteelBeltedRadius DSM RPM
2. Add a Log File protocol log source on the QRadar Console.

The following table describes the parameters that require specific values to collect Juniper Steel-Belted Radius events from Juniper Steel-Belted Radius by using the Log File protocol:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Juniper Steel-Belted Radius</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Log File</td>
</tr>
<tr>
<td>Service Type</td>
<td>FTP</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>The default directory is <code>/opt/JNPRsbr/radius/authReports/</code></td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>.*.*csv</td>
</tr>
<tr>
<td>Event Generator</td>
<td>Juniper SBR</td>
</tr>
</tbody>
</table>

**Related concepts**

Juniper Networks Steel-Belted Radius
The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

“Log File protocol configuration options” on page 62
To receive events from remote hosts, configure a log source to use the Log File protocol.

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Juniper Networks vGW Virtual Gateway**

The Juniper Networks vGW Virtual Gateway DSM for IBM QRadar accepts events by using syslog and NetFlow from your vGW management server or firewall.

**About this task**

QRadar records all relevant events, such as admin, policy, IDS logs, and firewall events. Before you configure a Juniper Networks vGW Virtual Gateway in QRadar, you must configure vGW to forward syslog events.

**Procedure**

1. Log in to your Juniper Networks vGW user interface.
2. Select **Settings**.
3. From **Security Settings**, select **Global**.
4. From **External Logging**, select one of the following options:
   - **Send Syslog from vGW management server** - Central logging with syslog event provided from a management server.
   - **Send Syslog from Firewalls** - Distribute logging with each Firewall Security VM providing syslog events.

   If you select the option **Send Syslog from vGW management server**, all events that are forwarded to QRadar contain the IP address of the vGW management server.
5. Type values for the following parameters:

<table>
<thead>
<tr>
<th>Table 387. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Syslog Server</td>
</tr>
<tr>
<td>Syslog Server Port</td>
</tr>
</tbody>
</table>

6. From the **External Logging** pane, click **Save**.

Only the changes that are made to the **External Logging** section are stored when you click **Save**. Any changes that are made to NetFlow require that you save by using the button within **NetFlow Configuration** section.

7. From the **NetFlow Configuration** pane, select the **enable** check box.

NetFlow does not support central logging from a vGW management server. From the **External Logging** section, you must select the option **Send Syslog from Firewalls**.

8. Type values for the following parameters:

<table>
<thead>
<tr>
<th>Table 388. Netflow parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>NetFlow collector address</td>
</tr>
<tr>
<td>Syslog Server Port</td>
</tr>
</tbody>
</table>

**Note:** QRadar typically uses port 2055 for NetFlow event data on QFlow Collectors. You must configure a different NetFlow collector port on your Juniper Networks vGW Series Virtual Gateway for NetFlow.

9. From the **NetFlow Configuration**, click **Save**.

10. You can now configure the log source in QRadar.

QRadar automatically detects syslog events that are forwarded from Juniper Networks vGW. If you want to manually configure QRadar to receive syslog events:

   From the **Log Source Type** list, select **Juniper vGW**.

   For more information, see your **Juniper Networks vGW** documentation.

**Related tasks**
- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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

---

**Juniper Networks Junos WebApp Secure**

The Juniper WebApp Secure DSM for IBM QRadar accepts events that are forwarded from Juniper Junos WebApp Secure appliances by using syslog.

Juniper Junos WebApp Secure provides incident logging and access logging events to QRadar. Before you can receive events in QRadar, you must configure event forwarding on your Juniper Junos WebApp Secure, then define the events that you want to forward.
Configuring syslog forwarding
To configure a remote syslog server for Juniper Junos WebApp Secure, you must use SSH to connect to a configuration interface. You can use the configuration interface to set up or configure core settings on your Juniper Junos WebApp Secure appliance.

Procedure
1. Use SSH on port 2022 to log in to your Juniper Junos WebApp device.
   https://<IP address>:<port>
   Where:
   • <IP address> is the IP address of your Juniper Junos WebApp Secure appliance.
   • <Port> is the port number of your Juniper Junos WebApp Secure appliance configuration interface.
   The default SSH configuration port is 2022.
2. From the Choose a Tool menu, select Logging.
3. Click Run Tool.
4. From the Log Destination menu, select Remote Syslog Server.
5. In the Syslog Server field, type the IP address of your QRadar Console or Event Collector.
6. Click Save.
7. From the Choose a Tool menu, select Quit.
8. Type Exit to close your SSH session.

What to do next
You are now ready to configure event logging on your Juniper Junos WebApp Secure appliance.

Configuring event logging
The Juniper Junos WebApp Secure appliance must be configured to determine which logs are forwarded to IBM QRadar.

Procedure
1. Using a web browser, log in to the configuration site for your Juniper Junos WebApp Secure appliance.
   https://<IP address>:<port>
   Where:
   • <IP address> is the IP address of your Juniper Junos WebApp Secure appliance.
   • <Port> is the port number of your Juniper Junos WebApp Secure appliance.
   The default configuration uses a port number of 5000.
2. From the navigation menu, select Configuration Manager.
3. From the configuration menu, select Basic Mode.
4. Click the Global Configuration tab and select Logging.
5. Click the link Show Advanced Options.
6. Configure the following parameters:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access logging: Log Level</strong></td>
<td>Click this option to configure the level of information that is logged when access logging is enabled. The options include the following levels: • 0 - Access logging is disabled. • 1 - Basic logging. • 2 - Basic logging with headers. • 3 - Basic logging with headers and body. <strong>Note:</strong> Access logging is disabled by default. It is suggested that you enable access logging only for debugging purposes. For more information, see your Juniper Junos WebApp Secure documentation.</td>
</tr>
<tr>
<td><strong>Access logging: Log requests before processing</strong></td>
<td>Click this option and select True to log the request before it is processed, then forward the event to QRadar.</td>
</tr>
<tr>
<td><strong>Access logging: Log requests to access log after processing</strong></td>
<td>Click this option and select True to log the request after it is processed. After Juniper Junos WebApp Secure processes the event, then it is forwarded to QRadar.</td>
</tr>
<tr>
<td><strong>Access logging: Log responses to access log after processing</strong></td>
<td>Click this option and select True to log the response after it is processed. After Juniper Junos WebApp Secure processes the event, then the event is forwarded to QRadar.</td>
</tr>
<tr>
<td><strong>Access logging: Log responses to access log before processing</strong></td>
<td>Click this option and select True to log the response before it is processed, then forward the event to QRadar.</td>
</tr>
<tr>
<td><strong>Incident severity log level</strong></td>
<td>Click this option to define the severity of the incident events to log. All incidents at or above the level that is defined are forwarded to QRadar. The options include the following levels: • 0 - Informational level and later incident events are logged and forwarded. • 1 - Suspicious level and later incident events are logged and forwarded. • 2 - Low level and later incident events are logged and forwarded. • 3 - Medium level and later incident events are logged and forwarded. • 4 - High level and later incident events are logged and forwarded.</td>
</tr>
<tr>
<td><strong>Log incidents to the syslog</strong></td>
<td>Click this option and select Yes to enable syslog forwarding to QRadar.</td>
</tr>
</tbody>
</table>

The configuration is complete. The log source is added to QRadar as Juniper Junos WebApp Secure events are automatically discovered. Events that are forwarded to QRadar by Juniper Junos WebApp Secure are displayed on the Log Activity tab of QRadar.
Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Juniper Junos WebApp Secure. The following configuration steps are optional.

Procedure

1. Log in to IBM 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 Juniper Junos WebApp Secure.
9. From the Protocol Configuration list, select Syslog.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Juniper Junos WebApp Secure appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

Juniper Networks WLC Series Wireless LAN Controller

IBM QRadar can collect and categorize syslog events from Juniper Networks WLC Series Wireless LAN Controllers.

To collect syslog events, you must configure your Juniper Networks Wireless LAN Controller to forward syslog events to QRadar. Administrators can use either the RingMaster interface or the command-line interface to configure syslog forwarding for their Juniper Networks Wireless LAN Controller appliance. QRadar automatically discovers and creates log sources for syslog events that are forwarded from Juniper Networks WLC Series Wireless LAN Controllers. QRadar supports syslog events from Juniper WLAN devices that run on Mobility System Software (MSS) V7.6.

To integrate Juniper WLC events with QRadar, administrators can complete the following tasks:

1. On your Juniper WLAN appliance, configure syslog server.
2. Use one of the following methods:
   - To use the RingMaster user interface to configure a syslog server, see “Configuring a syslog server from the Juniper WLC user interface” on page 698.
   - To use the command-line interface to configure a syslog server, see “Configuring a syslog server with the command-line interface for Juniper WLC” on page 698.
3. On your QRadar system, verify that the forwarded events are automatically discovered.
Configuring a syslog server from the Juniper WLC user interface

To collect events, you must configure a syslog server on your Juniper WLC system to forward syslog events to IBM QRadar.

Procedure

1. Log in to the RingMaster software.
2. From the Organizer panel, select a Wireless LAN Controller.
3. From the System panel, select Log.
4. From the Task panel, select Create Syslog Server.
5. In the Syslog Server field, type the IP address of your QRadar system.
6. In the Port field, type 514.
7. From the Severity Filter list, select a severity.
   Logging debug severity events can negatively affect system performance on the Juniper WLC appliance. It is a good practice for administrators to log events at the error or warning severity level and slowly increase the level to get the data you need. The default severity level is error.
8. From the Facility Mapping list, select a facility between local 0 - local 7.
9. Click Finish.

As events are generated by the Juniper WLC appliance, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded to QRadar. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created on the QRadar Console. The Log Activity tab displays events from the Juniper WLC appliance.

Configuring a syslog server with the command-line interface for Juniper WLC

To collect events, configure a syslog server on your Juniper WLC system to forward syslog events to IBM QRadar.

Procedure

1. Log in to the command-line interface of the Juniper WLC appliance.
2. To configure a syslog server, type the following command:
   
   ```
   set log server <ip-addr> [port 514 severity <severity-level> local-facility <facility-level>]
   ```
   
   Example:
   
   ```
   set log server 1.1.1.1 port 514 severity error local-facility local0.
   ```
3. To save the configuration, type the following command:
   
   ```
   save configuration
   ```

   As events are generated by the Juniper WLC appliance, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded to QRadar. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created. The Log Activity tab displays events from the Juniper WLC appliance.
Chapter 88. Kaspersky

IBM QRadar supports a range of Kaspersky DSMs.

Kaspersky CyberTrace

The IBM QRadar DSM for Kaspersky CyberTrace collects events from Kaspersky Feed Service.

To integrate Kaspersky CyberTrace with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the following RPMs on your QRadar Console.
   - DSMCommon RPM
   - Kaspersky CyberTrace DSM RPM
2. Install Kaspersky CyberTrace and configure Feed Service during the installation.
3. Integrate Kaspersky CyberTrace with QRadar.
   a. Configure forwarding events from QRadar to Kaspersky CyberTrace.
   b. Complete one of the following options.
      - Complete the verification test.
4. If QRadar does not automatically detect the log source, add a Kaspersky CyberTrace log source on the desired event collector. The following table describes the parameters that require specific values for Kaspersky CyberTrace event collection:

   **Note:** You need to clear the Coalescing Events check box when you configure the log source.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Kaspersky CyberTrace</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>KL_Threat_Feed_Service_V2</td>
</tr>
</tbody>
</table>

   **Related tasks**
   - “Adding a DSM” on page 4
   - “Adding a log source” on page 4

   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 Kaspersky CyberTrace to communicate with QRadar

To enable Kaspersky CyberTrace to communicate with QRadar, install and configure the Threat Feed Service on a device.

**Before you begin**
Before you install Kaspersky CyberTrace on a device, ensure that your device meets the hardware and software requirements. The requirements are specified in the Kaspersky CyberTrace documentation (https://help.kaspersky.com/CyberTrace/1.0/en-US/162416.htm).
About this task
You can install CyberTrace by using one of the following installation methods.

RPM installation
For this installation you must run the `run.sh` installation script, which installs the RPM package and runs the configurator. The configurator completes an interactive setup of Feed Service, Feed Utility, and Log Scanner.

DEB installation
The DEB installation is used on Linux systems that are based on Debian Linux. For this installation you must run the `run.sh` installation script, which installs the DEB package and runs the configurator. The configurator completes an interactive setup of Feed Service, Feed Utility, and Log Scanner.

TGZ installation
For this installation, you manually unpack the TGZ archive to the `/opt/kaspersky/ktfs` directory, create symbolic links to the configuration files and startup scripts, and register Feed Service in crontab. Then, you must manually run the configurator binary file and accept the End User License Agreement. The configurator completes an interactive setup of Feed Service, Feed Utility, and Log Scanner.

Procedure
1. Install CyberTrace by using the RPM/DEB method.
   a) Unpack the distribution kit contents to any directory on your system. The RPM/DEB package, installation script, and documentation is unpacked to this directory.
   b) Run the `run.sh` installation script. The installation script installs the RPM/DEB package, adds Feed Service to the list of services by using `chkconfig` or `systemd`, and then creates a cron job to update feeds every 30 minutes. Feed Service starts automatically on a system boot.
      After the RPM/DEB package is installed, the installation script automatically runs the configurator wizard.
   2. To accept the End user License Agreement, print Yes. Use PgUp and PgDn keys to navigate. Press q to quit.
   3. Specify the path to the certificate.
      a) If you want to use a demo certificate, click Enter.
      b) If you have a certificate for commercial feeds, specify the full path to it, and then click Enter.
         Note: The certificate must be in PEM format. The user who runs the configurator binary file must have read permissions for this file. The configurator creates a copy of the certificate file and stores it in a different directory. If you want to replace the certificate file, you must run the configurator again.
   4. Specify the proxy server settings by following the instructions. The specified proxy credentials are stored in encrypted form.
      To remove the specified proxy settings and stop using a proxy, you must manually delete the `ProxySettings` element and all nested elements from the Feed Utility configuration files.
   5. Specify the feeds that you want to use. The configurator obtains a list of feeds that are available for the certificate that you specified in Step 3.
   6. Specifying the connection parameters. The configuration automatically checks whether the specified connection parameters are correct. For example, the configurator checks that the SIEM software is present at the address and port for outbound events.
      The IP address must consist of four decimal octets that are separated by a dot. For example, `192.0.2.254` is a valid IP address.
      The following connection parameters are included:
      **IP address and port for incoming events**
      1. Feed Service listens on the specified address and port for incoming events.
      **QRadar connection string**
      1. Feed Service sends outbound events to the specified IP address and port or UNIX socket.
7. After the installation is complete, you can change the setting by using CybreTrace Web. See the product online help for details.

**What to do next**

Complete the verification test. For more information about the verification test, see “Completing the verification test” on page 701.

**Completing the verification test**

The verification test is a procedure that is used to check the capabilities of Kaspersky CyberTrace and to confirm the accuracy of the integration.

**About this task**

During this test you check to see whether events from QRadar are received by Feed Service, whether events from Feed Service are received by QRadar, and whether events are correctly parsed by Feed Service using the regular expressions.

The verification test file is a file that contains a set of events with URLs, IP addresses, and hashes. This file is located in the ./verification directory in the distribution kit. The name of this file is kl_verification_test.txt.

**Procedure**

1. Start Feed Service. For example, /etc/init.d/kl_feed_service start.
2. Ensure that the KL_Verification_Tool log source is added to QRadar, and routing rules are set in such a way that events from KL_Verification_Tool are sent to Feed Service.
3. Log in to the QRadar Console.
4. Click Admin > Add Filter.
5. From the Parameter list, select Log Source.
6. From the Operator list, select Equals.
7. From the Log Source list, in the Value group, select the required service name.
8. From the View list, select Real Time to clear the filter area. You can now browse the information about the service events.
9. In the Connection element of the Log Scanner configuration file ./log_sanner/log_scanner.conf, specify the IPV4 address and port of your QRadar Event Collector.
10. Run Log Scanner to send the kl_verification_test.txt file to QRadar (./log_scanner -p ../verification/kl_verification_test.txt)

The expected results that are displayed by QRadar depend on the feeds that you use. The following table displays the verification results.

<table>
<thead>
<tr>
<th>Feed used</th>
<th>Detected objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious URL Data Feed</td>
<td><a href="http://fakess123.nu">http://fakess123.nu</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://badb86360457963b90faac9ae17578ed.com">http://badb86360457963b90faac9ae17578ed.com</a></td>
</tr>
<tr>
<td></td>
<td>and many others, such as kaspersky.com/test/wmuf</td>
</tr>
<tr>
<td>Phishing URL Data Feed</td>
<td><a href="http://fakess123ap.nu">http://fakess123ap.nu</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://e77716a952f640b42e4371759a661663.com">http://e77716a952f640b42e4371759a661663.com</a></td>
</tr>
</tbody>
</table>
### Table 392. Verification test results (continued)

<table>
<thead>
<tr>
<th>Feed used</th>
<th>Detected objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet CnC URL Data Feed</td>
<td><a href="http://fakess123bn.nu">http://fakess123bn.nu</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://a7396d61cafe18a4cffbb3b428c9b60.com">http://a7396d61cafe18a4cffbb3b428c9b60.com</a></td>
</tr>
<tr>
<td>IP Reputation Data Feed</td>
<td>192.0.2.0</td>
</tr>
<tr>
<td></td>
<td>192.0.2.3</td>
</tr>
<tr>
<td>Malicious Hash Data Feed</td>
<td>FEAF2058298C1E174C2B79AFFC7CF4DF</td>
</tr>
<tr>
<td></td>
<td>44D88612FEA8A8F36DE82E1278ABB02F (The EICAR standard anti-virus test file.)</td>
</tr>
<tr>
<td></td>
<td>C912705B4BBB14EC7E78FA8B370532C9</td>
</tr>
<tr>
<td>Mobile Malicious Hash Data Feed</td>
<td>60300A92E1D0A55C7FDD360EE40A9DC1</td>
</tr>
<tr>
<td>Mobile Botnet Data Feed</td>
<td>001F6251169E6916C455495050A3FB8D (MD5 hash)</td>
</tr>
<tr>
<td></td>
<td>sdfed7233dsfg93acvblhsu/steallallsms.php (URL mask)</td>
</tr>
<tr>
<td>P-SMS Trojan Data Feed</td>
<td>FFAD85C453F0F29404491D8DAF0C646E (MD5 hash)</td>
</tr>
<tr>
<td>Demo Botnet CnC URL Data Feed</td>
<td><a href="http://5a015004f9fc05290d87e86d69c4b237.com">http://5a015004f9fc05290d87e86d69c4b237.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://fakess123bn.nu">http://fakess123bn.nu</a></td>
</tr>
<tr>
<td>Demo IP Reputation Data Feed</td>
<td>192.0.2.1</td>
</tr>
<tr>
<td></td>
<td>192.0.2.3</td>
</tr>
<tr>
<td>Demo Malicious Hash Data Feed</td>
<td>776735A8CA96DB15B422879DA599F474</td>
</tr>
<tr>
<td></td>
<td>FEAF2058298C1E174C2B79AFFC7CF4DF</td>
</tr>
<tr>
<td></td>
<td>44D88612FEA8A8F36DE82E1278ABB02F</td>
</tr>
</tbody>
</table>

### Configuring QRadar to forward events to Kaspersky CyberTrace

To have the Threat Feed Service check events that arrive in QRadar, you must configure QRadar to forward events to the Threat Feed Service.

**Procedure**

1. Log in to the QRadar Console UI.
2. Click the **Admin** tab, and select **System Configuration > Forwarding Destinations**.
3. In the **Forwarding Destinations** window, click **Add**.
4. In the Forwarding Destination Properties pane, configure the Forwarding Destination Properties.
Table 393. Forwarding Destination parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>An identifier for the destination. For example, KL_Threat_Feed_Service_V2</td>
</tr>
<tr>
<td>Destination Address</td>
<td>IP address of the host that runs the Threat Feed Service.</td>
</tr>
<tr>
<td>Event Format</td>
<td>JSON</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The port that is specified in kl_feed_service.conf InputSetting &gt; ConnectionString. The default value is 9995.</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Profile</td>
<td>Default profile</td>
</tr>
</tbody>
</table>

5. Click **Save**.

6. Click the **Admin** tab, and then select **System Configuration > Routing Rule**.

7. In the **Routing Rules** window, click **Add**.

8. In the **Routing Rules** window, configure the routing rule parameters.

Table 394. Routing Rules parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>An identifier for the rule name. For example, KL_Threat_Feed_Service_V2</td>
</tr>
<tr>
<td>Description</td>
<td>Create a description for the routing rule that you are creating.</td>
</tr>
<tr>
<td>Mode</td>
<td>Online</td>
</tr>
<tr>
<td>Forwarding Event Collector</td>
<td>Select the event collector that is used to forward events to the Threat Feed Service.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Events</td>
</tr>
<tr>
<td>Event Filters</td>
<td>Create a filter for the events that are going to be forwarded to the Threat Feed Service. To achieve maximum performance of the Threat Feed Service, only forward events that contain a URL or hash.</td>
</tr>
<tr>
<td>Routing Options</td>
<td>Enable Forward, and then select the <code>&lt;forwarding_destination&gt;</code> that you created.</td>
</tr>
</tbody>
</table>

9. Click **Save**.

**Kaspersky CyberTrace DSM specifications**

The following table describes the specifications for the Kaspersky CyberTrace DSM.

Table 395. Kaspersky CyberTrace DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Kaspersky Lab</td>
</tr>
</tbody>
</table>
### Table 395. Kaspersky CyberTrace DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSM name</td>
<td>Kaspersky CyberTrace</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-KasperskyCyberTrace-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>2.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Detect, Status, Evaluation</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Kaspersky website</td>
</tr>
</tbody>
</table>

### Sample event messages

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when using the syslog protocol for the Kaspersky CyberTrace DSM:

### Table 396. Kaspersky CyberTrace sample event message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| KL_Mobile_BotnetCnc_URL             | Botnet address         | Jul 10 10:10:14                                                     KL_Threat_Feed_Service_v2  
|                                     |                        | LEEF:1.0|Kaspersky Lab|%DATE% KL_Threat_Feed_Service_v2 LEEF:1.0|KasperskyLab|Threat Feed Service|2.0|EVENT%|CONTEXT%|2.0|KL_Mobile_BotnetCnc_URL|  
| url=xexample.com/                  |                        | testUser mask=xexample.com/xxx md5=-sha1=-sha256=-usrName=TestUser mask=xxx type=2  
| xxxxxxxxxxxxxxxxxxx/xxx            |                        | first_seen=04.01.2016 16:40 last_seen=27.01.2016 10:46 popularity=5         |

### Kaspersky Security Center

The IBM 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 397. Kaspersky Security Center DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Kaspersky</td>
</tr>
<tr>
<td>DSM name</td>
<td>Kaspersky Security Center</td>
</tr>
</tbody>
</table>
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, configure a JDBC log source to poll events from your Kaspersky Security Center database.

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:

     | Parameter                          | Value                                      |
     |------------------------------------|--------------------------------------------|
     | Log Source type                    | Kaspersky Security Center                   |
     | Protocol Configuration              | Syslog                                     |
     | Log Source Identifier              | Type the IP address or host name for the log source as an identifier for events that are collected from your Kaspersky Security Center appliance. |

   - If you use JDBC, configure the following parameters:

<pre><code> | Parameter                          | Value                                      |
 |------------------------------------|--------------------------------------------|
 | Log Source Description (Optional)  | Type a unique name for the log source.     |
</code></pre>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Kaspersky Security Center</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
</tbody>
</table>
| Log Source Identifier    | Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol.  
If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn’t collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2. |
| 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                     | Type the port number that is used by the database server. The default port for MSDE is 1433. You must enable and verify that you can communicate by using the port that you specified in the Port field.  
The JDBC configuration port must match the listener port of the Kaspersky Security Center database. To be able to communicate with QRadar, the Kaspersky Security Center 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. |
<p>| Username                 | Type the user name the log source can use to access the Kaspersky Security Center database.                                                                                                                                 |
| Password                 | Type the password the log source can use to access the Kaspersky Security Center database. The password can be up to 255 characters in length.                                                            |
| Confirm Password         | Confirm the password that is used to access the database. The confirmation password must be identical to the password entered in the Password field.                                                        |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Domain</td>
<td>If you did not select <strong>Use Microsoft JDBC, Authentication Domain</strong> is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>If you have multiple SQL server instances on your database server, type the database instance. If you use a non-standard port in your database configuration, or block access to port 1434 for SQL database resolution, you must leave the <strong>Database Instance</strong> parameter blank in your configuration.</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>From the list, select <strong>Kaspersky Security Center</strong>.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Select the <strong>Use Prepared Statements</strong> check box. Prepared statements allow the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
<tr>
<td>Start Date and Time (Optional)</td>
<td>Type the start date and time for database polling. The <strong>Start Date and Time</strong> 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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Type the polling interval, which is the amount of time between queries to the view you created. 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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Named Pipe Communication</td>
<td>If you did not select Use Microsoft JDBC, Use Named Pipe Communication is displayed.</td>
</tr>
<tr>
<td></td>
<td>MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>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 to ensure Named Pipe communication functions properly.</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select Use Microsoft JDBC, Use NTLMv2 is displayed.</td>
</tr>
<tr>
<td></td>
<td>Select the Use NTLMv2 check box.</td>
</tr>
<tr>
<td></td>
<td>This option forces MSDE connections to use the NTLMv2 protocol when they communicate with SQL servers that require NTLMv2 authentication.</td>
</tr>
<tr>
<td></td>
<td>If the Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable Use Microsoft JDBC.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If your connection supports SSL communication, select Use SSL. This option requires extra configuration on your Kaspersky Security Center database and also requires administrators to configure certificates on both appliances.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected Use Microsoft JDBC and Use SSL, the Microsoft SQL Server Hostname parameter is displayed.</td>
</tr>
<tr>
<td></td>
<td>You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

**Note:** Selecting a parameter value greater than 5 for the Credibility parameter weights your Kaspersky Security Center log source with a higher importance that is compared to other log sources in QRadar.

For more information about configuring the JDBC protocol, see `c_logsource_JDBCprotocol.dita`

**Related tasks**
- Adding a DSM
- Exporting syslog to QRadar from Kaspersky Security Center
Configure Kaspersky Security Center to forward syslog events to your IBM QRadar Console or Event Collector.

Creating a Database View for Kaspersky Security Center

To collect audit event data, you must create a database view on your Kaspersky server that is accessible to IBM QRadar.

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.

“Adding a DSM” on page 4

“Adding a log source” on page 4

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

To collect audit event data, you must create a database view on your Kaspersky server that is accessible to IBM QRadar.

About this task

To create a database view, you can download the klsq12.zip tool, which is available from Kaspersky or use another program that allows you to create database views. The instructions provided below define the steps required to create the dbo.events view using the Kaspersky Labs tool.

Procedure

1. From the Kaspersky Labs website, download the klsq12.zip file:


2. Copy klsq12.zip to your Kaspersky Security Center Administration Server.

3. Extract klsq12.zip to a directory.

4. The following files are included:

   • klsq12.exe
   • src.sql
   • start.cmd

5. In any text editor, edit the src.sql file.


7. Type the following Transact-SQL statement to create the dbo.events database view:

   ```sql
   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;
   ```

8. Save the src.sql file.

9. From the command line, navigate to the location of the klsq12 files.

10. Type the following command to create the view on your Kaspersky Security Center appliance:

    ```bash
    klsq12 -i src.sql -o result.xml
    ```

    The dbo.events view is created. You can now configure the log source in QRadar to poll the view for Kaspersky Security Center events.

    **Note:** Kaspersky Security Center database administrators should ensure that QRadar is allowed to poll the database for events using TCP port 1433 or the port configured for your log source. Protocol
connections are often disabled on databases by default and additional configuration steps might be required to allow connections for event polling. Any firewalls located between Kaspersky Security Center and QRadar should also be configured to allow traffic for event polling.

**Exporting syslog to QRadar from Kaspersky Security Center**

Configure Kaspersky Security Center to forward syslog events to your IBM 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**.
The IBM QRadar DSM for Kisco Information Systems SafeNet/i collects event logs from IBM i systems. The following table identifies the specifications for the Kisco Information Systems SafeNet/i DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Kisco Information Systems</td>
</tr>
<tr>
<td>DSM name</td>
<td>Kisco Information Systems SafeNet/i</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-KiscoInformationSystemsSafeNetI-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V10.11</td>
</tr>
<tr>
<td>Protocol</td>
<td>Log File</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Kisco Information Systems SafeNet/i</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Log File</td>
</tr>
<tr>
<td>Service Type</td>
<td>FTP</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>The IP or host name of Kisco Information systems SafeNet/i device.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>21</td>
</tr>
<tr>
<td>Remote User</td>
<td>The IBM i User ID that you created for QRadar in Kisco Information Systems SafeNet/i.</td>
</tr>
</tbody>
</table>
Table 401. Kisco Information Systems SafeNet/i log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Directory</td>
<td>Leave this field empty.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>.*</td>
</tr>
<tr>
<td>FTP Transfer Mode</td>
<td>BINARY</td>
</tr>
<tr>
<td>Processor</td>
<td>NONE</td>
</tr>
<tr>
<td>Event Generator</td>
<td>LINEBYLINE</td>
</tr>
<tr>
<td>File Encoding</td>
<td>US-ASCII</td>
</tr>
</tbody>
</table>

Related tasks
Adding a DSM
Configuring Kisco Information Systems SafeNet/i to communicate with QRadar
To collect SafeNet/i events, configure your IBM i system to accept FTP GET requests from your QRadar through Kisco Information Systems SafeNet/i.

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.

Configuring Kisco Information Systems SafeNet/i to communicate with QRadar
To collect SafeNet/i events, configure your IBM i 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 402. FTP access settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Name Format</td>
<td>*PATH</td>
</tr>
<tr>
<td>Initial List Format</td>
<td>*UNIX</td>
</tr>
<tr>
<td>Initial Library</td>
<td>*USRPRF</td>
</tr>
<tr>
<td>Initial Home Directory Path</td>
<td>The IFS directory</td>
</tr>
</tbody>
</table>

Procedure
1. Create an IFS directory on your IBM i system.
   a) Log in to your IBM i 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 402 on page 712.
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:

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate QRADAR Integration</td>
<td>Yes</td>
</tr>
<tr>
<td>This Host Identifier</td>
<td>The IP address or host name of the IBM i system.</td>
</tr>
<tr>
<td>IFS Path to QRADAR Alert File</td>
<td>Use the following format: /SafeNet/QRadar/*</td>
</tr>
</tbody>
</table>
```

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

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Notification Status</td>
<td>On</td>
</tr>
<tr>
<td>Summarized Alerts?</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```
Chapter 90. Lastline Enterprise

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Lastline</td>
</tr>
<tr>
<td>DSM name</td>
<td>Lastline Enterprise</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-LastlineEnterprise-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>6.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Anti-malware</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Lastline website (<a href="http://www.lastline.com">http://www.lastline.com</a>)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Lastline Enterprise</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks
- Adding a DSM
- 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.
- 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.

**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 91. Lieberman Random Password Manager

The Lieberman Random Password Manager DSM gives the option to integrate IBM QRadar with Lieberman Enterprise Random Password Manager and Lieberman Random Password Manager software by using syslog events in the Log Extended Event Format (LEEF).

About this task

The Lieberman Random Password Manager uses Port 514 to forward syslog events to QRadar. QRadar records all relevant password management events. For information on configuring syslog forwarding, see your vendor documentation.

QRadar automatically detects syslog events that are forwarded from Lieberman Random Password Manager and Lieberman Enterprise Random Password Manager devices. However, if you want to manually configure QRadar to receive events from these devices:

Procedure

From the Log Source Type list, select Lieberman Random Password Manager.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 92. LightCyber Magna

The IBM QRadar DSM for LightCyber Magna collects events from a LightCyber Magna device.

The following table describes the specifications for the LightCyber Magna DSM:

<table>
<thead>
<tr>
<th>Table 405. LightCyber Magna DSM specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>DSM name</td>
</tr>
<tr>
<td>RPM file name</td>
</tr>
<tr>
<td>Supported versions</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>Event format</td>
</tr>
<tr>
<td>Recorded event types</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Automatically discovered?</td>
</tr>
<tr>
<td>Includes identity?</td>
</tr>
<tr>
<td>Includes custom properties?</td>
</tr>
<tr>
<td>More information</td>
</tr>
</tbody>
</table>

To integrate LightCyber Magna 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
   - LightCyber Magna DSM RPM

2. Configure your LightCyber Magna device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a LightCyber Magna log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from LightCyber Magna:

<table>
<thead>
<tr>
<th>Table 406. LightCyber Magna log source parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

4. To verify that QRadar is configured correctly, review the following table to see an example of a normalized audit event message.
The following table shows a sample event message from LightCyber Magna:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Riskware</td>
<td>Misc Malware</td>
<td>LEEF:2.0</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 LightCyber Magna to communicate with QRadar

To collect LightCyber Magna events, configure your LightCyber Magna device to send syslog events to QRadar.

Procedure
1. Log in to the LightCyber Magna interface as administrator.
2. Click **Configuration** > **Syslog**.
3. Enable **Yes**.
4. Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td>The IP address or host name of the QRadar Event Collector.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>514</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>TCP</td>
</tr>
<tr>
<td><strong>Format</strong></td>
<td>LEEF</td>
</tr>
</tbody>
</table>

5. Click **Save**.
IBM QRadar supports the a range of Linux DSMs.

**Linux DHCP**

The Linux DHCP Server DSM for IBM QRadar accepts DHCP events using syslog. QRadar records all relevant events from a Linux DHCP Server. Before you configure QRadar to integrate with a Linux DHCP Server, you must configure syslog within your Linux DHCP Server to forward syslog events to QRadar.

For more information on configuring your Linux DHCP Server, consult the man pages or associated documentation for your DHCP daemon.

**Configuring a log source**

IBM QRadar automatically discovers and creates log sources for syslog events that are forwarded from Linux DHCP Servers. The following procedure is optional.

**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 Linux DHCP Server.
7. In the **Log Source Description** field, type a description for the log source.
8. From the **Log Source Type** list, select Linux **DHCP Server**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 409. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.

**Linux IPtables**

The Linux IPtables DSM for IBM QRadar accepts firewall IPtables events by using syslog. QRadar records all relevant from Linux IPtables where the syslog event contains any of the following words: Accept, Drop, Deny, or Reject. Creating a customized log prefix in the event payload enables QRadar to easily identify IPtables behavior.
Configuring IPtables

IPtables is a powerful tool, which is used to create rules on the Linux kernel firewall for routing traffic.

About this task

To configure IPtables, you must examine the existing rules, modify the rule to log the event, and assign a log identifier to your IPtables rule that can be identified by IBM QRadar. This process is used to determine which rules are logged by QRadar. QRadar includes any logged events that include the words: accept, drop, reject, or deny in the event payload.

Procedure

1. Using SSH, log in to your Linux Server as a root user.
2. Edit the IPtables file in the following directory:

```
/etc/iptables.conf
```

    **Note:** The file that contains the IPtables rules can vary according to the specific Linux operating system you are configuring. For example, a system using Red Hat Enterprise has the file in the `/etc/sysconfig/iptables` directory. Consult your *Linux operating system documentation* for more information about configuring IPtables.
3. Review the file to determine the IPtables rule you want to log.
   For example, if you want to log the rule that is defined by the entry, use:
   ```
   -A INPUT -i eth0 --dport 31337 -j DROP
   ```
4. Insert a matching rule immediately before each rule you want to log:
   ```
   -A INPUT -i eth0 --dport 31337 -j DROP -A INPUT -i eth0 --dport 31337 -j DROP
   ```
5. Update the target of the new rule to LOG for each rule you want to log:
   ```
   -A INPUT -i eth0 --dport 31337 -j LOG -A INPUT -i eth0 --dport 31337 -j DROP
   ```
6. Set the log level of the LOG target to a SYSLOG priority level, such as info or notice:
   ```
   -A INPUT -i eth0 --dport 31337 -j LOG --log-level info -A INPUT -i eth0 --dport 31337 -j DROP
   ```
7. Configure a log prefix to identify the rule behavior. Set the log prefix parameter to:
   ```
   Q1Target=<rule>
   ```
   Where `<rule>` is one of the following: **fw_accept, fw_drop, fw_reject, or fw_deny**.
   For example, if the rule that is logged by the firewall targets dropped events, the log prefix setting is:
   ```
   Q1Target=fw_drop
   ```
   ```
   -A INPUT -i eth0 --dport 31337 -j LOG --log-level info --log-prefix "Q1Target=fw_drop" -A INPUT -i eth0 --dport 31337 -j DROP
   ```
   **Note:** You must have a trailing space before the closing quotation mark.
8. Save and exit the file.
9. Restart IPtables using the following command:
   ```
   /etc/init.d/iptables restart
   ```
10. Open the syslog.conf file.
11. Add the following line:
    ```
    kern.<log level>@<IP address>
    ```
    Where:
• `<log level>` is the previously set log level.
• `<IP address>` is the IP address of QRadar.

12. Save and exit the file.
13. Restart the syslog daemon by using the following command:

```
/etc/init.d/syslog restart
```

After the syslog daemon restarts, events are forwarded to QRadar. IP table events that are forwarded from Linux Servers are automatically discovered and displayed in the **Log Activity** tab of QRadar.

### Configuring a log source

IBM QRadar automatically discovers and creates log sources for IP tables syslog events that are forwarded from Linux Servers. The following steps for configuring a log source are optional.

**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 Linux DHCP Server.
7. In the **Log Source Description** field, type a description for the log source.
8. From the **Log Source Type** list, select **Linux iptables Firewall**.
9. From the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for IP table events that are forwarded from your Linux Server.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete. IP table events that are forwarded from Linux Servers are automatically discovered and displayed in the **Log Activity** tab of QRadar.

For more information about configuring IP tables on Linux Servers, consult the man pages or your associated Linux documentation.

---

### Linux OS

The Linux OS DSM for IBM QRadar records Linux operating system events and forwards the events using syslog or syslog-ng.

If you are using syslog on a UNIX host, upgrade the standard syslog to a more recent version, such as, syslog-ng.

**Note:** Do not run both syslog and syslog-ng at the same time.

To integrate Linux OS with QRadar, select one of the following syslog configurations for event collection:

- “Configuring syslog on Linux OS” on page 724
- “Configuring syslog-ng on Linux OS” on page 724
You can also configure your Linux operating system to send audit logs to QRadar. For more information, see “Configuring Linux OS to send audit logs” on page 725.

**Supported event types**

The Linux OS DSM supports the following event types:
- cron
- HTTPS
- FTP
- NTP
- Simple Authentication Security Layer (SASL)
- SMTP
- SNMP
- SSH
- Switch User (SU)
- Pluggable Authentication Module (PAM) events.

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 syslog on Linux OS**

Configure the syslog protocol on Linux OS.

**Procedure**

1. Log in to your Linux OS device, as a root user.
2. Open the `/etc/syslog.conf` file.
3. Add the following facility information:
   ```
   authpriv.*@<IP address>
   ```
   Where: `<IP address>` is the IP address of IBM QRadar.
4. Save the file.
5. Restart syslog by using the following command:
   ```
   service syslog restart
   ```
6. Log in to the QRadar user interface.
7. Add a Linux OS log source.
8. On the Admin tab, click Deploy Changes.

   For more information on syslog, see your Linux operating system documentation.

**Configuring syslog-ng on Linux OS**

Configure Linux OS to use the syslog-ng protocol.

**Procedure**

1. Log in to your Linux OS device, as a root user.
2. Open the `/etc/syslog-ng/syslog-ng.conf` file.
3. Add the following facility information:
filter auth_filter{ facility(authpriv); }
destination auth_destination { tcp("<IP address>", port(514)); }
log{
source(<Sourcename>);
filter(auth_filter);
destination(auth_destination);
}

Where:
- `<IP address>` is the IP address of the IBM QRadar.
- `<Source name>` is the name of the source that is defined in the configuration file.

4. Save the file.
5. Restart syslog-ng by using the following command:
   ```
   service syslog-ng restart
   ```
6. Log in to the QRadar user interface.
7. Add a Linux OS log source.
8. On the Admin tab, click Deploy Changes.

For more information about syslog-ng, see your Linux operating system documentation.

Related tasks
“Adding a log source” on page 4
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 Linux OS to send audit logs
Configure Linux OS to send audit logs to QRadar.

About this task
This task applies to Red Hat Enterprise Linux V6 operating systems.
If you use a SUSE, Debian, or Ubuntu operating system, see your vendor documentation for specific steps for your operating system.

Procedure
1. Log in to your Linux OS device, as a root user.
2. Type the following command:
   ```
   yum install audit service auditd start chkconfig auditd on
   ```
3. Open the following file:
   ```
   /etc/audisp/plugins.d/syslog.conf
   ```
4. Verify that the parameters match the following values:
   ```
   active = yes direction = out path = builtin_syslog type = builtin args = LOG_LOCAL6 format = string
   ```
5. Open the following file:
   ```
   /etc/rsyslog.conf
   ```
6. Add the following line to the end of the file:
   ```
   local6.* @@<QRadar_Collector_IP_address>
   ```
7. Type the following commands:
service auditd restart
service syslog restart
8. Log in to the QRadar user interface.
9. Add a Linux OS log source.
10. Click Admin > Deploy Changes.

Related tasks
“Adding a log source” on page 4
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 94. LOGbinder

Configure your LOGbinder system to send event logs to IBM QRadar.

The following LOGbinder systems are supported:

- LOGbinder EX event collection from Microsoft Exchange Server.
- LOGbinder SP event collection from Microsoft SharePoint.
- LOGbinder SQL event collection from Microsoft SQL Server.

LOGbinder EX event collection from Microsoft Exchange Server

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>DSM name</td>
<td>Microsoft Exchange Server</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-MicrosoftExchange-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>LOGbinder EX V2.0</td>
</tr>
<tr>
<td>Protocol type</td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>LEEF</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Admin</td>
</tr>
<tr>
<td></td>
<td>Mailbox</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Included identity?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Microsoft Exchange website (<a href="http://www.office.microsoft.com/en-us/exchange/">http://www.office.microsoft.com/en-us/exchange/</a>)</td>
</tr>
</tbody>
</table>

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:
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 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.

LOGbinder SP event collection from Microsoft SharePoint

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>DSM name</td>
<td>Microsoft SharePoint</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-MicrosoftSharePoint-QRadar_version-build_number.noarch.rpm</td>
</tr>
</tbody>
</table>
Table 413. LOGbinder for Microsoft SharePoint specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported versions</td>
<td>LOGbinder SP V4.0</td>
</tr>
<tr>
<td>Protocol type</td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>LEEF</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Included identity?</td>
<td>No</td>
</tr>
</tbody>
</table>

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 414. Microsoft SharePoint log source parameters for LOGbinder event collection

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Microsoft SharePoint</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks

Adding a DSM
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 QRadar.

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.

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 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.

**LOGbinder SQL event collection from Microsoft SQL Server**

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>DSM name</td>
<td>Microsoft SQL Server</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-MicrosoftSQL-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>LOGBinder SQL V2.0</td>
</tr>
<tr>
<td>Protocol type</td>
<td>Syslog</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Included identity?</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| 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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Microsoft SQL Server</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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 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 95. McAfee

IBM QRadar supports a range of McAfee products.

McAfee Application / Change Control

The McAfee Application / Change Control DSM for IBM QRadar accepts change control events by using Java Database Connectivity (JDBC). QRadar records all relevant McAfee Application / Change Control events. This document includes information on configuring QRadar to access the database that contains events by using the JDBC protocol.

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.

You must refer to the Configure Database Settings on your Application/Change Control Management Console to configure the McAfee Application/Change Control DSM in QRadar.

5. Configure the parameters. The following table describes the JDBC protocol parameters that require specific values to collect events from McAfee Application/Change Control:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>McAfee Application/Change Control</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>MSDE</td>
</tr>
<tr>
<td>Database Name</td>
<td>Type the name of the McAfee Application / Change Control database.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>Type the IP address or host name of the McAfee Application / Change Control SQL Server.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port</td>
<td>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 McAfee Application / Change Control database. The McAfee Application / Change Control database must have incoming TCP connections enabled to communicate with QRadar. If you define a Database Instance when you use MSDE as the database type, you must leave the Port parameter blank in your configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name required to access the database.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password required to access the database. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Authentication Domain</td>
<td>If you did not select Use Microsoft JDBC, Authentication Domain is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Predefined Query (Optional)</td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the none option.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>Optional. Type 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 blocked access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.</td>
</tr>
<tr>
<td>Table Name</td>
<td>Type SCOR_EVENTS as the name of the table or view that includes the event records.</td>
</tr>
<tr>
<td>Select List</td>
<td>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 it's needed for your configuration. The list must contain the field that is defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Type AutoID as the compare field. The compare field is used to identify new events added between queries to the table.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.</td>
</tr>
</tbody>
</table>
### Table 417. McAfee Application/Change Control JDBC protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start Date and Time</strong> (Optional)</td>
<td>Type the start date and time for database polling in the following format: 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.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Type the polling interval, which 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.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td><strong>Use Named Pipe Communication</strong></td>
<td>If you did not select Use Microsoft JDBC, Use Named Pipe Communication is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
<tr>
<td><strong>Database Cluster Name</strong></td>
<td>If you selected 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 to ensure Named Pipe communication functions properly.</td>
</tr>
<tr>
<td><strong>Use NTLMv2</strong></td>
<td>If you did not select Use Microsoft JDBC, Use NTLMv2 is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td><strong>Use Microsoft JDBC</strong></td>
<td>If you want to use the Microsoft JDBC driver, you must enable Use Microsoft JDBC.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>Select this option if your connection supports SSL. This option appears only for MSDE.</td>
</tr>
<tr>
<td><strong>Microsoft SQL Server Hostname</strong></td>
<td>If you selected Use Microsoft JDBC and Use SSL, the Microsoft SQL Server Hostname parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

**Note:** Selecting a value greater than 5 for the **Credibility** parameter weights your McAfee Application / Change Control log source with a higher importance compared to other log sources in QRadar.

For more information about configuring the JDBC protocol, see [c_logsource_JDBCprotocol.dita](#).

6. Click **Save**.

7. On the **Admin** tab, click **Deploy Changes**.
Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

McAfee ePolicy Orchestrator

The IBM QRadar DSM for McAfee ePolicy Orchestrator collects events from a McAfee ePolicy Orchestrator device.

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

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>McAfee</td>
</tr>
<tr>
<td>DSM name</td>
<td>McAfee ePolicy Orchestrator</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-McAfeeEpo-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V3.5 to V5.x</td>
</tr>
</tbody>
</table>
| Protocol                 | JDBC
|                          | SNMPv1
|                          | SNMPv2
|                          | SNMPv3
|                          | TLS Syslog                                                |
| Recorded event types     | AntiVirus events                                          |
| Automatically discovered?| No                                                         |
| Includes identity?       | No                                                         |
| Includes custom properties?| No                                                       |

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

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console.
   - JDBC Protocol RPM
   - SNMP Protocol RPM
   - TLS Syslog Protocol RPM
   - DSMCommon RPM
   - McAfee ePolicy Orchestrator DSM RPM

2. Configure your McAfee ePolicy Orchestrator device to send events to QRadar.
   a. Add a registered server.
   b. Configure SNMP notifications, or the JDBC or TLS Syslog protocol.
c. Install the Java Cryptography Extension for high-level SNMP decryption algorithms.

3. Add a McAfee ePolicy Orchestrator log source on the QRadar Console. The following tables describe the SNMPv1, SNMPv2, SNMPv3, JDBC, and TLS Syslog protocol log source parameters that require specific values to collect events from McAfee ePolicy Orchestrator.

### Table 419. McAfee ePolicy Orchestrator SNMPv1 log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source type</td>
<td>McAfee ePolicy Orchestrator</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>SNMPv1</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>

### Table 420. McAfee ePolicy Orchestrator SNMPv2 log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source type</td>
<td>McAfee ePolicy Orchestrator</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>SNMPv2</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
<tr>
<td>Community</td>
<td>The SNMP community string for the SNMPv2 protocol, such as Public.</td>
</tr>
<tr>
<td>Include OIDs in Event Payload</td>
<td>To allow the McAfee ePolicy Orchestrator event payloads to be constructed as name-value pairs instead of the standard event payload format, enable the <strong>Include OIDs in Event Payload</strong> check box.</td>
</tr>
<tr>
<td>Important:</td>
<td>You must include OIDs in the event payload for processing SNMPv2 events for McAfee ePolicy Orchestrator.</td>
</tr>
</tbody>
</table>

### Table 421. McAfee ePolicy Orchestrator SNMPv3 log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source type</td>
<td>McAfee ePolicy Orchestrator</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>SNMPv3</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>
### Table 421. McAfee ePolicy Orchestrator SNMPv3 log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Protocol</td>
<td>The algorithm that you want to use to authenticate SNMPv3 traps:</td>
</tr>
<tr>
<td></td>
<td>• SHA uses Secure Hash Algorithm (SHA) as your authentication protocol.</td>
</tr>
<tr>
<td></td>
<td>• MD5 uses Message Digest 5 (MD5) as your authentication protocol.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>The password to authenticate SNMPv3. Your authentication password must include a minimum of 8 characters.</td>
</tr>
<tr>
<td>Decryption Protocol</td>
<td>Select the algorithm that you want to use to decrypt the SNMPv3 traps.</td>
</tr>
<tr>
<td></td>
<td>• DES</td>
</tr>
<tr>
<td></td>
<td>• AES128</td>
</tr>
<tr>
<td></td>
<td>• AES192</td>
</tr>
<tr>
<td></td>
<td>• AES256</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you select AES192 or AES256 as your decryption algorithm, you must install the Java Cryptography Extension. For more information about installing the Java Cryptography Extension on McAfee ePolicy Orchestrator, see Installing the Java Cryptography Extension.</td>
</tr>
<tr>
<td>Decryption Password</td>
<td>The password to decrypt SNMPv3 traps. Your decryption password must include a minimum of 8 characters.</td>
</tr>
<tr>
<td>User</td>
<td>The user name that was used to configure SNMPv3 on your McAfee ePO appliance.</td>
</tr>
<tr>
<td>Include OIDs in Event Payload</td>
<td>To allow the McAfee ePolicy Orchestrator event payloads to be constructed as name-value pairs instead of the standard event payload format, select the <strong>Include OIDs in Event Payload</strong> check box.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> You must include OIDs in the event payload for processing SNMPv3 events for McAfee ePolicy Orchestrator.</td>
</tr>
</tbody>
</table>

### Table 422. McAfee ePolicy Orchestrator JDBC log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source type</td>
<td>McAfee ePolicy Orchestrator</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
</tbody>
</table>
Table 422. McAfee ePolicy Orchestrator JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the <strong>Log Source Identifier</strong> value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the <strong>Log Source Identifier</strong> value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td><strong>Database Type</strong></td>
<td>Select MSDE from the list.</td>
</tr>
<tr>
<td><strong>Database Name</strong></td>
<td>The name of the McAfee ePolicy Orchestrator database.</td>
</tr>
<tr>
<td><strong>IP or Hostname</strong></td>
<td>The IP address or host name of the McAfee ePolicy Orchestrator SQL Server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Type the port number that is used by the database server. The default port for MSDE is 1433. You must enable and verify that you can communicate by using the port that you specified in the <strong>Port</strong> field. The JDBC configuration port must match the listener port of the McAfee ePolicy Orchestrator database. To be able to communicate with QRadar, the McAfee ePolicy Orchestrator database must have incoming TCP connections enabled. If you define a database instance that uses MSDE as the database type, you must leave the <strong>Port</strong> parameter blank in your configuration.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>A user account for QRadar in the database. The user name can be up to 255 alphanumeric characters in length and can include underscore (_) characters.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password that is required to connect to the database.</td>
</tr>
<tr>
<td><strong>Authentication Domain</strong></td>
<td>If you did not select <strong>Use Microsoft JDBC, Authentication Domain</strong> is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database Instance</td>
<td>The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or access is blocked to port 1433 for SQL database resolution, the Database Instance parameter must be blank in the log source configuration.</td>
</tr>
<tr>
<td>Predefined Query (Optional)</td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the none option.</td>
</tr>
</tbody>
</table>
| Table Name                             | A table or view that includes the event records as follows:  
  • For ePolicy Orchestrator 3.x, type Events.  
  • For ePolicy Orchestrator 4.x, type EPOEvents.  
  • For ePolicy Orchestrator 5.x, type EPOEvents |
| Select List                            | The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the Compare Field. |
| Compare Field                          | A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. Enables the protocol to identify events that were previously polled by the protocol to ensure that duplicate events are not created. |
| Use Prepared Statements                | Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements. |
| Start Date and Time (Optional)         | Type the start date and time for database polling in the following format: 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. |
| Polling Interval                       | Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value.                                               |
| EPS Throttle                           | The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000.                                                                                   |
### Table 422. McAfee ePolicy Orchestrator JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Named Pipe Communication</td>
<td>If you did not select <strong>Use Microsoft JDBC</strong>, <strong>Use Named Pipe Communication</strong> is displayed. Clear the <strong>Use Named Pipe Communication</strong> check box. When a Named Pipe connection is used, the user name and password must be the appropriate Windows authentication user name and password, not the MSDE database user name and password.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>If you selected <strong>Use Named Pipe Communication</strong>, the <strong>Database Cluster Name</strong> parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select <strong>Use Microsoft JDBC</strong>, <strong>Use NTLMv2</strong> is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable <strong>Use Microsoft JDBC</strong>.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option if your connection supports SSL. This option appears only for MSDE.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected <strong>Use Microsoft JDBC</strong> and <strong>Use SSL</strong>, the <strong>Microsoft SQL Server Hostname</strong> parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

### Table 423. McAfee ePolicy Orchestrator TLS Syslog log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>McAfee ePolicy Orchestrator</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>TLS Syslog</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>The mode by which your TLS connection is authenticated. If you select the <strong>TLS and Client Authentication</strong> option, you must configure the certificate parameters.</td>
</tr>
</tbody>
</table>
Table 423. McAfee ePolicy Orchestrator TLS Syslog log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Certificate Path</td>
<td>The absolute path to the client-certificate on disk. The certificate must be stored on the Console or Event Collector for this log source.</td>
</tr>
<tr>
<td>Certificate Type</td>
<td>The type of certificate to use for authentication. If you select the <strong>Provide Certificate</strong> option, you must configure the file paths for the server certificate and the private key.</td>
</tr>
<tr>
<td>Provided Server Certificate Path</td>
<td>The absolute path to the server certificate.</td>
</tr>
<tr>
<td>Provided Private Key Path</td>
<td>The absolute path to the private key. <strong>Note:</strong> The corresponding private key must be a DER-encoded PKCS8 key. The configuration fails with any other key format.</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>The <strong>Maximum Connections</strong> parameter controls how many simultaneous connections the TLS Syslog protocol can accept for each Event Collector. There is a limit of 1,000 connections across all TLS syslog log source configurations for each Event Collector. The default for each device connection is 50. <strong>Note:</strong> Automatically discovered log sources that share a listener with another log source, such as if you use the same port on the same event collector, count only one time towards the limit.</td>
</tr>
</tbody>
</table>

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

4. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from McAfee ePolicy Orchestrator:
### Table 424. McAfee ePolicy Orchestrator sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>

**Related concepts**

“SNMPv2 protocol configuration options” on page 83
You can configure a log source to use the SNMPv2 protocol to receive SNMPv2 events.

“SNMPv3 protocol configuration options” on page 83
You can configure a log source to use the SNMPv3 protocol to receive SNMPv3 events.

“TLS syslog protocol configuration options” on page 93
Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

**Related tasks**

“Adding a log source” on page 4
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 DSM” on page 4
“Configuring SNMP notifications on McAfee ePolicy Orchestrator” on page 744
To send SNMP events from McAfee ePolicy Orchestrator to IBM QRadar, you must configure SNMP notifications on your McAfee ePolicy Orchestrator device.

“Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator” on page 746
The Java™ Cryptography Extension (JCE) is a Java framework that is required for IBM QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your McAfee ePolicy Orchestrator (McAfee ePO) device.

**Adding a registered server to McAfee ePolicy Orchestrator**

To configure McAfee ePolicy Orchestrator to forward SNMP events, you must add a registered server to your McAfee ePolicy Orchestrator device.

**Procedure**

1. Log in to your McAfee ePolicy Orchestrator device.
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, and then 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 that you want to use:
   - If you use SNMPv2c, provide the Community name.
   - If you use SNMPv3, provide the SNMPv3 Security details.
8. To verify the SNMP configuration, click **Send Test Trap**.
9. Click **Save**.

**What to do next**

Configure SNMP notifications on your McAfee ePolicy Orchestrator device.

**Related tasks**

“Configuring SNMP notifications on McAfee ePolicy Orchestrator” on page 744

To send SNMP events from McAfee ePolicy Orchestrator to IBM QRadar, you must configure SNMP notifications on your McAfee ePolicy Orchestrator device.

**Configuring SNMP notifications on McAfee ePolicy Orchestrator**

To send SNMP events from McAfee ePolicy Orchestrator to IBM QRadar, you must configure SNMP notifications on your McAfee ePolicy Orchestrator device.

**Before you begin**

You must add a registered server to McAfee ePolicy Orchestrator before you complete the following steps.

**Procedure**

1. Select **Menu > Automation > Automatic Responses**.
2. Click **New Responses**, and then configure the following values.
   a. Type a name and description for the response.
   b. From the **Event group** list, select **ePO Notification Events**.
   c. From the **Event type** list, select **Threats**.
   d. From the **Status** list, select **Enabled**.
3. Click **Next**.
4. From the **Value** column, type a value to use for system selection, or click the ellipsis icon.
5. Optional: From the **Available Properties** list, select more filters to narrow the response results.
6. Click **Next**.
7. Select **Trigger this response for every event** and then click **Next**.
When you configure aggregation for your McAfee ePolicy Orchestrator responses, do not enable throttling.

8. From the Actions list, select **Send SNMP Trap**.

9. Configure the following values:

   a. From the list of SNMP servers, select the SNMP server that you registered when you added a registered server.

   b. From the **Available Types** list, select **List of All Values**.

   c. Click >> to add the event type that is associated with your McAfee ePolicy Orchestrator version. Use the following table as a guide:

<table>
<thead>
<tr>
<th>Available Types</th>
<th>Selected Types</th>
<th>ePolicy Orchestrator Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected UTC</td>
<td>{listOfDetectedUTC}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Received UTC</td>
<td>{listOfReceivedUTC}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Detecting Product IPv4 Address</td>
<td>{listOfAnalyzerIPV4}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Detecting Product IPv6 Address</td>
<td>{listOfAnalyzerIPV6}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Detecting Product MAC Address</td>
<td>{listOfAnalyzerMAC}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Source IPv4 Address</td>
<td>{listOfSourceIPV4}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Source IPv6 Address</td>
<td>{listOfSourceIPV6}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Source MAC Address</td>
<td>{listOfSourceMAC}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Source User Name</td>
<td>{listOfSourceUserName}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Target IPv4 Address</td>
<td>{listOfTargetIPV4}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Target IPv6 Address</td>
<td>{listOfTargetIPV6}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Target MAC</td>
<td>{listOfTargetMAC}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Target Port</td>
<td>{listOfTargetPort}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Threat Event ID</td>
<td>{listOfThreatEventID}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Threat Event ID</td>
<td>{listOfThreatEventID}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>Threat Severity</td>
<td>{listOfThreatSeverity}</td>
<td>4.5, 5.1</td>
</tr>
<tr>
<td>SourceComputers</td>
<td></td>
<td>4.0</td>
</tr>
<tr>
<td>AffectedComputerIPs</td>
<td></td>
<td>4.0</td>
</tr>
<tr>
<td>EventIDs</td>
<td></td>
<td>4.0</td>
</tr>
<tr>
<td>TimeNotificationSent</td>
<td></td>
<td>4.0</td>
</tr>
</tbody>
</table>

10. Click **Next**, and then click **Save**.

**What to do next**

1. Add a log source in QRadar.

2. Install the Java Cryptography Extension for high-level SNMP decryption algorithms.

**Related tasks**

“Adding a log source” on page 4

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 the Java Cryptography Extension on McAfee ePolicy Orchestrator” on page 746
The Java™ Cryptography Extension (JCE) is a Java framework that is required for IBM QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your McAfee ePolicy Orchestrator (McAfee ePO) device.

**Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator**

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

**Procedure**

1. Download the latest version of the Java™ Cryptography Extension from the following website:  
   The Java™ Cryptography Extension version must match the version of the Java™ installed on your McAfee ePO device.

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

   `<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 IBM 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 Java Cryptography Extension from the following website:  
   The Java 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 QRadar Event Collector as a root user.

4. Copy the JCE JAR files to the following directory on your QRadar Console or Event Collector:

   `/opt/ibm/java-x86_64/jre/lib/security/`

   **Note:** The JCE JAR files are only copied to the system that receives the AES192 or AE256 encrypted files.

5. Restart the QRadar services by typing one of the following commands:
   - If you are using QRadar 7.2.x, type `service ecs-ec restart`.
   - If you are using QRadar 7.3.0, type `systemctl restart ecs-ec.service`.
   - If you are using QRadar 7.3.1, type `systemctl restart ecs-ec-ingress.service`.

746 IBM QRadar : QRadar DSM Configuration Guide
Sample event message
Use this sample event message as a way of verifying a successful integration with QRadar. The following table provides a sample event message when using the JDBC protocol for the McAfee ePolicy Orchestrator DSM:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| Host intrusion detected | Notice             | AutoID: "231426750" AutoGUID: "995F34BA-4CA3-4CEF-B259-5E678106884E" ServerID: "QRADAR
SERVER1" ReceivedUTC: "2014-07-23 08:02:13.553" DetectedUTC: "2014-07-23 07:55:11.0" AgentGUID:
"2AB7C0C3-23C5-4FBD-B0A6-9A39B0029E" Analyzer:
"HOSTIPS_8000" AnalyzerName: "McAfee Host Intrusion Prevention" AnalyzerVersion: "8.0.0" Analyzer
Hostname: "QRADARANALYZER" AnalyzerIPV4: "739325208" AnalyzerIPV6: "[B@e00e408" AnalyzerMAC: "001cc4e0
Hostname: "null" SourceIPV4: "739325208" SourceIPV6: "[B@7d03cef5" SourceMAC: "null" SourceUserName: 
"QRADAR\SYSTEM" SourceProcessName: "C:\WINNT\SYSTEM32\SERVICES.EXE" SourceURL: "file://C:\WINNT\SYSTEM32
\SERVICES.EXE" TargetHostname: "QRADAR" TargetIPV4: 
"739325208" TargetIPV6: "[B@ef5e07d2" TargetMAC: "00005E005300" TargetUserName: "null" TargetPort: 
"null" TargetProtocol: "null" TargetProcessName: 
"null" TargetFileName: "null" ThreatCategory: 
"hip.Registry" ThreatEventID: "18000" ThreatSeverity: 
"2" ThreatName: "915" ThreatType: "modify" Threat
ActionTaken: "hip.reaction.permit" ThreatHandled: "false" TheTimestamp: 
"[B@6d04e225"

McAfee Network Security Platform (Formerly known as McAfee Intrushield)

The IBM QRadar McAfee Network Security Platform DSM accepts events that use syslog. QRadar records all relevant events.

Before you configure QRadar to integrate with a McAfee Network Security Platform device, you must select your McAfee Network Security Platform device version.

- To collect alert events from McAfee Intrushield V2.x - V5.x, see “Configuring alert events for McAfee
Intrushield V2.x - V5.x” on page 747.
- To collect alert events from McAfee Network Security Platform V6.x - V7.x, see “Configuring alert events for McAfee Network Security Platform V6.x and V7.x” on page 748.
- To collect fault notification events from McAfee Network Security Platform V6.x - V7.x, see “Configuring fault notification events for McAfee Network Security Platform V6.x and V7.x” on page 750.

Configuring alert events for McAfee Intrushield V2.x - V5.x

To collect alert notification events from McAfee Intrushield, administrators must configure a syslog forwarder to send events to IBM QRadar.

Procedure

1. Log in to the McAfee Intrushield Manager user interface.
2. In the dashboard click Configure.
3. From the Resource Tree, click the root node (Admin-Domain-Name).
4. Select **Alert Notification > Syslog Forwarder**.
5. Type the Syslog Server details.
   - The **Enable Syslog Forwarder** must be configured as Yes.
   - The **Port** must be configured to 514.
6. Click **Edit**.
7. Choose one of the following versions:

<table>
<thead>
<tr>
<th>Table 426. McAfee Intrushield V2.x - V5.x custom message formats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
</tbody>
</table>
   | Unpatched McAfee Intrushield V2.x systems     | `$ALERT_ID$|$ALERT_TYPE$|"$ATTACK_NAME$"
   |                                               | `$ATTACK_ID$|$ATTACK_SEVERITY$|$ATTACK_SIGNATURE$
   |                                               | `$ATTACK_CONFIDENCE$|$ADMIN_DOMAIN$|$SENSOR_NAME$
   |                                               | `$INTERFACE$|$SOURCE_IP$|$SOURCE_PORT$|$DESTINATION_IP$
   |                                               | `$DESTINATION_PORT$`                                  |
   |-----------------------------------------------|
   | McAfee Intrushield that has patches applied to | `$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$
   | update to V3.x - V5.x                          | "$IV_ATTACK_NAME$
   |                                               | `$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$
   |                                               | `$IV_ATTACK_CONFIDENCE$`
   |                                               | `$IV_ADMIN_DOMAIN$|$IV_SENSOR_NAME$|$IV_INTERFACE$
   |                                               | `$IV_SOURCE_IP$|$IV_SOURCE_PORT$`
   |                                               | `$IV_DESTINATION_IP$|$IV_DESTINATION_PORT$`         |

**Note**: The custom message string must be entered as a single line without carriage returns or spaces. McAfee Intrushield appliances that do not have software patches that are applied use different message strings than patched systems. McAfee Intrushield expects the format of the custom message to contain a dollar sign ($) as a delimiter before and after each alert element. If you are missing a dollar sign for an element, then the alert event might not be formatted properly.

If you are unsure what event message format to use, contact McAfee Customer Support.
8. Click **Save**.

As events are generated by McAfee Intrushield, they are forwarded to the syslog destination that you specified. The log source is automatically discovered after enough events are forwarded by the McAfee Intrushield appliance. It typically takes a minimum of 25 events to automatically discover a log source.

**What to do next**
Administrators can log in to the QRadar Console and verify that the log source is created on the QRadar Console and that the **Log Activity** tab displays events from the McAfee Intrushield appliance.

**Configuring alert events for McAfee Network Security Platform V6.x and V7.x**
To collect alert notification events from McAfee Network Security Platform, administrators must configure a syslog forwarder to send events to IBM QRadar.

**Before you begin**
To collect alert notification events from McAfee Network Security Platform, you need McAfee Network Security Platform Manager.

**Procedure**
1. Log in to the **McAfee Network Security Platform Manager** user interface.
2. On the **Network Security Manager** dashboard, click **Configure**.
3. Expand the **Resource Tree**, click **IPS Settings** node.
4. Click the **Alert Notification** tab.
5. On the **Alert Notification** menu, click the **Syslog** tab.
6. Configure the following parameters to forward alert notification events:

| Table 427. McAfee Network Security Platform v6.x & 7.x alert notification parameters |
|----------------------------------|-------------------------------------|
| Parameter                        | Description                                         |
| Enable Syslog Notification       | Select Yes to enable syslog notifications for McAfee Network Security Platform. You must enable this option to forward events to QRadar. |
| Admin Domain                     | Select any of the following options:          |
|                                  | • Current - Select this check box to send syslog notifications for alerts in the current domain. This option is selected by default. |
|                                  | • Children - Select this check box to send syslog notifications for alerts in any child domains within the current domain. |
| Server Name or IP Address        | Type the IP address of your QRadar Console or Event Collector. This field supports both IPv4 and IPv6 addresses. |
| UDP Port                         | Type 514 as the UDP port for syslog events. |
| Facility                         | Select a syslog facility value. |
| Severity Mappings                | Select a value to map the informational, low, medium, and high alert notification level to a syslog severity. |
|                                  | The options include the following levels: |
|                                  | • Emergency - The system is down or unusable. |
|                                  | • Alert - The system requires immediate user input or intervention. |
|                                  | • Critical - The system should be corrected for a critical condition. |
|                                  | • Error - The system has non-urgent failures. |
|                                  | • Warning - The system has a warning message that indicates an imminent error. |
|                                  | • Notice - The system has notifications, no immediate action required. |
|                                  | • Informational - Normal operating messages. |
| Send Notification If             | Select the following check boxes: |
|                                  | • The attack definition has this notification option explicitly enabled |
|                                  | • The following notification filter is matched, and From the list, select Severity Informational and later. |
| Notify on IPS Quarantine Alert   | Select No as the notify on IPS quarantine option. |
| Message Preference               | Select the Customized option. |

7. From the Message Preference field, click Edit to add a custom message filter.
8. To ensure that alert notifications are formatted correctly, type the following message string:

```$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IVAttack_TIME$
|"$IV_ATTACK_NAME$"|$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$
|$IV_ATTACK_SIGNATURE$|$IV_ATTACK_CONFIDENCES$|$IV_ADMIN_DOMAIN$
|$IV_SENSOR_NAMES$|$IV_INTERFACE$|$IV_SOURCE_IP$|$IV_SOURCE_PORT$
|$IV_DESTINATION_IPS$|$IV_DESTINATION_PORTS$|$IV_DIRECTION$
|$IV_SUB_CATEGORY$```
Note: The custom message string must be entered as a single line without carriage returns or spaces. McAfee Network Security Platform expects the format of the custom message to contain a dollar sign ($) as a delimiter before and after each alert element. If you are missing a dollar sign for an element, then the alert event might not be formatted properly.

You might require a text editor to properly format the custom message string as a single line.

9. Click Save.

As alert events are generated by McAfee Network Security Platform, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded by the McAfee Network Security Platform appliance. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next
Administrators can log in to the QRadar Console and verify that the log source is created on the QRadar Console and that the Log Activity tab displays events from the McAfee Network Security Platform appliance.

Configuring fault notification events for McAfee Network Security Platform V6.x and V7.x
To integrate fault notifications with McAfee Network Security Platform, you must configure your McAfee Network Security Platform to forward fault notification events.

Procedure
1. Log in to the McAfee Network Security Platform Manager user interface.
2. On the Network Security Manager dashboard, click Configure.
3. Expand the Resource Tree, click IPS Settings node.
4. Click the Fault Notification tab.
5. In the Alert Notification menu, click the Syslog tab.
6. Configure the following parameters to forward fault notification events:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Syslog Notification</td>
<td>Select Yes to enable syslog notifications for McAfee Network Security Platform. You must enable this option to forward events to QRadar.</td>
</tr>
<tr>
<td>Admin Domain</td>
<td>Select any of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Current - Select this check box to send syslog notifications for alerts in the current domain. This option is selected by default.</td>
</tr>
<tr>
<td></td>
<td>• Children - Select this check box to send syslog notifications for alerts in any child domains within the current domain.</td>
</tr>
<tr>
<td>Server Name or IP Address</td>
<td>Type the IP address of your QRadar Console or Event Collector. This field supports both IPv4 and IPv6 addresses.</td>
</tr>
<tr>
<td>Port</td>
<td>Type 514 as the port for syslog events.</td>
</tr>
<tr>
<td>Facilities</td>
<td>Select a syslog facility value.</td>
</tr>
</tbody>
</table>
Table 428. McAfee Network Security Platform V6.x - V7.x fault notification parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Severity Mappings</strong></td>
<td>Select a value to map the informational, low, medium, and high alert notification level to a syslog severity.</td>
</tr>
<tr>
<td></td>
<td>The options include the following levels:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Emergency</strong> - The system is down or unusable.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alert</strong> - The system requires immediate user input or intervention.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Critical</strong> - The system should be corrected for a critical condition.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Error</strong> - The system has non-urgent failures.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Warning</strong> - The system has a warning message that indicates an imminent error.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Notice</strong> - The system has notifications, no immediate action required.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Informational</strong> - Normal operating messages.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Forward Faults with severity level</th>
<th>Select <strong>Informational and later</strong>.</th>
</tr>
</thead>
</table>

| Message Preference | Select the **Customized** option.                                              |

7. From the **Message Preference** field, click **Edit** to add a custom message filter.

8. To ensure that fault notifications are formatted correctly, type the following message string:

   ```
   |%INTRUSHIELD-FAULT|$IV_FAULT_NAME$|$IV_FAULT_TIME$|
   ```

   **Note:** The custom message string must be entered as a single line with no carriage returns. McAfee Network Security Platform expects the format of the custom message syslog information to contain a dollar sign ($) delimiter before and after each element. If you are missing a dollar sign for an element, the event might not parse properly.

9. Click **Save**.

   As fault events are generated by McAfee Network Security Platform, they are forwarded to the syslog destination that you specified.

**What to do next**

You can log in to the QRadar Console and verify that the **Log Activity** tab contains fault events from the McAfee Network Security Platform appliance.

**McAfee Web Gateway**

You can configure McAfee Web Gateway to integrate with IBM QRadar.

Use one of the following methods:

- “Configuring McAfee Web Gateway to communicate with QRadar (syslog)” on page 752
- “Configuring McAfee Web Gateway to communicate with IBM QRadar (log file protocol)” on page 754

**Note:** McAfee Web Gateway is formerly known as McAfee WebWasher.

The following table identifies the specifications for the McAfee Web Gateway DSM:
**Table 429. McAfee Web Gateway DSM specifications**

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>McAfee</td>
</tr>
<tr>
<td>DSM</td>
<td>McAfee Web Gateway</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-McAfeeWebGateway-qradarversion-buildnumber.noarch</td>
</tr>
<tr>
<td>Supported versions</td>
<td>v6.0.0 and later</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog, log file protocol</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>All relevant events</td>
</tr>
<tr>
<td>Automatically discovered</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>McAfee website (<a href="http://www.mcafee.com">http://www.mcafee.com</a>)</td>
</tr>
</tbody>
</table>

**McAfee Web Gateway DSM integration process**

You can integrate McAfee Web Gateway DSM with IBM QRadar.

Use the following procedure:

- Download and install the most recent version of the McAfee Web Gateway DSM RPM on your QRadar Console.
- For each instance of McAfee Web Gateway, configure your McAfee Web Gateway VPN system to enable communication with QRadar.
- If QRadar does not automatically discover the log source, for each McAfee Web Gateway server you want to integrate, create a log source on the QRadar Console.
- If you use McAfee Web Gateway v7.0.0 or later, create an event map.

**Related tasks**

“Configuring McAfee Web Gateway to communicate with QRadar (syslog)” on page 752

“Configuring McAfee Web Gateway to communicate with IBM QRadar (log file protocol)” on page 754

“Creation of an event map for McAfee Web Gateway events” on page 755

**Configuring McAfee Web Gateway to communicate with QRadar (syslog)**

To collect all events from McAfee Web Gateway, you must specify IBM QRadar as the syslog server and configure the message format.

**Procedure**

1. Log in to your McAfee Web Gateway console.
2. On the **Toolbar**, click **Configuration**.
3. Click the **File Editor** tab.
4. Expand the **Appliance Files** and select the file `/etc/rsyslog.conf`. 
The file editor displays the `rsyslog.conf` file for editing.

5. Modify the `rsyslog.conf` file to include the following information:

```
# send access log to qradar *.info;
daemon. != info;
mail. none; authpriv. none;
cron. none -/var/log/messages *.info; mail. none;
authpriv. none;
cron. none
@<IP Address>:<Port>
```

Where:
- `<IP Address>` is the IP address of QRadar.
- `<Port>` is the syslog port number, for example 514.

6. Click **Save Changes**.

You are now ready to import a policy for the syslog handler on your McAfee Web Gateway appliance. For more information, see “Importing the Syslog Log Handler” on page 753.

**Importing the Syslog Log Handler**

**About this task**

To import a policy rule set for the syslog handler:

**Procedure**

1. From the support website, download the following compressed file:
   `log_handlers-1.1.tar.gz`
2. Extract the file.
   The extract file provides XML files that are version dependent to your McAfee Web Gateway appliance.

<table>
<thead>
<tr>
<th>Version</th>
<th>Required XML file</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Web Gateway V7.0</td>
<td>syslog_loghandler_70.xml</td>
</tr>
<tr>
<td>McAfee Web Gateway V7.3</td>
<td>syslog_loghandler_73.xml</td>
</tr>
</tbody>
</table>

3. Log in to your McAfee Web Gateway console.
4. Using the menu toolbar, click **Policy**.
5. Click **Log Handler**.
6. Using the menu tree, select **Default**.
7. From the **Add** list, select **Rule Set from Library**.
8. Click **Import from File** button.
9. Navigate to the directory containing the syslog_handler file you downloaded and select `syslog_loghandler.xml` as the file to import.
   **Note:** If the McAfee Web Gateway appliance detects any conflicts with the rule set, you must resolve the conflict. For more information, see your **McAfee Web Gateway documentation**.
10. Click **OK**.
11. Click **Save Changes**.
12. You are now ready to configure the log source in QRadar.

QRadar automatically discovers syslog events from a McAfee Web Gateway appliance.

If you want to manually configure QRadar to receive syslog events, select McAfee Web Gateway from the Log Source Type list.

Related tasks
“Adding a log source” on page 4
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 McAfee Web Gateway to communicate with IBM QRadar (log file protocol)
The McAfee Web Gateway appliance gives the option to forward event log files to an interim file server for retrieval by QRadar.

Procedure
1. From the support website, download the following file:
   
   `log_handlers-1.1.tar.gz`
2. Extract the file.
   This gives you the access handler file that is needed to configure your McAfee Web Gateway appliance.
   
   `access_log_file_loghandler.xml`
3. Log in to your McAfee Web Gateway console.
4. Using the menu toolbar, click Policy.
   
   **Note:** If there is an existing access log configuration in your McAfee Web Gateway appliance, you must delete the existing access log from the Rule Set Library before you add the access_log_file_loghandler.xml.
5. Click Log Handler.
6. Using the menu tree, select Default.
7. From the Add list, select Rule Set from Library.
8. Click Import from File button.
9. Navigate to the directory that contains the access_log_file_loghandler.xml file you downloaded and select syslog_loghandler.xml as the file to import.
   
   When the rule set is imported for access_log_file_loghandler.xml, a conflict can occur stating the Access Log Configuration exists already in the current configuration and a conflict solution is presented.
10. If the McAfee Web Gateway appliance detects that the Access Log Configuration exists already, select the Conflict Solution: Change name option that is presented to resolve the rule set conflict.
   
   For more information on resolving conflicts, see your McAfee Web Gateway vendor documentation.
   
   You must configure your access.log file to be pushed to an interim server on an auto rotation. It does not matter if you push your files to the interim server based on time or size for your access.log file. For more information on auto rotation, see your McAfee Web Gateway vendor documentation.
   
   **Note:** Due to the size of access.log files that are generated, it is suggested that you select the option GZIP files after rotation in your McAfee Web Gate appliance.
11. Click OK.
12. Click Save Changes.
   
   **Note:** By default McAfee Web Gateway is configured to write access logs to the /opt/mwg/log/user-defined-logs/access.log/ directory.
What to do next
You are now ready to configure QRadar to receive access.log files from McAfee Web Gateway. For more information, see “Pulling data by using the log file protocol” on page 755.

Pulling data by using the log file protocol
A log file protocol source allows IBM QRadar to retrieve archived log files from a remote host. The McAfee Web Gateway DSM supports the bulk loading of access.log files by using the log file protocol source. The default directory for the McAfee Web Gateway access logs is the /opt/mwg/log/user-defined-logs/access.log/ directory.

About this task
You can now configure the log source and protocol in QRadar.

Procedure
1. To configure QRadar to receive events from a McAfee Web Gateway appliance, select McAfee Web Gateway from the Log Source Type list.
2. To configure the protocol, you must select the Log File option from the Protocol Configuration list.
3. To configure the File Pattern parameter, you must type a regex string for the access.log file, such as access[0-9]+\log.

   Note: If you selected to GZIP your access.log files, you must type access[0-9]+\log\gz for the File Pattern field and from the Processor list, select GZIP.

Creation of an event map for McAfee Web Gateway events
Event mapping is needed for events that are collected from McAfee Web Gateway v7.0.0 and later, which are identified as Unknown and not covered by the base QID map.

You can individually map each event for your device to an event category in IBM QRadar. Mapping events allows QRadar to identify, coalesce, and track recurring events from your network devices. Until you map an event, some events that are displayed in the Log Activity tab for McAfee Web Gateway are categorized as Unknown, and some events might be already assigned to an existing QID map. Unknown events are easily identified as the Event Name column and Low Level Category columns display Unknown.

Discovering unknown events
This procedure ensures that you map all event types and that you do not miss events that are not generated frequently, repeat this procedure several times over a period.

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 the log source group or Other.
   Log sources that are not assigned to a group are categorized as Other.
6. From the Log Source list, select your McAfee Web Gateway log source.
7. Click Add Filter.
   The Log Activity tab is displayed with a filter for your log source.
8. From the View list, select Last Hour.
   Any events that are generated by the McAfee Web Gateway DSM in the last hour are displayed. Events that are displayed as Unknown in the Event Name column or Low Level Category column require event mapping.
Note: You can save your existing search filter by clicking Save Criteria.
You are now ready to modify the event map.

Modifying the event map
Modify an event map to manually categorize events to a QRadar Identifier (QID) map.

About this task
Any event that is categorized to a log source can be remapped to a new QRadar Identifier (QID).

Note: Events that do not have a defined log source cannot be mapped to an event. Events without a log source display SIM Generic Log in the Log Source column.

Procedure
1. On the Event Name column, double-click an unknown event for McAfee Web Gateway.
   The detailed event information is displayed.
2. Click Map Event.
3. From the Browse for QRadar Identifier 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 categorization.
   • From the Low-Level Category list, select a low-level event categorization.
   • From the Log Source Type list, select a log source type.
   The Log Source Type list gives the option to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, McAfee Web Gateway provides policy events, you might select another product that likely captures similar events.
   To search for a QID by name, type a name in the QID/Name field.
   The QID/Name field gives the option to filter the full list of QIDs for a specific word, for example, policy.
4. Click Search.
   A list of QIDs are displayed.
5. Select the QID that you want to associate to your unknown event.
6. Click OK.
   QRadar maps any additional events that are forwarded from your device with the same QID that matches the event payload. The event count increases each time that the event is identified by QRadar.
   If you update an event with a new QRadar Identifier (QID) map, past events that are stored in QRadar are not updated. Only new events are categorized with the new QID.
The MetaInfo MetaIP DSM for IBM QRadar accepts MetaIP events by using syslog.

**About this task**
QRadar records all relevant and available information from the event. Before you configure a MetaIP device in QRadar, you must configure your device to forward syslog events. For information on configuring your MetaInfo MetaIP appliance, see your vendor documentation.

After you configure your MetaInfo MetaIP appliance, the configuration for QRadar is complete. QRadar automatically discovers and creates a log source for syslog events that are forwarded from MetaInfo MetaIP appliances. However, you can manually create a log source for QRadar to receive syslog events. The following configuration steps are optional.

To manually configure a log source for MetaInfo MetaIP:

**Procedure**

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   - The Data Sources pane is displayed.
4. Click the Log Sources icon.
   - The Log Sources window is displayed.
5. Click Add.
   - The Add a log source window is displayed.
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 Metainfo MetaIP.
   - The syslog protocol configuration is displayed.
10. Configure the following values:
   
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your MetaInfo MetaIP appliances.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   - The configuration is complete.
Chapter 97. Microsoft

IBM QRadar supports a range of Microsoft products.

Microsoft Azure

The IBM QRadar DSM for Microsoft Azure collects events from a Microsoft Azure Log Integration service or Microsoft Azure Event Hubs.

To integrate Microsoft Azure with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console.
   - DSMCommon RPM
   - Microsoft Azure DSM RPM

2. Optional: Configure your Microsoft Azure Log Integration service to send syslog events to QRadar. If QRadar does not automatically detect the Syslog log source, add a Microsoft Azure log source on the QRadar Console. The following table describe the parameters that require specific values for Microsoft Azure event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Microsoft Azure</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the device that sends Microsoft Azure events to QRadar.</td>
</tr>
</tbody>
</table>

   a. RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console.
      - Protocol Common RPM
      - Microsoft Azure Event Hubs Protocol RPM
      
      Note: QRadar 7.2.8 Patch 7 and later is required for Microsoft Azure Event Hubs Protocol RPM.
   b. QRadar does not automatically detect the Microsoft Azure Event Hubs Protocol. For more information about configuring the protocol, go to Configuring QRadar to collect events from Microsoft Azure Event Hubs by using the Microsoft Azure Event Hubs protocol.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Azure Log Integration service to communicate with QRadar**

To collect events from Microsoft Azure, you must install Microsoft Azure Log Integration service on a machine, either on-premises or in the Cloud, running 64-bit Windows OS with .Net 4.5.1.

**Procedure**

1. If you have any previous versions of Microsoft Azure Log Integration service that is installed, you must uninstall the previous version. Uninstalling removes all registered sources. Complete the following steps to uninstall the Microsoft Azure Log Integration service.
   
a) Open a Windows command line interface as an administrator, and then type the following commands in the order that they are listed.
   
   • cd C:\Program Files\Microsoft Azure Log Integration\  
   • azlog removeazureid
   
b) From the Control Panel, click Add/Remove Program > Microsoft Azure Log Integration > Uninstall.


3. Open a Windows command line interface as an administrator.

4. To configure the Microsoft Azure Log Integration service, go to the following directory by running the following command: cd C:\Program Files\Microsoft Azure Log Integration\, and then complete the following steps.
   
a) Run the Azure PowerShell by typing the following command: azlog.exe powershell
   
b) From the PowerShell, type the following command: Add-AzLogEventDestination -Name <QRadar_Console_name> -SyslogServer <IP_address> -SyslogFormat LEEF
   
   If the syslog listerner for QRadar is not on the default port, you can specify the SyslogPort. The default is 514. For example,

   ```
   Add-AzLogEventDestination -Name <QRadar_Console_name> -SyslogServer <IP_address> -SyslogPort <port_number> -SyslogFormat LEEF
   ```

   c) Run the command: \azlog.exe createazureid, and then type your Azure login credentials in the prompt.
   
d) To assign reader access on the subscription, type the following command: .\azlog authorize <Subscription_ID>

**Configuring Microsoft Azure Event Hubs to communicate with QRadar**

The Microsoft Azure Event Hubs protocol collects Azure Activity logs, Diagnostic logs, and Syslog events from the Microsoft Azure Event Hubs cloud storage.

**Before you begin**

To collect events from Microsoft Azure Event Hubs, you need to create a Microsoft Azure Storage Account and an Event Hub entity under the Azure Event Hub Namespace. For every Namespace, port 5671 and port 5672 must be open. For every Storage Account, port 443 must be open. The Namespace host name is usually [Namespace_Name].servicebus.windows.net and the Storage Account host name is usually [Storage_Account_Name].blob.core.windows.net. The Event Hub must have at least one Shared Access Signature that is created with Listen Policy and at least one Consumer Group.

**Note:** The Microsoft Azure Event Hubs protocol can't connect by using a proxy server.

**Important:** Event Hub names must start with a letter or number and contain only letters, numbers, and the dash (-) character. Every dash (-) character must be immediately preceded and followed by a letter or number.
number. Do not use consecutive dashes. All letters must be lowercase. The name must be from 3 - 63 characters.

**Procedure**

1. Obtain a Microsoft Azure Storage Account Connection String.
   
   The Storage Account Connection String contains authentication for the Storage Account Name and the Storage Account Key that is used to access the data in the Azure Storage account.
   
   a) Log in to the [Azure Portal](https://portal.azure.com)
   
   b) From the dashboard, in the All resources section, select a Storage account.
   
   c) From the Storage account menu, select Access keys.
   
   d) Record the value for the Storage account name. Use this value for the Storage Account Name parameter value when you configure a log source in QRadar.
   
   e) From the key 1 or key 2 section, record the following values.
      
      • **Key** - Use this value for the Storage Account Key parameter value when you configure a log source in QRadar.
      
      • **Connection string** - Use this value for the Storage Account Connection String parameter value when you configure a log source in QRadar.
      
      **Example:**

      ```
      DefaultEndpointsProtocol=https;AccountName=[Storage Account Name];AccountKey=[Storage Account Key];EndpointSuffix=[EndpointSuffix]
      ```

   Most storage accounts use `core.windows.net` for the end point suffix, but this value can change depending on it's location. For example, a government related storage account might have a different endpoint suffix value.

   **Note:** You can use the Storage Account Name and Storage Account Key values, or you can use the Storage Account Connection String value to connect to the Storage Account.

2. Obtain a Microsoft Azure Event Hub Connection String.
   
   The Event Hub Connection String contains the Namespace Name, the path to the Event Hub within the namespace and the Shared Access Signature (SAS) authentication information.
   
   a) Log in to the [Azure Portal](https://portal.azure.com).
   
   b) From the dashboard, in the All resources section, select an Event Hubs Namespace. Record this value to use as the Namespace Name parameter value when you configure a log source in QRadar.
   
   c) In the Entities section, select Event Hubs. Record this value to use for the Event Hub Name parameter value when you configure a log source in QRadar.
   
   d) In the Event Hubs Instance section, select an Event Hub from the list.
   
   e) In the Settings section, select Shared access policies.
      
      1) Select a POLICY that contains a Listen CLAIMS. Record this value to use for the SAS Key Name parameter value when you configure a log source in QRadar.
      
      2) Record the values for the following parameters:
         
         • **Primary key or Secondary key** - Use the value for the SAS Key parameter value when you configure a log source in QRadar.
         
         • **Connection string-primary key or Connection string-secondary key** - Use this value for the Event Hub Connection String parameter value when you configure a log source in QRadar.
      
      **Example:**

      ```
      Endpoint=sb://[Namespace Name].servicebus.windows.net
      /;SharedAccessKeyName=[SAS Key Name];SharedAccessKey=[SAS Key];
      EntityPath=[Event Hub Name]
      ```
Note: You can use the Namespace Name, Event Hub Name, SAS Key Name and SAS Key values, or you can use the Event Hub Connection String value to connect to the Event Hub.

3. In the Entities section, select Consumer groups. Record the value to use for the Consumer Group parameter value when you configure a log source in QRadar.

Configuring QRadar to collect events from Microsoft Azure Event Hubs

To collect events from Microsoft Azure Event Hubs by using the Microsoft Azure Event Hubs protocol, you must manually configure a log source because IBM QRadar does not automatically detect these log sources.

Before you begin
RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:

- Protocol Common RPM
- Microsoft Azure Event Hubs Protocol RPM

Note: QRadar 7.2.8 Patch 7 and later is required for Microsoft Azure Event Hubs Protocol RPM.

Procedure

1. On the Admin tab, click Data Sources > Log Sources and then click Add.
2. From the Log Source Type list, select Microsoft Azure.
3. From the Protocol Configuration list, select Microsoft Azure Event Hubs.
4. Use the following table to help you configure these parameters:

   Note: Many parameters in the following table are obtained in “Configuring Microsoft Azure Event Hubs to communicate with QRadar” on page 760.

<table>
<thead>
<tr>
<th>Table 433. Configuring a log source in Microsoft Azure Event Hubs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Use as Gateway Log Source</td>
</tr>
<tr>
<td>Use Event Hub Connection String</td>
</tr>
<tr>
<td>Event Hub Connection String</td>
</tr>
<tr>
<td>Namespace Name</td>
</tr>
<tr>
<td>Event Hub Name</td>
</tr>
<tr>
<td>SAS Key Name</td>
</tr>
</tbody>
</table>
Table 433. Configuring a log source in Microsoft Azure Event Hubs (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Key</td>
<td>Available if the Use Event Hub Connection String check box is cleared. Enter the Primary key.</td>
</tr>
<tr>
<td>Consumer Group</td>
<td>The view that is used during the connection.</td>
</tr>
<tr>
<td>Use Storage Account Connection String</td>
<td>Clear this check box to manually enter the Storage Account Name and Storage Account Key.</td>
</tr>
<tr>
<td>Storage Account Connection String</td>
<td>Available if the Use Storage Account Connection String check box is enabled. Enter the CONNECTION STRING.</td>
</tr>
<tr>
<td>Storage Account Name</td>
<td>Available if the Use Storage Account Connection String check box is cleared.</td>
</tr>
<tr>
<td>Storage Account Key</td>
<td>Available if the Use Storage Account Connection String check box is cleared.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificates</td>
<td>If you select Yes from the list, QRadar automatically downloads the certificate and begins trusting the target server.</td>
</tr>
</tbody>
</table>
| EPS Throttle                                   | The maximum number of events that the Microsoft Azure Event Hubs Protocol forwards per second.  
                                           | 100 EPS is the minimum value.  
                                           | 10,000 EPS is the maximum value. |

5. Click Save.
6. On the Admin tab, click Deploy Changes.

What to do next
For more information about configuring QRadar to collect events from Microsoft Azure Event Hubs, watch the Configuring QRadar Log Source to collect events from QRadar video (https://www.youtube.com/watch?v=SylTkIpn2ko&amp;feature=youtu.be).

Microsoft Azure DSM specifications
The following table describes the specifications for the Microsoft Azure DSM.

Table 434. Microsoft Azure DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>DSM name</td>
<td>Microsoft Azure</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-MicrosoftAzure-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>Microsoft Azure Event Hubs</td>
</tr>
</tbody>
</table>
Table 434. Microsoft Azure DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event format</td>
<td>LEEF, JSON</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>
Microsoft Azure Portal (https://portal.azure.com) |

Sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following tables provide sample event messages for the Microsoft Azure DSM:

Table 435. Microsoft Azure sample syslog message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| Restarts virtual machines.        | Start Activity Attempted  | LEEF:1.0|Microsoft|Azure  
Resource Manager|1.0|  
MICROSOFT.CLASSICCOMPUTE  
/VIRTUALMACHINES/RESTART/  
ACTION|devTime=Jun 07 2016  
17:04:26 devTimeFormat  
=MMM dd yyyy HH:mm:ss  
cat=Compute src=  
<TIP_address>  
usrName  
=name@example.com  
sev=4 resource=  
testvm resourceGroup=Test  
Resource Group  
description  
=Restart a Virtual Machine  |

764 IBM QRadar : QRadar DSM Configuration Guide
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the access keys for the specified storage account</td>
<td>Read Activity Attempted</td>
<td></td>
</tr>
</tbody>
</table>

```json
"records": [{
  "time": "2017-09-14T11:47:36.1987564Z",
  "resourceId": "/SUBSCRIPTIONS//RESOURCEGROUPS//PROVIDERS/MICROSOFT_STORAGE/STORAGEACCOUNTS/",
  "operationName": "MICROSOFT.STORAGE/STORAGEACCOUNTS/LISTKEYS/ACTION",
  "category": "Action",
  "resultType": "Start",
  "resultSignature": "Started.",
  "durationMs": 0,
  "callerIpAddress": "<IP_address>",
  "correlationId": "",
  "identity": {
    "authorization": {
      "scope": "/subscriptions/resourceGroups/providers/Microsoft.Storage/storageAccounts/",
      "role": "Insights Management Service Role",
      "roleAssignmentScope": "/subscriptions/",
      "roleAssignmentId": "",
      "roleDefinitionId": "",
      "principalId": "",
      "principalType": "ServicePrincipal"
    },
    "claims": {
      "aud": "https://management.azure.com/",
      "iss": "https://sts.windows.net/",
      "iat": "1505389356",
      "nbf": "1505389356",
      "exp": "1505393256",
      "aio": "Y2VgYBBQEA5y0vTd4PVnSp9qVwAA==",
      "appid": "",
      "appidacr": "2",
      "e_exp": "262800",
      "http://schemas.microsoft.com/identity/claims/tenantid": "",
      "uti": "xxxxxx__xxxxxxxxxxxxxx",
      "ver": "1.0"
    },
    "level": "Information",
    "location": "global"
  },
  "level": "Information",
  "location": "global"
},
```

Chapter 97. Microsoft
### Microsoft DHCP Server

The Microsoft DHCP Server DSM for IBM QRadar accepts DHCP events by using the Microsoft DHCP Server protocol or WinCollect.

#### About this task

Before you can integrate your Microsoft DHCP Server with QRadar, you must enable audit logging.

To configure the Microsoft DHCP Server:

#### Procedure

1. Log in to the DHCP Server Administration Tool.
2. From the DHCP Administration Tool, right-click on the DHCP server and select **Properties**.
The Properties window is displayed.
3. Click the General tab.
   The General pane is displayed.
4. Click Enable DHCP Audit Logging.
   The audit log file is created at midnight and must contain a three-character day of the week abbreviation.

<table>
<thead>
<tr>
<th>Table 437. Microsoft DHCP log file examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Type</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>IPv4</td>
</tr>
<tr>
<td>IPv6</td>
</tr>
</tbody>
</table>

By default Microsoft DHCP is configured to write audit logs to the %WINDIR%\system32\dhcp\ directory.
5. Restart the DHCP service.
6. You can now configure the log source and protocol in QRadar.
   a) To configure QRadar to receive events from a Microsoft DHCP Server, you must select the Microsoft DHCP Server option from the Log Source Type list.
   b) To configure the protocol, you must select the Microsoft DHCP option from the Protocol Configuration list.

   Note: To integrate Microsoft DHCP Server versions 2000/2003 with QRadar by using WinCollect, see the IBM QRadar WinCollect User Guide.

Related concepts
“Microsoft DHCP protocol configuration options” on page 65
To receive events from Microsoft DHCP servers, configure a log source to use the Microsoft DHCP protocol.

Related tasks
“Adding a log source” on page 4
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 DNS Debug**

The IBM QRadar DSM for Microsoft DNS Debug collects events from a Microsoft Windows system.

Note:

The following table describes the specifications for the Microsoft DNS Debug DSM:

<table>
<thead>
<tr>
<th>Table 438. Microsoft DNS Debug DSM specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>DSM name</td>
</tr>
<tr>
<td>RPM file name</td>
</tr>
</tbody>
</table>
Table 438. Microsoft DNS Debug DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported versions</td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Protocol</td>
<td>WinCollect Microsoft DNS Debug</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All operational and configuration network events.</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td><a href="http://www.microsoft.com">http://www.microsoft.com</a></td>
</tr>
</tbody>
</table>

To integrate Microsoft DNS Debug with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following files in the order that they are listed on your QRadar Console:
   - .sfs file for WinCollect
   - DSMCommon RPM
   - Microsoft DNS Debug RPM


3. If QRadar does not automatically detect the log source, add a Microsoft DNS Debug log source on the QRadar Console.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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

Enabling DNS debugging on Windows Server

Enable DNS debugging on Windows Server to collect information that the DNS server sends and receives.

Before you begin
The DNS role must be installed on the Windows Server.

Important: DNS debug logging can affect system performance and disk space because it provides detailed data about information that the DNS server sends and receives. Enable DNS debug logging only when you require this information.

Procedure

1. Open the DNS Manager with the following command:

dnsmgmt.msc
2. Right-click the DNS server and click Properties.
3. Click the Debug Logging tab.
4. Select Log packets for debugging.
5. Enter the File path and name, and Maximum size.
   Important: The File path and name, need to align with the Root Directory and File Pattern you provided when the Microsoft DNS debug log source was created in QRadar.
6. Click Apply and OK.

**Microsoft Endpoint Protection**

The Microsoft Endpoint Protection DSM for IBM QRadar collects malware detection events. QRadar collects malware detection events by using the JDBC protocol. Adding malware detection events to QRadar gives the capability to monitor and detect malware infected computers in your deployment.

Malware detection events include the following event types:
- Site name and the source from which the malware was detected.
- Threat name, threat ID, and severity.
- User ID associated with the threat.
- Event type, time stamp, and the cleaning action that is taken on the malware.

**Configuration overview**

The Microsoft Endpoint Protection DSM uses JDBC to poll an SQL database for malware detection event data. This DSM does not automatically discover. To integrate Microsoft Endpoint Protection with QRadar, take the following steps:

1. If your database is not configured with Predefined Query, create an SQL database view for QRadar with the malware detection event data.
2. Configure a JDBC log source to poll for events from the Microsoft Endpoint Protection database.
3. Ensure that no firewall rules are blocking communication between QRadar and the database that is associated with Microsoft Endpoint Protection.

**Configuring an Endpoint Protection log source for predefined database queries**

Administrators who do not have permission to create a database view because of policy restrictions can collect Microsoft Endpoint Protection events with a log source that uses predefined queries.

**About this task**

Predefined queries are customized statements that can join data from separate tables when the database is polled by the JDBC protocol. To successfully poll for audit data from the Microsoft Endpoint Protection database, create a new user or provide the log source with existing user credentials. For more information about creating a user account, see the Microsoft website (https://www.microsoft.com).

**Procedure**

1. Click the Admin tab.
2. Click the Log Sources icon.
3. Click Add.
4. Configure the parameters. The following table describes the parameters that require specific values to collect events from SAP Enterprise Threat Protection by using the JDBC protocol:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the logsource.</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>Microsoft Endpoint Protection</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol.</td>
</tr>
<tr>
<td></td>
<td>If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>MSDE</td>
</tr>
<tr>
<td>Database Name</td>
<td>The name of the database to which you want to connect.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>Type the IP address or host name of the Microsoft Endpoint Protection SQL Server.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number that is used by the database server. The default port for MSDE is 1433.</td>
</tr>
<tr>
<td></td>
<td>The JDBC configuration port must match the listener port of the Microsoft Endpoint Protection database. The Microsoft Endpoint Protection database must have incoming TCP connections that are enabled to communicate with QRadar.</td>
</tr>
<tr>
<td></td>
<td>If you define a Database Instance when MSDE is used as the database type, you must leave the Port field blank in your configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name the log source can use to access the Microsoft Endpoint Protection database.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password the log source can use to access the Microsoft Endpoint Protection database. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password that is used to access the database. The confirmation password must be identical to the password entered in the Password field.</td>
</tr>
<tr>
<td>Authentication Domain</td>
<td>If you did not select Use Microsoft JDBC, Authentication Domain is displayed.</td>
</tr>
<tr>
<td></td>
<td>If you select MSDE as the Database Type and the database is configured for Windows Authentication, you must populate the Authentication Domain field. Otherwise, leave this field blank.</td>
</tr>
</tbody>
</table>
Table 439. Microsoft Endpoint Protection JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Instance</td>
<td>If you have multiple SQL server instances on your database server, type the database instance. If you use a non-standard port in your database configuration, or block access to port 1434 for SQL database resolution, you must leave the <strong>Database Instance</strong> parameter blank in your configuration.</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>From the list, select <strong>Microsoft Endpoint Protection</strong>.</td>
</tr>
<tr>
<td>Table Name</td>
<td>The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td>Select List</td>
<td>The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the <strong>Compare Field</strong>.</td>
</tr>
<tr>
<td>Compare Field</td>
<td>A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. Enables the protocol to identify events that were previously polled by the protocol to ensure that duplicate events are not created.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Select the <strong>Use Prepared Statements</strong> check box. Prepared statements allow the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>Type the start date and time for database polling. The <strong>Start Date and Time</strong> 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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Type the polling interval, which is the amount of time between queries to the view you created. 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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000.</td>
</tr>
<tr>
<td>Use Named Pipe</td>
<td>If you did not select <strong>Use Microsoft JDBC, Use Named Pipe Communication</strong> is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
</tbody>
</table>

Chapter 97. Microsoft 771
Table 439. Microsoft Endpoint Protection JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Cluster Name</td>
<td>If you selected the Use Named Pipe Communication, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select Use Microsoft JDBC, Use NTLMv2 is displayed. Select the Use NTLMv2 check box. This option forces MSDE connections to use the NTLMv2 protocol when they communicate with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable Use Microsoft JDBC.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If your connection supports SSL communication, select Use SSL. This option requires extra configuration on your Endpoint Protection database and also requires administrators to configure certificates on both appliances.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected Use Microsoft JDBC and Use SSL, the Microsoft SQL Server Hostname parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC parameters, see [c_logsource_JDBCprotocol.dita](#).

**Note:** Selecting a parameter value greater than 5 for the Credibility parameter weights your Microsoft Endpoint Protection log source with a higher importance that is compared to other log sources in QRadar.

5. Click Save.
6. On the Admin tab, click Deploy Changes.

---

**Microsoft Exchange Server**

The IBM 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 440. Microsoft Exchange Server

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>DSM name</td>
<td>Exchange Server</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-MicrosoftExchange-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Specification</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Outlook Web Access events (OWA)&lt;br&gt;Simple Mail Transfer Protocol events (SMTP)&lt;br&gt;Message Tracking Protocol events (MSGTRK)</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Included identity?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Microsoft website (<a href="http://www.microsoft.com">http://www.microsoft.com</a>)</td>
</tr>
</tbody>
</table>

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 DSM” on page 4
“Adding a log source” on page 4
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 135 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 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, or IIS 8.5 for Microsoft Server 2012 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 2003, 2007, and 2010
To prepare your Microsoft Exchange Server 2003, 2007 and 2010 to communicate with IBM 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**.

**Enabling SMTP logs on your Microsoft Exchange Server 2013, and 2016**
To prepare your Microsoft Exchange Server 2013 and 2016 to communicate with IBM QRadar, enable SMTP event logs.

**Procedure**
1. Start the Exchange Administration Center.
2. To configure your receive connector, select **Mail Flow > Receive Connectors**.
3. Select your receive connector and click **Edit**.
4. Click the **General** tab.
5. From the **Protocol logging level** list, select **Verbose**.
6. Click **Save**.
7. To configure your send connector, select **Mail Flow > Send Connectors**
8. Select your send connector and click **Edit**.
9. Click the **General** tab.
10. From the **Protocol logging level** list, select **Verbose**.
11. Click **Save**.

**Configuring MSGTRK logs for Microsoft Exchange 2003, 2007, and 2010**
Message Tracking logs created by the Microsoft Exchange Server detail the message activity that takes place on your Microsoft Exchange Server, including the message path information.

**About this task**
MSGTRK logs are enabled by default on Microsoft Exchange 2007 or Exchange 2010 installations. The following configuration steps are optional.

To enable MSGTRK event logs:

**Procedure**
1. Start the Exchange Management Console.
2. Configure your receive connector based on the server type:
   • For edge transport servers - In the **console tree**, select **Edge Transport** and click **Properties**.
   • For hub transport servers - In the console tree, select **Server Configuration > Hub Transport**, and then select the server and click **Properties**.
3. Click the **Log Settings** tab.
4. Select the **Enable message tracking** check box.
5. Click **Apply**.
6. Click **OK**.

    MSGTRK events are now enabled on your Exchange Server.
Configuring MSGTRK logs for Exchange 2013 and 2016
Message Tracking logs created by the Microsoft Exchange Server detail the message activity that takes place on your Exchange Server, including the message path information.

Procedure
1. Start the Exchange Administration Center.
2. Click Servers > Servers.
3. Select the mailbox server that you want to configure, and then click Edit.
4. Click Transport Logs.
5. In the Message tracking log section, configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable message tracking log</td>
<td>Enable or disable message tracking on the server.</td>
</tr>
<tr>
<td>Message tracking log path</td>
<td>The value that you specify must be on the local Exchange server. If the folder does not exist, it is created when you click Save.</td>
</tr>
</tbody>
</table>

6. Click Save.

Configuring a log source for Microsoft Exchange
IBM 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 log source parameters.

Learn more about Microsoft Exchange log source parameters:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name to identify the Windows Exchange event source in the QRadar user interface.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IP address of the Microsoft Exchange server.</td>
</tr>
<tr>
<td>SMTP Log Folder Path</td>
<td>The directory path to access the SMTP log files. Use one of the following directory paths:</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2003, use c$$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/.</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2007, use c$$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/.</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2010, use c$$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/ProtocolLog/.</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2013, use c$$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/ProtocolLog/.</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2016, use c$$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/ProtocolLog/.</td>
</tr>
<tr>
<td>OWA Log Folder Path</td>
<td>The directory path to access the OWA log files. Use one of the following directory paths:</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2003, use c$$/WINDOWS/system32/LogFiles/W3SVC1/.</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2007, use c$$/WINDOWS/system32/LogFiles/W3SVC1/.</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2010, use c$$/inetpub/logs/LogFiles/W3SVC1/.</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2013, use c$$/inetpub/logs/LogFiles/W3SVC1/.</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2016, use c$$/inetpub/logs/LogFiles/W3SVC1/.</td>
</tr>
<tr>
<td>MSGTRK Log Folder Path</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft Exchange 2007, use c$$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/MessageTracking/.</td>
</tr>
</tbody>
</table>
Parameter | Description
--- | ---
• For Microsoft Exchange 2010, use c$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/MessageTracking/.
• For Microsoft Exchange 2013, use c$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/MessageTracking/.
• For Microsoft Exchange 2016, use c$/Program Files/Microsoft/Exchange Server/V15/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**.

**Microsoft Hyper-V**

The IBM QRadar DSM for Microsoft Hyper-V can collect event logs from your Microsoft Hyper-V servers. The following table describes the specifications for the Microsoft Hyper-V Server DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>DSM</td>
<td>Microsoft Hyper-V</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-MicrosoftHyperV-QRadar_version-build_number.rpm</td>
</tr>
</tbody>
</table>
| Supported versions | Windows Server 2016  
Windows Server 2012 (most recent)  
Windows Server 2012 Core  
Windows Server 2008 (most recent)  
Windows Server 2008 Core  
Windows 10 (most recent)  
Windows 8 (most recent)  
Windows 7 (most recent)  
Windows Vista (most recent) |
| Protocol | WinCollect |
### Microsoft Hyper-V DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRadar recorded events</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

### Microsoft Hyper-V DSM integration process

You can integrate Microsoft Hyper-V DSM with IBM QRadar.

Use the following procedures:

1. Download and install the most recent WinCollect RPM on your QRadar Console.
2. Install a WinCollect agent on the Hyper-V system or on another system that has a route to the Hyper-V system. You can also use an existing WinCollect agent. For more information, see the IBM QRadar WinCollect User Guide.
3. If automatic updates are not enabled, download and install the DSM RPM for Microsoft Hyper-V on your QRadar Console. RPMs need to be installed only one time.
4. For each Microsoft Hyper-V server that you want to integrate, create a log source on the QRadar Console.

### Related tasks

“Configuring a Microsoft Hyper-V log source in QRadar” on page 779

### Configuring a Microsoft Hyper-V log source in QRadar

To collect Microsoft Hyper-V events, configure a log source in IBM QRadar.

#### About this task

Ensure that you have the current credentials for the Microsoft Hyper-V server and the WinCollect agent can access it.

#### 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 Microsoft **Hyper-V**.
7. From the **Protocol Configuration** list, select **WinCollect**.
8. From the **Application or Service Log Type** list, select Microsoft **Hyper-V**.
9. From the **WinCollect Agent** list, select the WinCollect agent that accesses the Microsoft Hyper-V server.
10. Configure the remaining parameters.
11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

**Microsoft IAS Server**

The Microsoft IAS Server DSM for IBM QRadar accepts RADIUS events by using syslog.

**About this task**

You can integrate Internet Authentication Service (IAS) or Network Policy Server (NPS) logs with QRadar by using WinCollect. For more information, see the *IBM QRadar WinCollect User Guide*.

You can now configure the log source in QRadar.

To configure QRadar to receive events from a Microsoft Windows IAS Server.

**Procedure**

From the **Log Source Type** list, select the Microsoft **IAS Server** option.

For more information about your server, see your vendor documentation.

**Related tasks**

“Adding a log source” on page 4

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 IIS Server**

The Microsoft Internet Information Services (IIS) Server DSM for IBM QRadar accepts FTP, HTTP, NNTP, and SMTP events using syslog.

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

- Configure QRadar to connect to your Microsoft IIS Server by using the IIS Protocol which collects HTTP events from Microsoft IIS servers. For more information, see “Configuring Microsoft IIS by using the IIS Protocol” on page 780.


<table>
<thead>
<tr>
<th>Method of Import</th>
<th>Supported Log Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIS Protocol</td>
<td>HTTP</td>
</tr>
<tr>
<td>WinCollect</td>
<td>SMTP, NNTP, FTP, HTTP</td>
</tr>
</tbody>
</table>

**Configuring Microsoft IIS by using the IIS Protocol**

You can configure Microsoft IIS Protocol to communicate with QRadar by using the IIS Protocol.

**Before you begin**

Before you configure IBM QRadar with the Microsoft IIS protocol, you must configure your Microsoft IIS Server to generate the correct log format.
About this task
The Microsoft IIS Protocol supports only the W3C Extended log file format. The Microsoft authentication protocol NTLMv2 Session is not supported by the Microsoft IIS protocol.

Procedure
1. Log in to your Microsoft Information Services (IIS) Manager.
2. Expand **IIS Manager > Local Computer > Sites**.
3. Select **Web Site**.
4. Double-click the **Logging** icon.
5. Select **W3C** as the log file format from the **Log File** window.
6. Click the **Select Fields** push button.
7. From the list of properties, select check boxes for the following W3C properties:

<table>
<thead>
<tr>
<th>Table 443. Required Properties for IIS event logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIS 6.0 Required Properties</td>
</tr>
<tr>
<td>Date (date)</td>
</tr>
<tr>
<td>Time (time)</td>
</tr>
<tr>
<td>Client IP Address (c-ip)</td>
</tr>
<tr>
<td>User Name (cs-username)</td>
</tr>
<tr>
<td>Server IP Address (s-ip)</td>
</tr>
<tr>
<td>Server Port (s-port)</td>
</tr>
<tr>
<td>URI Stem (cs-uri-stem)</td>
</tr>
<tr>
<td>URI Query (cs-uri-query)</td>
</tr>
<tr>
<td>Protocol Version (cs-version)</td>
</tr>
<tr>
<td>User Agent (cs(User-Agent))</td>
</tr>
</tbody>
</table>

8. Click **OK**.
9. Click **Apply** in the top right corner.

What to do next
You are now ready to configure the log source in QRadar.
Configuring the Microsoft IIS Protocol in IBM QRadar

You can configure the log source for Microsoft IIS in QRadar.

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   - The Data Sources pane is displayed.
4. Click the Log Sources icon.
   - The Log Sources window is displayed.
5. Click Add.
   - The Add a log source window is displayed.
6. From the Log Source Type list, select Microsoft IIS Server.
7. From the Protocol Configuration list, select Microsoft IIS.
8. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Type the IP address of the Microsoft IIS server.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name that is required to access the Microsoft IIS server.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password that is required to access the Microsoft IIS server.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password that is required to access the Microsoft IIS server.</td>
</tr>
<tr>
<td>Domain</td>
<td>Type the domain that is required to access the Microsoft IIS server.</td>
</tr>
<tr>
<td>Folder Path</td>
<td>Type the directory path to access the IIS log files. The default is /WINDOWS/system32/LogFiles/W3SVC1/ Parameters that support file paths give you the option to define a drive letter with the path information. For example, you can use c$/LogFiles/ for an administrative share or LogFiles/ for a public share folder path, but not c:/LogFiles. If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the proper access that is needed to read the log files. Local or domain administrators have sufficient privileges to access log files on administrative shares.</td>
</tr>
<tr>
<td>File Pattern</td>
<td>Type the regular expression (regex) that is needed to filter the file names. All matching files are included in the processing. The default is (?::u_)? ex.*.(?:log</td>
</tr>
</tbody>
</table>
Table 444. Microsoft IIS protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recursive</td>
<td>Select this check box if you want the file pattern to search sub folders. By default, the check box is selected.</td>
</tr>
<tr>
<td>Polling Interval (s)</td>
<td>Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds.</td>
</tr>
</tbody>
</table>

9. Click **Save**.
10. The Microsoft IIS protocol configuration is complete.

**Configuring a Microsoft IIS log source**

IBM QRadar automatically discovers and creates a log source for syslog events from Microsoft IIS forwarded from a stand-alone WinCollect agent. These configuration steps are optional.

**About this task**

To manually create a Microsoft IIS log source in QRadar:

**Procedure**
1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
   The **Log Sources** window is displayed.
5. Click **Add**.
   The Add a log source window is displayed.
6. From the **Log Source Type** list, select Microsoft IIS Server.
7. From the **Protocol Configuration** list, select **Syslog**.
8. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source.</td>
</tr>
</tbody>
</table>

9. Click **Save**.
10. On the **Admin** tab, click **Deploy Changes**.
    The configuration is complete.

**Microsoft ISA**

The Microsoft Internet and Acceleration (ISA) DSM for IBM QRadar accepts events by using syslog.

You can integrate Microsoft ISA Server with QRadar by using WinCollect. For more information, see the *IBM QRadar WinCollect User Guide*.

**Note**: The Microsoft ISA DSM also supports events from Microsoft Threat Management Gateway by using WinCollect.
The IBM QRadar DSM for Microsoft Office 365 collects events from Microsoft Office 365 online services.

The following table describes the specifications for the Microsoft Office 365 DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>DSM name</td>
<td>Microsoft Office 365</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-MicrosoftOffice365-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Office 365 REST API</td>
</tr>
<tr>
<td>Event format</td>
<td>JSON</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Exchange Audit, SharePoint Audit, Azure Active Directory Audit, Service Communications</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Microsoft website (<a href="https://www.microsoft.com">https://www.microsoft.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Microsoft Office 365 with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - Office 365 REST API Protocol RPM
   - Microsoft Office 365 DSM RPM

2. Configure a Microsoft Office 365 account in the Microsoft Azure portal.

3. Add a Microsoft Office 365 log source on the QRadar Console. For more information about adding a log source, see the “Adding a log source” on page 4 topic. The following table describes the log source parameters that require specific values for Microsoft Office 365 event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Microsoft Office 365</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Office 365 REST API</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>A unique identifier for the log source.</td>
</tr>
<tr>
<td></td>
<td>The Log Source Identifier can be any valid value and does not need to reference a specific server.</td>
</tr>
<tr>
<td></td>
<td>The Log Source Identifier can be the same value as the Log Source Name. If you configured multiple Microsoft Office 365 log sources, you might want to identify the first log source as MSOffice365-1, the second log source as MSOffice365-2, and the third log source as MSOffice365-3.</td>
</tr>
<tr>
<td>Client ID</td>
<td>In your application configuration of Azure Active Directory, this parameter is under <strong>Client ID</strong>.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>In your application configuration of Azure Active Directory, this parameter is under <strong>Keys</strong>.</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>Used for Azure AD authentication.</td>
</tr>
<tr>
<td>Event Filter</td>
<td>The type of audit events to retrieve from Microsoft Office.</td>
</tr>
<tr>
<td></td>
<td>• Azure Active Directory</td>
</tr>
<tr>
<td></td>
<td>• Exchange</td>
</tr>
<tr>
<td></td>
<td>• SharePoint</td>
</tr>
<tr>
<td></td>
<td>• General</td>
</tr>
<tr>
<td></td>
<td>• DLP</td>
</tr>
<tr>
<td></td>
<td>• Service Communications</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>For QRadar to access the Office 365 Management APIs, all traffic for the log source travels through configured proxies.</td>
</tr>
<tr>
<td></td>
<td>Configure the <strong>Proxy Server</strong>, <strong>Proxy Port</strong>, <strong>Proxy Username</strong>, and <strong>Proxy Password</strong> fields.</td>
</tr>
<tr>
<td></td>
<td>If the proxy does not require authentication, keep the <strong>Proxy Username</strong> and <strong>Proxy Password</strong> fields empty.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum number of events per second. The default is 5000.</td>
</tr>
</tbody>
</table>

**Related tasks**

“Configuring a Microsoft Office 365 account in Microsoft Azure Active Directory” on page 786
Before you can add a log source in QRadar, you must run the Azure Active Directory PowerShell cmdlet and then configure Azure Active Directory for Microsoft Office 365.

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 a Microsoft Office 365 account in Microsoft Azure Active Directory**

Before you can add a log source in QRadar, you must run the Azure Active Directory PowerShell cmdlet and then configure Azure Active Directory for Microsoft Office 365.

**Procedure**

1. Run the Azure Active Directory PowerShell cmdlet. For more information, see How to install and configure Azure PowerShell (https://azure.microsoft.com/en-us/documentation/articles/powershell-install-configure/).

2. Identify the Tenant ID of the tenant that is subscribed to Microsoft Office 365 by typing the following commands:

   ```powershell
   import-module MSOnline
   $userCredential = Get-Credential
   Connect-MsolService -Credential $userCredential
   Get-MsolAccountSku | % {$_.AccountObjectID}
   ```

   Use the **Tenant ID** value for the **Tenant ID** value when you configure a log source in QRadar.

3. To use Azure Active Directory to register an application, such as Microsoft Excel or Microsoft SharePoint, log in to the Azure Management Portal (https://portal.azure.com) with the credentials of the tenant that is subscribed to Microsoft Office 365.

   a. From the navigation menu, select **Azure Active Directory**.

   b. From the **Overview** pane, select **App registrations**, and then click **New registration**.

   c. In the **Supported account types** section, select the type of account to use the application or to access the API.

   d. In the **Redirect URI (optional)** section, select **Web**, and type `http://localhost` in the **Web** field.

   e. Click **Register**, and then copy and store the **Application (client) ID** value. Use this value for the **Client ID** value when you configure a log source in QRadar.

4. Generate a client secret for the application.

   a. From the **Manage** pane, select **Certificates & secrets > New client secret**.

   b. Select an expiry period, and then click **Add**.

   c. Copy and store your client secret key value because it can't be retrieved later. Use this value for the **Client Secret** value when you configure a log source in QRadar.

5. Specify the permissions that the Microsoft Azure application must use to access Microsoft Office 365 Management APIs.

   a. From the **Manage** pane, select **API permissions**.

   b. Click **Add a permission > Delegated permissions**, and then select the following options:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Feed</td>
<td>ActivityFeed.Read</td>
</tr>
<tr>
<td></td>
<td>ActivityFeed.ReadDlp</td>
</tr>
<tr>
<td>Activity Reports</td>
<td>ActivityReports.Read</td>
</tr>
<tr>
<td>ServiceHealth</td>
<td>ServiceHealth.Read</td>
</tr>
</tbody>
</table>
c. Click Application permissions, and then select the following options:
Table 449. Application permissions
Permission

Values

Activity Feed

ActivityFeed.Read
ActivityFeed.ReadDlp

ActivityReports

ActivityReports.Read

ServiceHealth

ServiceHealth.Read

d. Click Add permssions.
e. In the API permissions window, go to the Grant consent section, click Grant admin consent >
Yes.
What to do next
Adding a log source
Related concepts
“Microsoft Office 365” on page 784
The IBM QRadar DSM for Microsoft Office 365 collects events from Microsoft Office 365 online services.

Sample event messages
Use these sample event messages as a way of verifying a successful integration with QRadar.
The following table provides sample event messages when using the Office 365 REST API protocol for the
Microsoft Office 365 DSM:
Table 450. Microsoft Office 365 sample message supported by the Microsoft Office 365 service
Event name

Low level category

Update user-fail

Update Activity Failed

Sample log message
{"CreationTime":"2016-05-05T08:53:
46","Id":"xxx-xxxx-xxxx-xxxxxxxxxxxxxxxx","Operation":
"Update user.","OrganizationId":
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx
xxxxx","RecordType":8,"Result
Status":"fail","UserKey":"Not
Available","UserType":6,"Workload"
:"AzureActiveDirectory","ObjectId"
:"xxxxxxxxxxxxxxxx","UserId":"xxxxxx-xxxx-xxxx-xxxxxxxxxxxx",
"AzureActiveDirectoryEventType"
:1,"ExtendedProperties":[{"Name":
"MethodExecutionResult.","Value":
"Microsoft.Online.Workflows.
ValidationException"}],"Actor":
[{"ID":"x-xxxx-xxxx-xxxx-xxxxxx
xxxxxx","Type":4},{"ID":"xxxxxx_
xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx
xxxx","Type":2}],"ActorContextId"
:"xxxxxxxx-xxxx-xxxx-xxxx-xxxxx
xxxxxxx","InterSystemsId":
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx
xxxxx","IntraSystemId":"xxxxxxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx",
"Target":[{"ID":"x-xxxx-xxxxxxxx-xxxxxxxxxxxx","Type":2},
{"ID":"username@example.com","Type"
:1},{"ID":"1706BDBF","Type":3}]
,"TargetContextId":"xxxxxxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx"}

Chapter 97. Microsoft 787


Microsoft Operations Manager

The Microsoft Operations Manager DSM for IBM QRadar accepts Microsoft Operations Manager (MOM) events by polling the OnePoint database that allows QRadar to record the relevant events.

About this task

Before you configure QRadar to integrate with the Microsoft Operations Manager, you must ensure that a database user account is configured with appropriate permissions to access the MOM OnePoint SQL Server database. Access to the OnePoint database SDK views is managed through the MOM SDK View User database role. For more information, see your Microsoft Operations Manager documentation.

**Note:** Make sure that the firewall rules are not blocking the communication between QRadar and the SQL Server database that is associated with MOM. For MOM installations that use a separate, dedicated computer for the SQL Server database, the SDKEventView view is queried on the database system, not the system that runs MOM.

To configure QRadar to receive MOM events:

1. Click the Admin tab.
2. On the navigation menu, click Data Sources.
3. Click the Log Sources icon, and then click Add.
4. Configure the following values:

| Table 451. Microsoft Operations Manager JDBC parameters |
|-------------------------|-----------------|
| **Parameter**            | **Description**  |
| Log Source Name          | Type a unique name for the log source. |
| Log Source Description   | Type a description for the log source. (Optional) |
| Log Source Type          | Microsoft Operations Manager |
| Protocol Configuration   | JDBC |
### Table 451. Microsoft Operations Manager JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td><strong>Database Type</strong></td>
<td>From the list, select MSDE.</td>
</tr>
<tr>
<td><strong>Database Name</strong></td>
<td>Type OnePoint as the name of the Microsoft Operations Manager database.</td>
</tr>
<tr>
<td><strong>IP or Hostname</strong></td>
<td>Type the IP address or host name of the Microsoft Operations Manager SQL Server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>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 Operations Manager database. The Microsoft Operations Manager database must have incoming TCP connections that are enabled to communicate with QRadar. If you define a Database Instance when MSDE is used as the database type, you must leave the Port parameter blank in your configuration.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Type the user name that is required to access the database.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Type the password that is required to access the database. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the Password parameter.</td>
</tr>
<tr>
<td><strong>Authentication Domain</strong></td>
<td>If you did not select Use Microsoft JDBC, Authentication Domain is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td><strong>Database Instance</strong></td>
<td>If you have multiple SQL server instances on your database server, type the database instance. If you use a non-standard port in your database configuration, or block access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your log source configuration.</td>
</tr>
<tr>
<td><strong>Table Name</strong></td>
<td>Type SDKEventView as the name of the table or view that includes the event records.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Select List</td>
<td>The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the Compare Field.</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Type TimeStored as the compare field. The compare field is used to identify new events that are added between queries to the table.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Select this check box to use prepared statements. Prepared statements allow the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, most JDBC protocol configurations use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>Type the start date and time for database polling in the following format: 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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td>Use Named Pipe Communication</td>
<td>If you did not select Use Microsoft JDBC, Use Named Pipe Communication is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>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 to ensure Named Pipe communication functions properly.</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select Use Microsoft JDBC, Use NTLMv2 is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
</tbody>
</table>
Table 451. Microsoft Operations Manager JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable Use Microsoft JDBC.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option if your connection supports SSL.</td>
</tr>
<tr>
<td>Credibility</td>
<td>Selecting a value greater than 5 for the Credibility parameter weights your Microsoft Operations Manager log source with a higher importance compared to other log sources in QRadar.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected Use Microsoft JDBC and Use SSL, the Microsoft SQL Server Hostname parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC parameters, see [c_logsource_JDBCprotocol.dita](#).

5. Click **Save**.
6. On the **Admin** tab, click **Deploy Changes**.

**Related tasks**
- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 SharePoint**

The Microsoft SharePoint DSM for IBM QRadar collects audit events from the SharePoint database by using JDBC to poll an SQL database for audit events.

Audit events can track changes that are made to sites, files, and content that is managed by Microsoft SharePoint.

Microsoft SharePoint audit events include the following elements:
- Site name and the source from which the event originated
- Item ID, item name, and event location
- User ID associated with the event
- Event type, time stamp, and event action

Two log source configurations can be used to collect Microsoft SharePoint database events.

1. Create a database view in your SharePoint database to poll for events with the JDBC protocol. See “Configuring a database view to collect audit events” on page 792.
2. Create a JDBC log source and use predefined database queries to collect SharePoint events. This option does not require an administrator to create database view. See “Configuring a SharePoint log source for predefined database queries” on page 797.

**Note:** The collection of Microsoft SharePoint events now uses a predefined query, instead of requiring an administrator to create a database view. If you are an administrator, you might want to update existing Microsoft Sharepoint log sources so that they use the Microsoft Sharepoint predefined query.
Configuring a database view to collect audit events

Before you can integrate Microsoft SharePoint events with IBM QRadar, you must complete three tasks.

About this task

Use the following procedure:

Procedure

1. Configure the audit events you want to collect for Microsoft SharePoint.
2. Create an SQL database view for QRadar in Microsoft SharePoint.
3. Configure a log source to collect audit events from Microsoft SharePoint.

   Note: Ensure that firewall rules are not blocking the communication between QRadar and the database associated with Microsoft SharePoint.

Configuring Microsoft SharePoint audit events

The audit settings for Microsoft SharePoint give you the option to define what events are tracked for each site that is managed by Microsoft SharePoint.

Procedure

1. Log in to your Microsoft SharePoint site.
2. From the Site Actions list, select Site Settings.
3. From the Site Collection Administration list, click Site collection audit settings.
4. From the Documents and Items section, select a check box for each document and item audit event you want to audit.
5. From the Lists, Libraries, and Sites section, select a check box for each content audit event you want to enable.
6. Click OK.

    You are now ready to create a database view for IBM QRadar to poll Microsoft SharePoint events.

Creating a database view for Microsoft SharePoint

Microsoft SharePoint uses SQL Server Management Studio (SSMS) to manage the SharePoint SQL databases. To collect audit event data, you must create a database view on your Microsoft SharePoint server that is accessible to IBM QRadar.

Before you begin

Do not use a period (.) in the name of your view, or in any of the table names. If you use a period in your view or table name, JDBC cannot access the data within the view and access is denied. Anything after a (.) is treated as a child object.

Procedure

1. Log in to the system that hosts your Microsoft SharePoint SQL database.
2. From the Start menu, select Run.
3. Type the following command:
   
   sssm

4. Click OK.

    The Microsoft SQL Server 2008 displays the Connect to Server window.
5. Log in to your Microsoft SharePoint database.
6. Click Connect.
7. From the **Object Explorer** for your SharePoint database, click **Databases > WSS_Logging > Views**.

8. From the navigation menu, click **New Query**.

9. In the **Query** pane, type the following Transact-SQL statement to create the AuditEvent database view:

```sql
CREATE VIEW dbo.AuditEvent AS
SELECT a.siteID,
a.ItemId,
a.ItemType,
u.tp_Title AS "User",
a.MachineName,
a.MachineIp,
a.DocLocation,
a.LocationType,
a.Occurred AS "EventTime",
a.Event AS "EventID",
a.EventName,
a.EventSource,
a.SourceName,
a.EventData,
FROM WSS_Content.dbo.AuditData a,
WSS_Content.dbo.UserInfo u
WHERE a.UserId = u.tp_ID
AND a.SiteId = u.tp_SiteID;
```

10. From the **Query** pane, right-click and select **Execute**.

   If the view is created, the following message is displayed in the results pane:
   
   Command(s) completed successfully.

   The dbo.AuditEvent view is created. You are now ready to configure the log source in QRadar to poll the view for audit events.

### Creating read-only permissions for Microsoft SharePoint database users

Restrict user access on the SharePoint database by granting read-only permissions on objects.

**Procedure**

1. From the **Object Explorer** in your SharePoint database, click **Security**. Expand the **Security** folder tree.

2. Right-click **Logins** and select **New Login**.

3. For Windows authentication, complete the following steps:
   a) On the **General** page, click **Search**.
   b) Click **Locations**. From the **Locations** page, select a location that the user belongs to and click **OK**.
   c) Enter the object name in the text-box, and click **Check Names** to validate the user.

   **Note:** Set the Default database to **WSS_Logging**.

   d) On the **Server Roles** page, select **public**.

   e) On the **User Mapping** page, select the **WSS_Content** and **WSS_Logging**. In the Default Schema column, click ... > **Browse...** and select db_datadreader as the default schema.

   f) On the **Status** page, select **Grant** permission to connect to the database engine and select Enabled login.

4. From the **Object Explorer** in your SharePoint database, click **Databases > WSS_Logging > Security > Users**.

   a) Double-click the Windows user that was created in step 3.

   b) On the **Securables** page, click **Search**.

   c) On the **Add Objects** page, select **Specific objects...** and click **OK**.

   d) Click **Object Types...** and select **Views**.

   e) For object names, click **Browse** and select the database view that you created. For example, [dbo]. [AuditEvent].

   f) For the permissions of the database view you select, grant **Select**.

   g) Click **OK**.
5. From the **Object Explorer** in your SharePoint database, click **Databases > WSS_Content > Security > Users**.
   a) Double-click the Windows user that was created in step 3.
   b) On the **Securables** page, click **Search**.
   c) On the **Add Objects** page, select **Specific objects...** and click **OK**.
   d) Click **Object Types...** and select **Tables**.
   e) For object names, click **Browse**. Select `[dbo].[AuditData]` and `[dbo].[UserInfo]`.
   f) For the permissions of the **AuditData** table, grant **Select**.
   g) For the permissions of the **UserInfo** table, grant **Select**.
   h) Click **OK**.

### Configuring a SharePoint log source in QRadar

IBM QRadar requires a user account with the proper credentials to access the view you created in the Microsoft SharePoint database.

**About this task**

To successfully poll for audit data from the Microsoft SharePoint database, you must create a new user or provide the log source with existing user credentials to read from the AuditEvent view. For more information on creating a user account, see your vendor documentation.

To configure QRadar to receive SharePoint events:

**Procedure**

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Configure the following Microsoft SharePoint parameter values:

   **Table 452. Microsoft SharePoint JDBC parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>Microsoft SharePoint</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be</td>
</tr>
<tr>
<td></td>
<td>unique among all log sources of the log source type that is configured to</td>
</tr>
<tr>
<td></td>
<td>use the JDBC protocol.</td>
</tr>
<tr>
<td></td>
<td>If the log source collects events from a single appliance that has a static</td>
</tr>
<tr>
<td></td>
<td>IP address or host name, use the IP address or host name of the appliance</td>
</tr>
<tr>
<td></td>
<td>as all or part of the <strong>Log Source Identifier</strong> value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the <strong>Log Source Identifier</strong> value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>From the list, select <strong>MSDE</strong>.</td>
</tr>
<tr>
<td>Database Name</td>
<td>Type <strong>WSS_Logging</strong> as the name of the Microsoft SharePoint database.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>Type the IP address or host name of the Microsoft SharePoint SQL Server.</td>
</tr>
<tr>
<td>Port</td>
<td>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 SharePoint database. The Microsoft SharePoint database must have incoming TCP connections that are enabled to communicate with QRadar. If you define a Database Instance when you use MSDE as the database type, you must leave the Port parameter blank in your configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name the log source can use to access the Microsoft SharePoint database.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password the log source can use to access the Microsoft SharePoint database. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the Password field.</td>
</tr>
<tr>
<td>Authentication Domain</td>
<td>If you did not select Use Microsoft JDBC, Authentication Domain is displayed. The domain for MSDE databases that are a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the Database Instance parameter must be blank in the log source configuration.</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the none option.</td>
</tr>
<tr>
<td>Table Name</td>
<td>Type AuditEvent as the name of the table or view that includes the event records.</td>
</tr>
<tr>
<td>Select List</td>
<td>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 it is needed for your configuration. The list must contain the field that is defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Type EventTime as the compare field. The compare field is used to identify new events added between queries to the table.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Use Prepared Statements</strong></td>
<td>Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.</td>
</tr>
<tr>
<td><strong>Start Date and Time (Optional)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Type the polling interval, which is the amount of time between queries to the AuditEvent view you created. 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.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td><strong>Use Named Pipe Communication</strong></td>
<td>If you did not select <strong>Use Microsoft JDBC</strong>, <strong>Use Named Pipe Communication</strong> is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
<tr>
<td><strong>Use NTLMv2</strong></td>
<td>If you did not select <strong>Use Microsoft JDBC</strong>, <strong>Use NTLMv2</strong> is displayed. Select the <strong>Use NTLMv2</strong> check box. This option forces MSDE connections to use the NTLMv2 protocol when it communicates with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the <strong>Use NTLMv2</strong> check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td><strong>Use Microsoft JDBC</strong></td>
<td>If you want to use the Microsoft JDBC driver, you must enable <strong>Use Microsoft JDBC</strong>.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>Select this check box if your connection supports SSL communication. This option requires extra configuration on your SharePoint database and also requires administrators to configure certificates on both appliances.</td>
</tr>
<tr>
<td><strong>Microsoft SQL Server Hostname</strong></td>
<td>If you selected <strong>Use Microsoft JDBC</strong> and <strong>Use SSL</strong>, the <strong>Microsoft SQL Server Hostname</strong> parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC parameters, see c_logsource_JDBCprotocol.dita.
Note: Selecting a parameter value greater than 5 for the Credibility weights your Microsoft SharePoint log source with a higher importance compared to other log sources in QRadar.

4. Click Save.
5. On the Admin tab, click Deploy Changes.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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 a SharePoint log source for predefined database queries

Administrators who do not have permission to create a database view because of policy restrictions can collect Microsoft SharePoint events with a log source that uses predefined queries.

About this task
Predefined queries are customized statements that can join data from separate tables when the database is polled by the JDBC protocol. To successfully poll for audit data from the Microsoft SharePoint database, you must create a new user or provide the log source with existing user credentials. For more information on creating a user account, see your vendor documentation.

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 SharePoint.
7. From the Protocol Configuration list, select JDBC.
8. Configure the following values:

<table>
<thead>
<tr>
<th>Table 453. Microsoft SharePoint JDBC parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
</tbody>
</table>
| Log Source Identifier | Type the identifier for the log source. Type the log source identifier in the following format:  
                                          \(<SharePoint Database>@\langleSharePoint Database Server IP or Host Name>\)  
                                          Where:  
                                          • \(<SharePoint Database>\) is the database name, as entered in the Database Name parameter.  
                                          • \(<SharePoint Database Server IP or Host Name>\) is the host name or IP address for this log source, as entered in the IP or Hostname parameter. |
<p>| Database Type      | From the list, select MSDE.                                                   |
| Database Name      | Type WSS_Logging as the name of the Microsoft SharePoint database.            |
| IP or Hostname     | Type the IP address or host name of the Microsoft SharePoint SQL Server.      |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>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 SharePoint database. The Microsoft SharePoint database must have incoming TCP connections that are enabled to communicate with IBM QRadar. If you define a <strong>Database Instance</strong> when you use <strong>MSDE</strong> as the database type, you must leave the <strong>Port</strong> parameter blank in your configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name the log source can use to access the Microsoft SharePoint database.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password the log source can use to access the Microsoft SharePoint database. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the <strong>Password</strong> field.</td>
</tr>
<tr>
<td>Authentication Domain</td>
<td>If you select <strong>MSDE</strong> as the <strong>Database Type</strong> and the database is configured for Windows Authentication, you must specify the Windows Authentication Domain. Otherwise, leave this field blank.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>Optional. Type 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 block access to port 1434 for SQL database resolution, you must leave the <strong>Database Instance</strong> parameter blank in your configuration.</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>From the list, select <strong>Microsoft SharePoint</strong>.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Select the <strong>Use Prepared Statements</strong> check box. Prepared statements allow the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>Optional. Type the start date and time for database polling. If a start date or time is not selected, polling begins immediately and repeats at the specified polling interval.</td>
</tr>
</tbody>
</table>
### Microsoft SharePoint JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Type the polling interval, which is the amount of time between queries to the AuditEvent view you created. 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.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td><strong>Use Named Pipe Communication</strong></td>
<td>Clear the Use Named Pipe Communications check box. When 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.</td>
</tr>
<tr>
<td><strong>Use NTLMv2</strong></td>
<td>Select the Use NTLMv2 check box. This option forces MSDE connections to use the NTLMv2 protocol when they communicate with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>Select this check box if your connection supports SSL communication. This option requires extra configuration on your SharePoint database and also requires administrators to configure certificates on both appliances.</td>
</tr>
<tr>
<td><strong>Database Cluster Name</strong></td>
<td>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 to ensure Named Pipe communication functions properly.</td>
</tr>
</tbody>
</table>

**Note:** Selecting a parameter value greater than 5 for the Credibility weights your Microsoft SharePoint log source with a higher importance compared to other log sources in QRadar.

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

---

**Microsoft SQL Server**

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
</tbody>
</table>
You can integrate Microsoft SQL Server with QRadar by using one of the following methods:

**Syslog**

The IBM QRadar DSM for Microsoft SQL Server can collect LOGbinder SQL events. For information about configuring LOGbinder SQL to collect events from your Microsoft SQL Server, go to the IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/en/SS42VS_DSM/c_dsm_guide_logbinderex_ms_sql_overview.html)

**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, 2014 Enterprise, and 2016.

**WinCollect**


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 concepts**

“LOGbinder SQL event collection from Microsoft SQL Server” on page 730
The IBM QRadar DSM for Microsoft SQL Server can collect LOGbinder SQL events.

**Related tasks**

“Configuring your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar” on page 731
To collect Microsoft SQL Server LOGbinder events, you must configure your LOGbinder SQL system to send events to IBM QRadar.

“Adding a DSM” on page 4
“Adding a log source” on page 4
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” on page 801.

**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);
GO
```

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. Click the Log Sources icon.
3. Click the Add button.
4. From the Log Source Type list, select Microsoft SQL Server.
5. From the Protocol Configuration list, select JDBC or WinCollect.
6. Optional. If you want to configure events for JDBC, configure the parameters. The following table describes the JDBC parameters that require specific values to collect events from Microsoft SQL Server:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description (Optional)</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>From the list, select Microsoft SQL Server.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>From the list, select JDBC.</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database Type</td>
<td>From the list, select <strong>MSDE</strong>.</td>
</tr>
<tr>
<td>Database Name</td>
<td>Type <strong>Master</strong> as the name of the Microsoft SQL database.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>Type the IP address or host name of the Microsoft SQL server.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number that is used by the database server. The default port for MSDE is 1433.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> If you define a <strong>Database Instance</strong> when you are using MSDE as the <strong>Database Type</strong>, you must leave the <strong>Port</strong> parameter blank in your configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name to access the SQL database.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password to access the SQL database.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Type the password to access the SQL database.</td>
</tr>
<tr>
<td>Authentication Domain</td>
<td>If you did not select <strong>Use Microsoft JDBC, Authentication Domain</strong> is displayed.</td>
</tr>
<tr>
<td></td>
<td>The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Database Instance</td>
<td><strong>Optional:</strong> If you have multiple SQL server instances on your database server, type the database instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> 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 <strong>Database Instance</strong> parameter blank.</td>
</tr>
<tr>
<td>Predefined Query (Optional)</td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the <strong>none</strong> option.</td>
</tr>
<tr>
<td>Table Name</td>
<td>Type <strong>dbo.AuditData</strong> as the name of the table or view that includes the audit event records.</td>
</tr>
<tr>
<td>Select List</td>
<td>Type * for all fields from the table or view.</td>
</tr>
<tr>
<td></td>
<td>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 <strong>Compare Field</strong> 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 (.).</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Type <strong>event_time</strong> in the <strong>Compare Field</strong> parameter. The <strong>Compare Field</strong> identifies new events that are added between queries, in the table.</td>
</tr>
<tr>
<td>Start Date and Time (Optional)</td>
<td><strong>Optional:</strong> Type the start date and time for database polling.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Start Date and Time</strong> parameter must be formatted as <strong>yyyy-MM-dd HH:mm</strong> with <strong>HH</strong> 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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td>Use Named Pipe Communication</td>
<td>If you did not select Use Microsoft JDBC, Use Named Pipe Communication is displayed. 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.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>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.</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select Use Microsoft JDBC, Use NTLMv2 is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable Use Microsoft JDBC.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option if your connection supports SSL. This option appears only for MSDE.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected Use Microsoft JDBC and Use SSL, the Microsoft SQL Server Hostname parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

For more information about configuring the JDBC protocol, see JDBC Protocol configuration options.

7. Optional. If you want to configure events for WinCollect, see the IBM QRadar WinCollect User Guide.

8. Click Save.

**Microsoft System Center Operations Manager**

A QRadar Microsoft System Center Operations Manager (SCOM) DSM accepts SCOM events by polling the Operations Manager database and this allows QRadar to record the relevant events.

**About this task**

Before you configure QRadar to integrate with the Microsoft SCOM, check that a database user account is configured with appropriate permissions to access the SCOM Operations Manager SQL Server database. The appropriate authentication mode might need to be enabled in the Security settings of the SQL Server properties. For more information, see your Microsoft SCOM documentation.

**Note:** Ensure that no firewall rules are blocking the communication between QRadar and the SQL Server database that is associated with SCOM. For SCOM installations that use a separate, dedicated computer for the SQL Server database, the EventView view is queried on the database system, not the system that runs SCOM.

To configure QRadar to receive SCOM events:

**Procedure**

1. Click the Admin tab.
2. Click the Log Sources icon.
3. Click Add.
4. Configure the parameters. The following table describes the parameters that require specific values to collect events from Microsoft SCOM by using the JDBC protocol:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Microsoft SCOM</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
</tbody>
</table>
| Log Source Identifier   | Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol.  
 If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2. |
| Database Type           | From the list, select MSDE.                                                                                                               |
| Database Name           | The name of the Microsoft SCOM database.                                                                                                  |
| IP or Hostname          | Type the IP address or host name of the Microsoft SCOM SQL Server.                                                                       |
Table 455. Microsoft SCOM JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>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 SCOM database. The Microsoft SCOM database must have incoming TCP connections that are enabled to communicate with QRadar. If you define a Database Instance when MSDE is used as the database type, you must leave the Port parameter blank in your configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name that is required to access the database.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password that is required to access the database. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the Password parameter.</td>
</tr>
<tr>
<td>Authentication Domain</td>
<td>If you did not select Use Microsoft JDBC, Authentication Domain is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>Optional. Type 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 block access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.</td>
</tr>
<tr>
<td>Table Name</td>
<td>Type EventView as the name of the table or view that includes the event records.</td>
</tr>
<tr>
<td>Select List</td>
<td>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 you need it for your configuration. The list must contain the field that is defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Type TimeAdded as the compare field. The compare field is used to identify new events added between queries to the table.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>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 the 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.</td>
</tr>
</tbody>
</table>
### Table 455. Microsoft SCOM JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Prepared Statements</strong></td>
<td>Select this check box to use prepared statements. Prepared statements allow the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Type the polling interval, which 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.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td><strong>Use Named Pipe Communication</strong></td>
<td>If you did not select <strong>Use Microsoft JDBC, Use Named Pipe Communication</strong> is displayed. Clear the <strong>Use Named Pipe Communications</strong> check box. When 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.</td>
</tr>
<tr>
<td><strong>Database Cluster Name</strong></td>
<td>If you select the <strong>Use Named Pipe Communication</strong> check box, the <strong>Database Cluster Name</strong> parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.</td>
</tr>
<tr>
<td><strong>Use NTLMv2</strong></td>
<td>If you did not select <strong>Use Microsoft JDBC, Use Named Pipe Communication</strong> is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td><strong>Use Microsoft JDBC</strong></td>
<td>If you selected <strong>Use Microsoft JDBC</strong> and <strong>Use SSL</strong>, the <strong>Microsoft SQL Server Hostname</strong> parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>Select this option if your connection supports SSL.</td>
</tr>
<tr>
<td><strong>Microsoft SQL Server Hostname</strong></td>
<td>If you selected <strong>Use SSL</strong>, the <strong>Microsoft SQL Server Hostname</strong> parameter displays. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>
Note: Selecting a value greater than 5 for the Credibility parameter weights your Microsoft SCOM log source with a higher importance compared to other log sources in QRadar.

5. Click **Save**.
6. On the **Admin** tab, click **Deploy Changes**.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 Windows Defender ATP

The IBM QRadar DSM for Microsoft Windows Defender® ATP collects events from a Microsoft Windows Defender ATP system.

To integrate Microsoft Windows Defender ATP with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - Windows Defender ATP REST API Protocol RPM
   - DSMCommon RPM
   - Microsoft Windows Defender ATP DSM RPM

2. Configure your Microsoft Windows Defender ATP appliance to send events to QRadar.

3. Add a Microsoft Windows Defender ATP log source that uses the Microsoft Windows Defender ATP REST API on the QRadar Console. QRadar does not automatically detect the Microsoft Windows Defender ATP REST API.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 Windows Defender ATP DSM specifications

The following table describes the specifications for the Microsoft Windows Defender ATP DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>DSM name</td>
<td>Microsoft Windows Defender ATP</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-MicrosoftWindowsDefenderATP-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol</td>
<td>Windows Defender ATP REST API</td>
</tr>
<tr>
<td>Event format</td>
<td>JSON</td>
</tr>
</tbody>
</table>

---
Table 456. Microsoft Windows Defender ATP DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recorded event types</td>
<td>Windows Defender ATP</td>
</tr>
<tr>
<td></td>
<td>Windows Defender AV</td>
</tr>
<tr>
<td></td>
<td>Third Party TI</td>
</tr>
<tr>
<td></td>
<td>Customer TI</td>
</tr>
<tr>
<td></td>
<td>Bitdefender</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

Configuring QRadar to collect events from Microsoft Windows Defender ATP by using the Windows Defender ATP REST API

The Microsoft Windows Defender ATP REST API collects alerts from the Windows Defender Advanced Threat Protection security service.

**Before you begin**

Before you can add a log source in QRadar, you must obtain the Microsoft Windows Defender ATP connection information by completing the following steps:

1. Log in to the Windows Defender Security Center.
2. From the menu on the left, click Settings.
3. From the Settings window, in the API section, click SIEM.
4. From the SIEM application details list, copy and record the values for the Client ID and the Authorization server URL and Resource fields. You need these values when you configure a log source in QRadar.

**Note:** You need the Client Secret value to connect to QRadar. The Client Secret value is only displayed the first time that you go to the page. If you don’t have access to the Client Secret value, contact your Microsoft Azure administrator to request a new client secret.

**Procedure**

1. Click the Admin tab.
2. Click the Log Sources, and then click Add.
3. From the Log Source Type list, select Microsoft Windows Defender ATP.
4. From the Protocol Configuration list, select Windows Defender ATP REST API, and configure the parameters.

The following table describes the parameters that require specific values to collect alerts from Microsoft Windows Defender ATP by using the Windows Defender ATP REST API.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Server URL</td>
<td>The URL for the server that provides the authorization to obtain an access token. The access token is used as the authorization to obtain events from Windows Defender ATP. The Authorization Server URL uses the format, “<a href="https://login.windows.net/%E2%80%9D%5BTenant_ID%5D/oauth2/token">https://login.windows.net/”[Tenant_ID]/oauth2/token</a> Where &lt;Tenant_ID&gt; is a UUID.</td>
</tr>
<tr>
<td>Resource</td>
<td>The resource that is used to access Windows Defender ATP events.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Ensures that the user is authorized to obtain an access token.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Ensures that the user is authorized to obtain an access token. The Client Secret value is displayed only one time, and then is no longer visible. If you don't have access to the Client Secret value, contact your Microsoft Azure administrator to request a new client secret.</td>
</tr>
<tr>
<td>Regions</td>
<td>Select the regions that are associated with Windows Defender ATP that you want to collect logs from.</td>
</tr>
<tr>
<td>Other Region</td>
<td>Type the names of any additional regions that are associated with Windows Defender ATP that you want to collect logs from. Use a comma-separated list; for example, region1,region2.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If a proxy for QRadar is configured, all traffic for the log source travels through the proxy for QRadar to access Windows Defender ATP. Configure the Proxy Server, Proxy Port, Proxy Username, and Proxy Password fields. If the proxy does not require authentication, configure the Proxy Server and Proxy Port fields.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>You can specify how often the log collects data. The format is M/H/D for Months/Hours/Days. The default is 5 M.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The upper limit for the maximum number of events per second (EPS). The default is 5000.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

6. On the **Admin** tab, click **Deploy Changes**.
**Sample event messages**

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when using the Microsoft Windows Defender ATP REST API protocol for the Microsoft Windows Defender ATP DSM:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Defender ATP command and control alert</td>
<td>Suspicious Activity</td>
<td>`{&quot;AlertTime&quot;:&quot;2017-12-27T03:54:41.194393Z&quot;,&quot;ComputerDnsName&quot;:&quot;&lt;ComputerDnsName&gt;&quot;,&quot;AlertTitle&quot;:&quot;&lt;AlertTitle&gt;&quot;,&quot;Category&quot;:&quot;CommandAndControl&quot;,&quot;Severity&quot;:&quot;&lt;Severity&gt;&quot;,&quot;AlertId&quot;:&quot;&lt;AlertId&gt;&quot;,&quot;Actor&quot;:&quot;&lt;Actor&gt;&quot;,&quot;LinkToWDATP&quot;:&quot;&lt;LinkToWDATP&gt;&quot;,&quot;IocName&quot;:&quot;&lt;IocName&gt;&quot;,&quot;IocValue&quot;:&quot;&lt;IocValue&gt;&quot;,&quot;CreatorIocName&quot;:&quot;&lt;CreatorIocName&gt;&quot;,&quot;CreatorIocValue&quot;:&quot;&lt;CreatorIocValue&gt;&quot;,&quot;Sha1&quot;:&quot;&lt;Sha1&gt;&quot;,&quot;FileName&quot;:&quot;&lt;FileName&gt;&quot;,&quot;FilePath&quot;:&quot;&lt;FilePath&gt;&quot;,&quot;IpAddress&quot;:&quot;192.0.2.0&quot;,&quot;Url&quot;:&quot;&lt;Url&gt;&quot;,&quot;IoaDefinitionId&quot;:&quot;&lt;IoaDefinitionId&gt;&quot;,&quot;UserName&quot;:&quot;&lt;UserName&gt;&quot;,&quot;AlertPart&quot;:&quot;&lt;AlertPart&gt;&quot;,&quot;FullId&quot;:&quot;&lt;FullId&gt;&quot;,&quot;LastProcessedTimeUtc&quot;:&quot;2017-12-27T07:16:34.1412283Z&quot;,&quot;ThreatCategory&quot;:&quot;&lt;ThreatCategory&gt;&quot;,&quot;ThreatFamily&quot;:&quot;&lt;ThreatFamily&gt;&quot;,&quot;ThreatName&quot;:&quot;&lt;ThreatName&gt;&quot;,&quot;RemediationAction&quot;:&quot;&lt;RemediationAction&gt;&quot;,&quot;RemediationIsSuccess&quot;:&quot;&lt;RemediationIsSuccess&gt;&quot;,&quot;Source&quot;:&quot;WindowsDefenderAtp&quot;,&quot;Md5&quot;:&quot;&lt;Md5&gt;&quot;,&quot;Sha256&quot;:&quot;&lt;Sha256&gt;&quot;,&quot;WasExecutingWhileDetected&quot;:&quot;&lt;WasExecutingWhileDetected&gt;&quot;,&quot;UserDomain&quot;:&quot;&lt;UserDomain&gt;&quot;,&quot;LogOnUsers&quot;:&quot;&lt;LogOnUsers&gt;&quot;,&quot;MachineDomain&quot;:&quot;&lt;MachineDomain&gt;&quot;,&quot;MachineName&quot;:&quot;&lt;MachineName&gt;&quot;}</td>
</tr>
<tr>
<td>Windows Defender ATP malware alert</td>
<td>Misc. Malware</td>
<td>`{&quot;AlertTime&quot;:&quot;2017-12-26T21:28:21.5123241Z&quot;,&quot;ComputerDnsName&quot;:&quot;&lt;ComputerDnsName&gt;&quot;,&quot;AlertTitle&quot;:&quot;&lt;AlertTitle&gt;&quot;,&quot;Category&quot;:&quot;Malware&quot;,&quot;Severity&quot;:&quot;&lt;Severity&gt;&quot;,&quot;AlertId&quot;:&quot;&lt;AlertId&gt;&quot;,&quot;Actor&quot;:&quot;&lt;Actor&gt;&quot;,&quot;LinkToWDATP&quot;:&quot;&lt;LinkToWDATP&gt;&quot;,&quot;IocName&quot;:&quot;&lt;IocName&gt;&quot;,&quot;IocValue&quot;:&quot;&lt;IocValue&gt;&quot;,&quot;CreatorIocName&quot;:&quot;&lt;CreatorIocName&gt;&quot;,&quot;CreatorIocValue&quot;:&quot;&lt;CreatorIocValue&gt;&quot;,&quot;Sha1&quot;:&quot;&lt;Sha1&gt;&quot;,&quot;FileName&quot;:&quot;&lt;FileName&gt;&quot;,&quot;FilePath&quot;:&quot;&lt;FilePath&gt;&quot;,&quot;IpAddress&quot;:&quot;192.0.2.0&quot;,&quot;Url&quot;:&quot;&lt;Url&gt;&quot;,&quot;IoaDefinitionId&quot;:&quot;&lt;IoaDefinitionId&gt;&quot;,&quot;UserName&quot;:&quot;&lt;UserName&gt;&quot;,&quot;AlertPart&quot;:&quot;&lt;AlertPart&gt;&quot;,&quot;FullId&quot;:&quot;&lt;FullId&gt;&quot;,&quot;LastProcessedTimeUtc&quot;:&quot;2017-12-27T04:54:17.1700156Z&quot;,&quot;ThreatCategory&quot;:&quot;&lt;ThreatCategory&gt;&quot;,&quot;ThreatFamily&quot;:&quot;&lt;ThreatFamily&gt;&quot;,&quot;ThreatName&quot;:&quot;&lt;ThreatName&gt;&quot;,&quot;RemediationAction&quot;:&quot;&lt;RemediationAction&gt;&quot;,&quot;RemediationIsSuccess&quot;:&quot;&lt;RemediationIsSuccess&gt;&quot;,&quot;Source&quot;:&quot;WindowsDefenderAtp&quot;,&quot;Md5&quot;:&quot;&lt;Md5&gt;&quot;,&quot;Sha256&quot;:&quot;&lt;Sha256&gt;&quot;,&quot;WasExecutingWhileDetected&quot;:&quot;&lt;WasExecutingWhileDetected&gt;&quot;,&quot;UserDomain&quot;:&quot;&lt;UserDomain&gt;&quot;,&quot;LogOnUsers&quot;:&quot;&lt;LogOnUsers&gt;&quot;,&quot;MachineDomain&quot;:&quot;&lt;MachineDomain&gt;&quot;,&quot;MachineName&quot;:&quot;&lt;MachineName&gt;&quot;,&quot;InternalIPv4List&quot;:&quot;192.0.2.0;127.0.0.1&quot;,&quot;InternalIPv6List&quot;:&quot;2001:0DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF&quot;,&quot;FileHash&quot;:&quot;&lt;FileHash&gt;&quot;,&quot;ExternalId&quot;:&quot;&lt;ExternalId&gt;&quot;,&quot;IocUniqueId&quot;:&quot;IocUniqueId&quot;}</td>
</tr>
<tr>
<td>Event name</td>
<td>Low-level category</td>
<td>Sample log message</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
                                             "AlertTitle": "<AlertTitle>", "Category": "Exploit",
                                             "Severity": "<Severity>", "AlertId": "<AlertId>", "Actor": "<Actor>",
                                             "LinkToWDATP": "<LinkToWDATP>", "IocName": "<IocName>",
                                             "IocValue": "<IocValue>", "CreatorIocName": "<CreatorIocName>",
                                             "CreatorIocValue": "<CreatorIocValue>", "Sha1": "<Sha1>",
                                             "FileName": "<FileName>", "FilePath": "<FilePath>", "IpAddress": "192.0.2.0",
                                             "Url": "<Url>", "IoaDefinitionId": "<IoaDefinitionId>", "UserName": "qradar1",
                                             "AlertPart": "<AlertPart>", "FullId": "<FullId>", "LastProcessedTimeUtc": "2017-11-22T17:04:04.8338919Z",
                                             "ThreatCategory": "<ThreatCategory>", "ThreatFamily": "<ThreatFamily>",
                                             "ThreatName": "<ThreatName>", "RemediationAction": "<RemediationAction>",
                                             "RemediationIsSuccess": "<RemediationIsSuccess>"} |
| Windows Defender ATP backdoor alert | Backdoor Detected | { "AlertTime": "2017-11-22T18:01:32.1887752Z", "ComputerDnsName": "<ComputerDnsName>",
                                             "AlertTitle": "<AlertTitle>", "Category": "Backdoor",
                                             "Severity": "<Severity>", "AlertId": "<AlertId>", "Actor": "<Actor>",
                                             "LinkToWDATP": "<LinkToWDATP>", "IocName": "<IocName>",
                                             "IocValue": "<IocValue>", "CreatorIocName": "<CreatorIocName>",
                                             "CreatorIocValue": "<CreatorIocValue>", "Sha1": "<Sha1>",
                                             "FileName": "<FileName>", "FilePath": "<FilePath>", "IpAddress": "192.0.2.0",
                                             "Url": "<Url>", "IoaDefinitionId": "<IoaDefinitionId>", "UserName": "qradar1",
                                             "AlertPart": "<AlertPart>", "FullId": "<FullId>", "LastProcessedTimeUtc": "2017-11-22T18:01:49.8739015Z",
                                             "ThreatCategory": "<ThreatCategory>", "ThreatFamily": "<ThreatFamily>",
                                             "ThreatName": "<ThreatName>", "RemediationAction": "<RemediationAction>",
                                             "RemediationIsSuccess": "<RemediationIsSuccess>"} |
Microsoft Windows Security Event Log

The IBM 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.

All events, including Sysmon, are supported.

**Related tasks**

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

Enabling WMI on Windows hosts

**Verifying MSRPC Protocol**

For most users, the Microsoft Security Event Log over MSRPC protocol is provided automatically to the IBM QRadar appliance through automatic updates.

The MSRPC can be verified through the log sources user interface or by verifying that the Windows Event RPC protocol RPM file is installed from the QRadar console.

**Verifying MSRPC protocol from the QRadar Console**

You can verify that the MSRPC protocol is installed on QRadar Console by using SSH.

**About this task**

The following RPM files are required to collect and parse events with the MSRPC protocol.

- PROTOCOL-WindowsEventRPC-<version>.noarch.rpm
- DSM-DSMCommon-<version>.noarch.rpm
- DSM-MicrosoftWindows-<version>.noarch.rpm

**Procedure**

1. Log in to QRadar Console as the root user through SSH.
2. Type `yum list|grep -i windows` to verify that MSRPC protocol is installed.
3. From the output, verify that PROTOCOL-WindowsEventRPC-<version>.noarch.rpm is installed.

   If the MSRPC RPM is installed, but doesn't appear in the user interface as part of the protocols for Microsoft Windows Security Event Log, the administrator needs to restart the web server.

**Related tasks**

“Restarting the Web Server” on page 814
You must be an administrator to restart the Web Server.

**Verifying MSRPC protocol from QRadar user interface**
You can verify that the MSRPC is installed through the user interface of the QRadar Console.

**Procedure**
1. Log in to QRadar
2. Click **Admin** > **Data sources**.
3. Click the **Log Sources** icon
4. Click **Add**
5. In the Log Source Type field, select Microsoft Windows Security Event Log from the list
6. In the Protocol Configuration field, verify that Microsoft Security Event Log over MSRPC appears in the list

**Restarting the Web Server**
You must be an administrator to restart the Web Server.

**Procedure**
1. Log in to QRadar.
2. Click the **Admin** tab.
3. From the **Advanced** menu, click **Restart Web Service**.

**Installing the MSRPC protocol on the QRadar Console**
You must install the MSRPC protocol RPM on the QRadar Console before events can be collected from a Windows host.

**Before you begin**
Ensure that you download the MSRPC protocol RPM from IBM Fix Central.

**Procedure**
1. Log in to the QRadar Console as a root user.
2. Copy the MSRPC protocol RPM to a directory on the QRadar Console.
3. Go to the directory where you copied the MSRPC protocol RPM by typing the following command:

   ```
cd <path_to_directory>
   ```

4. Install the MSRPC protocol RPM by typing the following command:

   ```
yum -y install PROTOCOL-WindowsEventRPC-<version_number>.noarch.rpm
   ```

5. From the **Admin** tab of the QRadar Console, select **Advanced** > **Deploy Full Configuration**.
6. After you deploy the configuration, select **Advanced** > **Restart Web Server**.

**Enabling MSRPC on Windows hosts**
To enable communication between your Windows host and IBM 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 QRadar QRadar Event Processor 1628 appliance with 128 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.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Protocol type</td>
<td>The operating system dependant type of the remote procedure protocol for collection of events. Select one of the following options from the Protocol Type list:</td>
</tr>
</tbody>
</table>
|                               | **MS-EVEN6**  
The default protocol type for new log sources.  
The protocol type that is used by QRadar to communicate with Windows Vista and Windows Server 2008 and later. |
|                               | **MS-EVEN (for Windows XP/2003)**  
The protocol type that is used by QRadar to communicate with Windows XP and Windows Server 2003.  
Windows XP and Windows Server 2003 are not supported by Microsoft. The use of this option might not be successful. |
|                               | **auto-detect (for legacy configurations)**  
Previous log source configurations for the Microsoft Windows Security Event Log DSM use the auto-detect (for legacy configurations) protocol type.  
Upgrade to the MS_EVEN6 or the MS-EVEN (for Windows XP/2003) protocol type. |
| Supported versions            | Windows Server 2016  
Windows Server 2012 (most recent)  
Windows Server 2012 Core  
Windows Server 2008 (most recent)  
Windows Server 2008 Core  
Windows 10 (most recent)  
Windows 8 (most recent)  
Windows 7 (most recent)  
Windows Vista (most recent) |
<p>| 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                                      |</p>
<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special features</td>
<td>Supports encrypted events by default.</td>
</tr>
<tr>
<td>Required permissions</td>
<td>The log source user must be a member of the <strong>Event Log Readers</strong> 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 <strong>Backup operators</strong> group can also be used depending on how Microsoft Group Policy Objects are configured. Windows XP and 2003 operating system users require read access to the following registry keys:</td>
</tr>
<tr>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog</td>
</tr>
<tr>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language</td>
</tr>
<tr>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft Windows\CurrentVersion</td>
</tr>
<tr>
<td>Supported event types</td>
<td>Application</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>DNS Server</td>
</tr>
<tr>
<td></td>
<td>File Replication</td>
</tr>
<tr>
<td></td>
<td>Directory Service logs</td>
</tr>
<tr>
<td>Windows service requirements</td>
<td>For Windows Server 2008 and Windows Vista, use the following services:</td>
</tr>
<tr>
<td></td>
<td>• Remote Procedure Call (RPC)</td>
</tr>
<tr>
<td></td>
<td>• RPC Endpoint Mapper</td>
</tr>
<tr>
<td></td>
<td>For Windows 2003, use the Remote Registry and Server.</td>
</tr>
<tr>
<td>Windows port requirements</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>For Windows Server 2008 and Windows Vista, use the following ports:</td>
</tr>
<tr>
<td></td>
<td>• TCP port 135</td>
</tr>
<tr>
<td></td>
<td>• TCP port that is dynamically allocated for RPC, above 49152</td>
</tr>
<tr>
<td></td>
<td>For Windows 2003, use the following ports:</td>
</tr>
<tr>
<td></td>
<td>• TCP port 445</td>
</tr>
<tr>
<td></td>
<td>• TCP port 139</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Specification</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>A security content pack with Windows custom event properties is available on IBM Fix Central.</td>
</tr>
<tr>
<td>Required RPM files</td>
<td>PROTOCOL-WindowsEventRPC-QRadar_release-Build_number.noarch.rpm</td>
</tr>
<tr>
<td></td>
<td>DSM-MicrosoftWindows-QRadar_release-Build_number.noarch.rpm</td>
</tr>
<tr>
<td></td>
<td>DSM-DSMCommon-QRadar_release-Build_number.noarch.rpm</td>
</tr>
<tr>
<td>More information</td>
<td>Microsoft support (<a href="http://support.microsoft.com/">http://support.microsoft.com/</a>)</td>
</tr>
<tr>
<td>Troubleshooting tool available</td>
<td>MSRPC test tool is part of the MSRPC protocol RPM. After installation of the MSRPC protocol RPM, the MSRPC test tool can be found in /opt/qradar/jars</td>
</tr>
</tbody>
</table>

**Procedure**

1. Log in to QRadar as administrator.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. From the **Log Source Type** list, select **Microsoft Windows Security Event Log**.
6. From the **Protocol Configuration** list, select **Microsoft Security Event Log over MSRPC**.
7. 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.
8. From the **Domain** field, type the domain of the Windows system.
9. Configure the log source user name and password parameters.
10. 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.
11. Configure the **Event Throttle** field.
12. From the **Protocol Type** list, select the protocol type for your operating system.
13. 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.
14. Select at least one of the **Event Types** check boxes.
15. Click **Save**.
16. On the **Admin** tab, click **Deploy Changes**.

**Diagnosing connection issues with the MSRPC test tool**

Use the MSRPC test tool to check the connection between the IBM QRadar appliance and a Windows host.

**Before you begin**

Ensure that the **PROTOCOL-WindowsEventRPC-<version_number>** is installed on the QRadar appliance.
About this task

The MSRPC test tool can be used for troubleshooting connection problems and to test the initial connection between the host and the QRadar appliance to ensure that the host is configured properly. Table 1 describes the MSRPC test tool option flags.

<table>
<thead>
<tr>
<th>Flags</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-? or --help</td>
<td>Displays the help and usage information for the MSRPC tool.</td>
</tr>
<tr>
<td>-b</td>
<td>Displays debugging information, if available.</td>
</tr>
<tr>
<td>-d &lt;domain&gt;</td>
<td>Active Directory Domain, or hostname if in a workgroup.</td>
</tr>
<tr>
<td>-e &lt;protocol&gt;</td>
<td>EventLog Remoting protocol. Values: MSEVEN, MSEVEN6, and AUTO</td>
</tr>
<tr>
<td>-h &lt;hostname/ip&gt;</td>
<td>Hostname or IP address of the Windows host.</td>
</tr>
<tr>
<td>-p &lt;password&gt;</td>
<td>Password</td>
</tr>
<tr>
<td>-u &lt;username&gt;</td>
<td>Username</td>
</tr>
</tbody>
</table>

Procedure

1. Log in to the QRadar Console.
2. To use the MSRPC test tool, type the following command:
   
   ```
   cd /opt/qradar/jars
   ```

3. To test for connection between the QRadar and the Windows host, type the following command:

   ```
   java -jar Q1MSRPCTest.jar
   ```

4. Optional: For more usage options, type java -jar Q1MSRPCTest.jar --help

Enabling WMI on Windows hosts

To enable communication between your Windows host and IBM 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.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Microsoft</td>
</tr>
<tr>
<td>DSM name</td>
<td>Windows Security Event Log</td>
</tr>
<tr>
<td>Supported versions</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 (most recent)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 Core</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 (most recent)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 Core</td>
</tr>
<tr>
<td></td>
<td>Windows 10 (most recent)</td>
</tr>
<tr>
<td></td>
<td>Windows 8 (most recent)</td>
</tr>
<tr>
<td></td>
<td>Windows 7 (most recent)</td>
</tr>
<tr>
<td></td>
<td>Windows Vista (most recent)</td>
</tr>
<tr>
<td>Special features</td>
<td>Supports encrypted events by default.</td>
</tr>
<tr>
<td>Intended application</td>
<td>Agentless event collection for Windows operating systems over WMI that is capable of 50 EPS per log source.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This is a legacy protocol. In most cases, new log sources should be configured by using the Microsoft Security Event Log over MSRPC protocol.</td>
</tr>
<tr>
<td>Special configuration instructions</td>
<td>Configuring DCOM and WMI to Remotely Retrieve Windows 7 Events (<a href="http://www.ibm.com/support/docview.wss?uid=swg21678809">http://www.ibm.com/support/docview.wss?uid=swg21678809</a>)</td>
</tr>
<tr>
<td>Windows port requirements</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• TCP port 135 (all operating system versions)</td>
</tr>
<tr>
<td></td>
<td>• TCP port that is dynamically allocated above 49152 (required for Vista and above operating systems)</td>
</tr>
<tr>
<td>Specification</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Windows service requirements</td>
<td>The following services must be configured to start automatically:</td>
</tr>
<tr>
<td></td>
<td>• Remote Procedure Call (RPC)</td>
</tr>
<tr>
<td></td>
<td>• Remote Procedure Call (RPC) Locator</td>
</tr>
<tr>
<td></td>
<td>• RPC Endpoint Mapper</td>
</tr>
<tr>
<td></td>
<td>• Remote Registry</td>
</tr>
<tr>
<td></td>
<td>• Server</td>
</tr>
<tr>
<td></td>
<td>• Windows Management Instrumentation</td>
</tr>
<tr>
<td>Log source permissions</td>
<td>The log source user must be a member of the <strong>Event Log Readers</strong> 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 <strong>Backup operators</strong> group can also be used depending on how Microsoft Group Policy Objects are configured. The log source user must have access to following components:</td>
</tr>
<tr>
<td></td>
<td>• Window event log protocol DCOM components</td>
</tr>
<tr>
<td></td>
<td>• Windows event log protocol name space</td>
</tr>
<tr>
<td></td>
<td>• Appropriate access to the remote registry keys</td>
</tr>
<tr>
<td>Supported event types</td>
<td>Application</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>DNS Server</td>
</tr>
<tr>
<td></td>
<td>File Replication</td>
</tr>
<tr>
<td></td>
<td>Directory Service logs</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No, manual log source creation is required</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>A security content pack with Windows custom event properties is available on IBM Fix Central.</td>
</tr>
<tr>
<td>Required RPM files</td>
<td>PROTOCOL-WinCollectWindowsEventLog-QRadar_release-Build_number.noarch.rpm</td>
</tr>
<tr>
<td></td>
<td>DSM-MicrosoftWindows-QRadar_release-Build_number.noarch.rpm</td>
</tr>
<tr>
<td></td>
<td>DSM-DSMCommon-QRadar_release-Build_number.noarch.rpm</td>
</tr>
<tr>
<td>More information</td>
<td>Microsoft support (support.microsoft.com/)</td>
</tr>
<tr>
<td>Troubleshooting tools available</td>
<td>Yes, a WMI test tool is available in /opt/qradar/jars.</td>
</tr>
</tbody>
</table>

**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 98. Motorola Symbol AP

The Motorola Symbol AP DSM for IBM QRadar records all relevant events forwarded from Motorola Symbol AP devices using syslog.

Configuring a log source

To integrate Motorola Symbol AP with IBM QRadar, you must manually create a log source to receive events.

About this task

QRadar does not automatically discover or create log sources for syslog events from Motorola Symbol AP appliances. In cases where the log source is not automatically discovered, it is suggested that you create a log source before you forward events to QRadar.

To configure a log source:

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   - The Data Sources pane is displayed.
4. Click the Log Sources icon.
   - The Log Sources window is displayed.
5. Click Add.
   - The Add a log source window is displayed.
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 Motorola Symbol AP.
   - The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Motorola Symbol AP appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   - The log source is added to QRadar.
Configure syslog events for Motorola Symbol AP

You can configure the device to forward syslog events to IBM QRadar.

**Procedure**

1. Log in to your Symbol AP device user interface.
2. From the menu, select **System Configuration > Logging Configuration**.
   The Access Point window is displayed.
3. Using the **Logging Level** list, select the desired log level for tracking system events. The options are:
   - 0 - Emergency
   - 1 - Alert
   - 2 - Critical
   - 3 - Errors
   - 4 - Warning
   - 5 - Notice
   - 6 - Info. This is the default.
   - 7 - Debug
4. Select the Enable logging to an external syslog server check box.
5. In the **Syslog Server IP Address** field, type the IP address of an external syslog server, such as QRadar.
   This is required to route the syslog events to QRadar.
6. Click **Apply**.
7. Click **Logout**.
   A confirmation window is displayed.
8. Click **OK** to exit the application.
   The configuration is complete. Events forwarded to QRadar are displayed on the **Log Activity** tab.
Chapter 99. Name Value Pair

The Name Value Pair DSM gives you the option to integrate IBM QRadar with devices that might not normally send syslog logs.

The Name Value Pair DSM provides a log format that gives you the option to send logs to QRadar. For example, for a device that does not export logs natively with syslog, you can create a script to export the logs from a device that QRadar does not support, format the logs in the Name Value Pair log format, and send the logs to QRadar using syslog.

The Name Value Pair DSM log source that is configured in QRadar then receives the logs and is able to parse the data since the logs are received in the Name Value Pair log format.

**Note:** Events for the Name Value Pair DSM are not automatically discovered by QRadar.

The Name Value Pair DSM accepts events by using syslog. QRadar records all relevant events. The log format for the Name Value Pair DSM must be a tab-separated single-line list of Name=Parameter. The Name Value Pair DSM does not require a valid syslog header.

**Note:** The Name Value Pair DSM assumes an ability to create custom scripts or thorough knowledge of your device capabilities to send logs to QRadar using syslog in Name Value Pair format.

The Name Value Pair DSM is able to parse the following tags:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DeviceType</strong></td>
<td>Type NVP as the <strong>DeviceType</strong>. This identifies the log formats as a Name Value Pair log message. This is a required parameter and DeviceType=NVP must be the first pair in the list.</td>
</tr>
<tr>
<td><strong>EventName</strong></td>
<td>Type the event name that you want to use to identify the event in the Events interface when using the Event Mapping functions. For more information on mapping events, see the <em>IBM QRadar User Guide</em>. This is a required parameter.</td>
</tr>
<tr>
<td><strong>EventCategory</strong></td>
<td>Type the event category that you want to use to identify the event in the Events interface. If this value is not included in the log message, the value NameValuePair value is used.</td>
</tr>
<tr>
<td><strong>SourceIp</strong></td>
<td>Type the source IP address for the message.</td>
</tr>
<tr>
<td><strong>SourcePort</strong></td>
<td>Type the source port for the message.</td>
</tr>
<tr>
<td><strong>SourceIpPreNAT</strong></td>
<td>Type the source IP address for the message before Network Address Translation (NAT) occurred.</td>
</tr>
<tr>
<td><strong>SourceIpPostNAT</strong></td>
<td>Type the source IP address for the message after NAT occurs.</td>
</tr>
<tr>
<td><strong>SourceMAC</strong></td>
<td>Type the source MAC address for the message.</td>
</tr>
<tr>
<td><strong>SourcePortPreNAT</strong></td>
<td>Type the source port for the message before NAT occurs.</td>
</tr>
<tr>
<td>Tag</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SourcePortPostNAT</td>
<td>Type the source port for the message after NAT occurs.</td>
</tr>
<tr>
<td>DestinationIp</td>
<td>Type the destination IP address for the message.</td>
</tr>
<tr>
<td>DestinationPort</td>
<td>Type the destination port for the message.</td>
</tr>
<tr>
<td>DestinationIpPreNAT</td>
<td>Type the destination IP address for the message before NAT occurs.</td>
</tr>
<tr>
<td>DestinationIpPostNAT</td>
<td>Type the IP address for the message after NAT occurs.</td>
</tr>
<tr>
<td>DestinationPortPreNAT</td>
<td>Type the destination port for the message before NAT occurs.</td>
</tr>
<tr>
<td>DestinationPortPostNAT</td>
<td>Type the destination port for the message after NAT occurs.</td>
</tr>
<tr>
<td>DestinationMAC</td>
<td>Type the destination MAC address for the message.</td>
</tr>
<tr>
<td>DeviceTime</td>
<td>Type the time that the event was sent, according to the device. The format is: YY/MM/DD hh:mm:ss. If no specific time is provided, the syslog header or DeviceType parameter is applied.</td>
</tr>
<tr>
<td>UserName</td>
<td>Type the user name that is associated with the event.</td>
</tr>
<tr>
<td>HostName</td>
<td>Type the host name that is associated with the event. Typically, this parameter is only associated with identity events.</td>
</tr>
<tr>
<td>GroupName</td>
<td>Type the group name that is associated with the event. Typically, this parameter is only associated with identity events.</td>
</tr>
<tr>
<td>NetBIOSName</td>
<td>Type the NetBIOS name that is associated with the event. Typically, this parameter is only associated with identity events.</td>
</tr>
<tr>
<td>Identity</td>
<td>Type TRUE or FALSE to indicate whether you want this event to generate an identity event. An identity event is generated if the log message contains the SourceIp (if the IdentityUseSrcIp parameter is set to TRUE) or DestinationIp (if the IdentityUseSrcIp parameter is set to FALSE) and one of the following parameters: UserName, SourceMAC, HostName, NetBIOSName, or GroupName.</td>
</tr>
<tr>
<td>IdentityUseSrcIp</td>
<td>Type TRUE or FALSE (default). TRUE indicates that you want to use the source IP address for identity. FALSE indicates that you want to use the destination IP address for identity. This parameter is used only if the Identity parameter is set to TRUE.</td>
</tr>
</tbody>
</table>

**Example 1**
The following example parses all fields:
Example 2
The following example provides identity by using the destination IP address:

```
<133>Apr 16 12:41:00 192.0.2.1 namevaluepair: DeviceType=NVP EventName=Test EventCategory=Accept Identity=TRUE SourceMAC=<MAC_address> SourceIp=<Source_IP_address> DestinationIp=<Destination_IP_address> Username=<Username>
```

Example 3
The following example provides identity by using the source IP address:

```
DeviceType=NVP EventName=Test EventCategory=Accept DeviceTime=2007/12/14 09:53:49 SourcePort=5014 Identity=TRUE IdentityUseSrcIp=TRUE SourceMAC=<MAC_address> SourceIp=<Source_IP_address> DestinationIp=<Destination_IP_address> DestinationMAC=<MAC_address> Username=<Username>
```

Example 4
The following example provides an entry with no identity:

```
DeviceType=NVP EventName=Test EventCategory=Accept DeviceTime=2007/12/14 09:53:49 SourcePort=5014 Identity=FALSE SourceMAC=<MAC_address> SourceIp=<Source_IP_address> DestinationIp=<Destination_IP_address> DestinationMAC=<MAC_address> Username=<Username>
```
The IBM QRadar DSM for NCC Group DDoS Secure collects events from NCC Group DDoS Secure devices. The following table describes the specifications for the NCC Group DDoS Secure DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>NCC Group</td>
</tr>
<tr>
<td>DSM name</td>
<td>NCC Group DDoS Secure</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-NCCGroupDDoSSecure-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>5.13.1-2s to 5.16.1-0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>NCC Group website (<a href="https://www.nccgroup.trust/uk/">https://www.nccgroup.trust/uk/</a>)</td>
</tr>
</tbody>
</table>

To integrate NCC Group DDoS Secure 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
   - NCC Group DDoS Secure DSM RPM

2. Configure your NCC Group DDoS Secure device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add an NCC Group DDoS Secure log source on the QRadar Console. The following table describes the parameters that require specific values to collect event from NCC Group DDoS Secure:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>NCC Group DDoS Secure</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

4. To verify that QRadar is configured correctly, review the following table to see an example of a normalized event message.

The following table shows a sample event message from NCC Group DDoS Secure:
Table 464. NCC Group DDoS Secure sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Attack - Port Scan - END</td>
<td>Host Port Scan</td>
<td>`&lt;134&gt;LEEF:1.0</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 NCC Group DDoS Secure to communicate with QRadar

The NCC Group DDoS Secure DSM for IBM QRadar receives events from NCC Group DDoS Secure devices by using syslog in Log Event Extended Format (LEEF) format. QRadar records all relevant status and network condition events.

Procedure
1. Log in to NCC Group DDoS Secure.
2. Go to the Structured Syslog Server window.
3. In the Server IP Address(es) field, type the IP address of the QRadar Console.
4. From the Format list, select LEEF.
5. Optional: If you do not want to use the default of local0 in the Facility field, type a syslog facility value.
6. From the Priority list, select the syslog priority level that you want to include. Events that meet or exceed the syslog priority level that you select are forwarded to QRadar.
7. In the Log Refresh (Secs) field, specify a refresh update time for structured logs. The refresh update time is specified in seconds.
8. In the Normal Peak Bandwith field, specify the expected normal peak bandwidth of the appliance.
IBM QRadar accepts syslog events from a Windows host by using the WinCollect NetApp Data ONTAP plug-in.

For more information about NetApp Data ONTAP configuration, see the *IBM QRadar WinCollect User Guide*. 

Chapter 102. Netskope Active

The IBM QRadar DSM for Netskope Active collects events from your Netskope Active servers. The following table identifies the specifications for the Netskope Active DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Netskope</td>
</tr>
<tr>
<td>DSM name</td>
<td>Netskope Active</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-NetskopeActive-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>Netskope Active REST API</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Alert, All</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td>Netskope Active website (<a href="http://www.netskope.com">www.netskope.com</a>)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Netskope Active</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Netskope Active REST API</td>
</tr>
</tbody>
</table>

**Related tasks**

- “Adding a DSM” on page 4
- “Configuring QRadar to collect events from your Netskope Active system” on page 834

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 4
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>
<thead>
<tr>
<th>Table 467. Netskope Active DSM log source parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>IP or Hostname</td>
</tr>
<tr>
<td>Authentication Token</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificates</td>
</tr>
<tr>
<td>Throttle</td>
</tr>
<tr>
<td>Recurrence</td>
</tr>
</tbody>
</table>
| 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 103. NGINX HTTP Server

The IBM QRadar DSM for NGINX HTTP Server collects Syslog events from an NGINX HTTP Server device. To integrate NGINX HTTP Server with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Apache HTTP Server DSM RPM
   - NGINX HTTP Server DSM RPM

2. Configure your NGINX HTTP Server device to send events to QRadar.

3. If QRadar does not automatically detect the log source, add an NGINX HTTP Server log source on the QRadar Console. The following table describes the parameters that require specific values to collect Syslog events from NGINX HTTP Server:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>NGINX HTTP Server</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>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, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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

NGINX HTTP Server DSM specifications

The following table describes the specifications for the NGINX HTTP Server DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>NGINX</td>
</tr>
<tr>
<td>DSM name</td>
<td>NGINX HTTP Server</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-NginxWebserver-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>1.15.5</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
</tbody>
</table>
Table 469. NGINX HTTP Server DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event format</td>
<td>LEEF, Standard syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Error log, Access log</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Nginx HTTP Server product information (<a href="https://nginx.com">https://nginx.com</a>)</td>
</tr>
</tbody>
</table>

Configuring NGINX HTTP Server to communicate with QRadar

To collect events from NGINX HTTP Server, configure your NGINX HTTP Server device to forward Syslog events to QRadar.

Procedure

1. Log in to your NGINX HTTP Server device.
2. Open the nginx.conf file.
3. Add the following LEEF format string under http block. For more information about configuring logging, see https://docs.nginx.com/nginx/admin-guide/monitoring/logging/.

   ```
   log_format qradar
   'LEEF:1.0|NGINX|NGINX|$nginx_version|$status|devTime=$time_local	devTimeFormat=dd/MMM/yyyy:HH:mm:ss
   Z\tsrc=$remote_addr\tdst=$server_addr\tdstPort=$server_port\t'proto=$server_protocol\tusUsername=$remote_user\trequest=$request\t'
   'body_bytes_sent=$body_bytes_sent\thttp_referer=$http_referer\thttp_true_client_ip=$http_true_client_ip\t'
   'http_user_agent=$http_user_agent\thttp_x_header=$http_x_header\thttp_x_forwarded_for=$http_x_forwarded_for\t'
   'request_time=$request_time\tupstream_response_time=$upstream_response_time\n   tpipe=$pipe\t'uri_query=$query_string\uri_path=$uri\tcookie=$http_cookie';
   ```

4. Add the following syslog server configuration under http block.

   ```
   access_log syslog:server=QRadar_Server_IP:514,facility=Facility_Parameter qradar;
   ```

5. Save the configuration.
6. To verify the configuration, type the following command:

   ```
   nginx -t
   ```

7. If NGINX is running, reload the configuration by typing the following command:

   ```
   nginx -s reload
   ```

Sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides sample event messages when using the Syslog protocol for the NGINX HTTP Server DSM:
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>404</td>
<td>System Status</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>
Chapter 104. Niksun

The Niksun DSM for IBM QRadar records all relevant Niksun events by using syslog.

You can integrate NetDetector/NetVCR2005, version 3.2.1sp1_2 with QRadar. Before you configure QRadar to integrate with a Niksun device, you must configure a log source, then enable syslog forwarding on your Niksun appliance. For more information about configuring Niksun, see your Niksun appliance documentation.

Configuring a log source

To integrate Niksun with IBM QRadar, you must manually create a log source to receive events.

About this task

QRadar does not automatically discover or create log sources for syslog events from Niksun appliances. In cases where the log source is not automatically discovered, it is suggested that you create a log source before you forward events to QRadar.

To configure a log source:

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.

   The Data Sources pane is displayed.
4. Click the Log Sources icon.

   The Log Sources window is displayed.
5. Click Add.

   The Add a log source window is displayed.
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 Niksun 2005 v3.5.

   The syslog protocol configuration is displayed.
10. Configure the following values:

   Table 471. Syslog parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Niksun appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

   The log source is added to QRadar.
Chapter 105. Nokia Firewall

The Check Point Firewall-1 DSM allows IBM QRadar to accept Check Point-based Firewall events sent from Nokia Firewall appliances by using syslog or OPSEC protocols.

Integration with a Nokia Firewall by using syslog

This method gives you the option to configure your Nokia Firewall to accept Check Point syslog events that are forwarded from your Nokia Firewall appliance.

To configure IBM QRadar to integrate with a Nokia Firewall device, take the following steps:

1. Configure iptables on your QRadar Console or Event Collector to receive syslog events from Nokia Firewall.
2. Configure your Nokia Firewall to forward syslog event data.
3. Configure the events that are logged by the Nokia Firewall.

Configuring IPtables

Nokia Firewalls require a TCP reset (rst) or a TCP acknowledge (ack) from IBM QRadar on port 256 before they forward syslog events.

About this task

The Nokia Firewall TCP request is an online status request that is designed to ensure that QRadar is online and able to receive syslog events. If a valid reset or acknowledge is received from QRadar, then Nokia Firewall begins forwarding events to QRadar on UDP port 514. By default, QRadar does not respond to any online status requests from TCP port 256.

You must configure IPtables on your QRadar Console or any Event Collector that receives Check Point events from a Nokia Firewall to respond to an online status request.

Procedure

1. Using SSH, log in to QRadar as the root user.
   
   Login: root
   
   Password: <password>

2. Type the following command to edit the IPtables file:

   `vi /opt/qradar/conf/iptables.pre`

   The IPtables configuration file is displayed.

3. Type the following command to instruct QRadar to respond to your Nokia Firewall with a TCP reset on port 256:

   `-A INPUT -s <IP address> -p tcp --dport 256 -j REJECT --reject-with tcp-reset`

   Where `<IP address>` is the IP address of your Nokia Firewall. You must include a TCP reset for each Nokia Firewall IP address that sends events to your QRadar Console or Event Collector, for example,

   - `-A INPUT -s <IP_address1>/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset`
   - `-A INPUT -s <IP_address2>/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset`
   - `-A INPUT -s <IP_address3>/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset`

4. Save your IPtables configuration.
5. Type the following command to update IPtables in QRadar:
   
   ./opt/qradar/bin/iptables_update.pl

6. Repeat steps 1 - 5 to configure any additional QRadar Event Collectors that receive syslog events from a Nokia Firewall.

   You are now ready to configure your Nokia Firewall to forward events to QRadar.

**Configuring syslog**

To configure your Nokia Firewall to forward syslog events to IBM QRadar:

**Procedure**

1. Log in to the Nokia Voyager.
2. Click **Config**.
3. In the **System Configuration** pane, click **System Logging**.
4. In the **Add new remote IP address to log to** field, type the IP address of your QRadar Console or Event Collector.
5. Click **Apply**.
6. Click **Save**.

   You are now ready to configure which events are logged by your Nokia Firewall to the logger.

**Configuring the logged events custom script**

To configure which events are logged by your Nokia Firewall and forwarded to IBM QRadar, you must configure a custom script for your Nokia Firewall.

**Procedure**

1. Using SSH, log in to Nokia Firewall as an administrative user.
   
   If you cannot connect to your Nokia Firewall, check that SSH is enabled. You must enable the command-line by using the Nokia Voyager web interface or connect directly by using a serial connection. For more information, see your Nokia Voyager documentation.

2. Type the following command to edit your Nokia Firewall rc.local file:
   
   vi /var/etc/rc.local

3. Add the following command to your rc.local file:
   
   `$FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &`

4. Save the changes to your rc.local file.

   The terminal is displayed.

5. To begin logging immediately, type the following command:
   
   nohup `$FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &`

   You can now configure the log source in QRadar.

**Configuring a log source**

Events that are forwarded by your Nokia Firewall are automatically discovered by the Check Point Firewall-1 DSM. The automatic discovery process creates a log source for syslog events from Nokia Firewall appliances.

**About this task**

The following steps are optional.
**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 **Check Point Firewall-1**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Nokia Firewall appliance.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The syslog configuration for receiving Check Point events from Nokia Firewalls over syslog is complete. Check Point events from your Nokia Firewall are displayed in the **Log Activity** tab in IBM QRadar.

### Integration with a Nokia Firewall by using OPSEC

IBM QRadar can accept Check Point FireWall-1 events from Nokia Firewalls using the Check Point FireWall-1 DSM configured using the OPSEC/LEA protocol.

Before you configure QRadar to integrate with a Nokia Firewall device, you must:

1. Configure Nokia Firewall using OPSEC, see “Configuring a Nokia Firewall for OPSEC” on page 843.
2. Configure a log source in QRadar for your Nokia Firewall using the OPSEC LEA protocol, see “Configuring an OPSEC log source” on page 844.

### Configuring a Nokia Firewall for OPSEC

You can configure Nokia Firewall by using OPSEC.

**Procedure**

1. To create a host object for your IBM QRadar, open up the Check Point SmartDashboard GUI, and select **Manage > Network Objects > New > Node > Host**.
2. Type the Name, IP address, and an optional comment for your QRadar.
3. Click **OK**.
4. Select **Close**.
5. To create the OPSEC connection, select **Manage > Servers and OPSEC Applications > New > OPSEC Application Properties**.
6. Type the Name and an optional comment.

   The name that you type must be different from the name in “Configuring a Nokia Firewall for OPSEC” on page 843.
7. From the **Host drop-down** menu, select the QRadar host object that you created.
8. From Application Properties, select User Defined as the Vendor Type.
9. From Client Entries, select LEA.
10. Select Communication and enter an activation key to configure the Secure Internal Communication (SIC) certificate.
11. Select OK and then select Close.
12. To install the policy on your firewall, select Policy > Install > OK.

For more information on policies, see your vendor documentation. You can now configure a log source for your Nokia Firewall in QRadar.

**Configuring an OPSEC log source**

You must create an OPSEC log source to collect events, because OPSEC/LEA log sources are not automatically discovered in IBM QRadar.

**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 Check Point FireWall-1.
9. Using the Protocol Configuration list, select OPSEC/LEA.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type an IP address, host name, or name to identify the event source. IP addresses or host names are better because they enable QRadar to match a log file to a unique event source.</td>
</tr>
<tr>
<td>Server IP</td>
<td>Type the IP address of the server.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Type the port that is used for OPSEC communication. The valid range is 0 - 65,536 and the default is 18184.</td>
</tr>
<tr>
<td>Use Server IP for Log Source</td>
<td>Select this check box if you want to use the LEA server's IP address instead of the managed device's IP address for a log source. By default, the check box is selected.</td>
</tr>
<tr>
<td>Statistics Report Interval</td>
<td>Type the interval, in seconds, during which syslog events are recorded in the qradar.log file. The valid range is 4 - 2,147,483,648 and the default is 600.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>From the list, select the authentication type that you want to use for this LEA configuration. The options are <strong>sslca</strong> (default), <strong>sslca_clear</strong>, or <strong>clear</strong>. This value must match the authentication method that is used by the server. The following parameters appear if <strong>sslca</strong> or <strong>sslca_clear</strong> is selected as the authentication type:</td>
</tr>
<tr>
<td></td>
<td>• <strong>OPSEC Application Object SIC Attribute (SIC Name)</strong> - Type the Secure Internal Communications (SIC) name of the OPSEC Application Object. The SIC name is the distinguished name (DN) of the application, for example: CN=LEA, o=xxxxxxxxx..xxxxxx. The name can be up to 255 characters in length and is case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log Source SIC Attribute (Entity SIC Name)</strong> - Type the SIC name of the server, for example: cn=cp_mgmt,o=xxxxxxxxx..xxxxxx. The name can be up to 255 characters in length and is case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Specify Certificate</strong> - Select this check box if you want to define a certificate for this LEA configuration. QRadar attempts to retrieve the certificate by using these parameters when the certificate is required.</td>
</tr>
<tr>
<td></td>
<td>If you select the <strong>Specify Certificate</strong> check box, the <strong>Certificate Filename</strong> parameter is displayed:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Certificate Filename</strong> - This option appears only if <strong>Specify Certificate</strong> is selected. Type the file name of the certificate that you want to use for this configuration. The certificate file must be located in the /opt/qradar/conf/trusted_certificates/lea directory.</td>
</tr>
<tr>
<td></td>
<td>If you clear the <strong>Specify Certificate</strong> check box, the following parameters appear:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Certificate Authority IP</strong> - Type the IP address of the SmartCenter server from which you want to pull your certificate.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pull Certificate Password</strong> - Type the password that you want to use when a certificate is requested. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OPSEC Application</strong> - Type the name of the application you want to use when a certificate is requested. This value can be up to 255 characters in length.</td>
</tr>
</tbody>
</table>

11. Click **Save**.

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

   The configuration is complete. As events are received, they are displayed in the **Log Activity** tab in QRadar.
Chapter 106. Nominum Vantio

**Note:** The Nominum Vantio DSM for QRadar is deprecated.

The Nominum Vantio DSM for IBM QRadar accepts syslog events in Log Extended Event Format (LEEF) forwarded from Nominum Vantio engines that are installed with the Nominum Vantio LEEF Adapter.

QRadar accepts all relevant events that are forwarded from Nominum Vantio.

The Vantio LEEF Adapter creates LEEF messages based on Lightweight View Policy (LVP) matches. To generate LVP matches for the Vantio LEEF Adapter to process, you must configure Lightweight Views and the lvp-monitor for the Vantio engine. LVP is an optionally licensed component of the Nominum Vantio product.

Before you can integrate Nominum Vantio events with QRadar, you must install and configure the Vantio LEEF adapter.
Chapter 107. Nortel Networks

Several Nortel Networks DSMs can be integrated with IBM QRadar.

Nortel Multiprotocol Router

The Nortel Multiprotocol Router DSM for IBM QRadar records all relevant Nortel Multiprotocol Router events by using syslog.

About this task

Before you configure QRadar to integrate with a Nortel Multiprotocol Router device, you must:

Procedure

1. Log in to your Nortel Multiprotocol Router device.
2. At the prompt, type the following command:
   
   bcc

   The Bay Command Console prompt is displayed.

   Welcome to the Bay Command Console!

   * To enter configuration mode, type config
   * To list all system commands, type ?
   * To exit the BCC, type exit
   bcc>

3. Type the following command to access configuration mode:

   config

4. Type the following command to access syslog configuration:

   syslog

5. Type the following commands:

   log-host address <IP address>

   Where <IP address> is the IP address of your QRadar.

6. View current default settings for your QRadar:

   info

   For example:

   log-host/<IP_address># info
   address <IP_address>
   log-facility local0
   state enabled

7. If the output of the command entered in “Nortel Multiprotocol Router” on page 849 indicates that the state is not enabled, type the following command to enable forwarding for the syslog host:

   state enable

8. Configure the log facility parameter:

   log-facility local0
9. Create a filter for the hardware slots to enable them to forward the syslog events. Type the following command to create a filter with the name WILDCARD:

   `filter name WILDCARD entity all`

10. Configure the slot-upper bound parameter:

    `slot-upper bound <number of slots>`

    Where `<number of slots>` is the number of slots available on your device. This parameter can require different configuration which depends on your version of Nortel Multiprotocol Router device, which determines the maximum number of slots available on the device.

11. Configure the level of syslog messages you want to send to your QRadar.

    `severity-mask all`

12. View the current settings for this filter:

    `info`

    For example:

    `filter/<IP_address>/WILDCARD# info`

    `debug-map debug`

    `entity all`

    `event-lower-bound 0`

    `event-upper-bound 255`

    `fault-map critical`

    `info-map info`

    `name WILDCARD`

    `severity-mask {fault warning info trace debug}`

    `slot-lower-bound 0`

    `slot-upper-bound 1`

    `state enabled`

    `trace-map debug`

    `warning-map warning`

13. View the currently configured settings for the syslog filters:

    `show syslog filters`

    When the syslog and filter parameters are correctly configured, the Operational State indicates up.

    For example:

    `syslog# show syslog filters`

    `show syslog filters Sep 15, 2008 18:21:25 [GMT+8]`

    | Host IP address | Filter Name | Entity Name | Entity Code | Configured State | Operational State |
    |-----------------|-------------|-------------|-------------|------------------|-------------------|
    | <IP_address1>   | WILDCARD    | all         | 255         | enabled          | up                |
    | <IP_address2>   | WILDCARD    | all         | 255         | enabled          | up                |

14. View the currently configured syslog host information:
show syslog log-host
The host log displays the number of packets that are going to the various syslog hosts.
For example:

syslog# show syslog log-host
show syslog log-host Sep 15, 2008 18:21:32 [GMT+8]

<table>
<thead>
<tr>
<th>Host IP address</th>
<th>Configured State</th>
<th>Operational State</th>
<th>Time Sequencing</th>
<th>UDP Port</th>
<th>Facility Code</th>
<th>#Messages Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP_address 1&gt;</td>
<td>enabled</td>
<td>up</td>
<td>disabled</td>
<td>514</td>
<td>local0</td>
<td>1402</td>
</tr>
<tr>
<td>&lt;IP_address 2&gt;</td>
<td>enabled</td>
<td>up</td>
<td>disabled</td>
<td>514</td>
<td>local0</td>
<td>131</td>
</tr>
</tbody>
</table>

15. Exit the command line interface:
   a) Exit the current command line to return to the bcc command line:
      exit
16. Exit the bbc command line:
    exit
17. Exit the command-line session:
    logout
18. You can now configure the log source in QRadar.
   To configure QRadar to receive events from a Nortel Multiprotocol Router device:
   a) From the Log Source Type list, select the Nortel Multiprotocol Router option.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Nortel Application Switch**

Nortel Application Switches integrate routing and switching by forwarding traffic at layer 2 speed by using layer 4-7 information.

**About this task**

The Nortel Application Switch DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant status and network condition events. Before you configure a Nortel Application Switch device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

**Procedure**

1. Log in to the Nortel Application Switch command-line interface (CLI).
2. Type the following command:
   /cfg/sys/syslog/host
3. At the prompt, type the IP address of your QRadar:
   Enter new syslog host: <IP address>
   Where <IP address> is the IP address of your QRadar.
4. Apply the configuration:
   apply
5. After the new configuration is applied, save your configuration:
   save
6. Type y at the prompt to confirm that you want to save the configuration to flash.
   See the following example:
   Confirm saving to FLASH [y/n]: y
   New config successfully saved to FLASH
   Next you will need to configure QRadar to receive events from a Nortel Application Switch:
7. Configure the log source in QRadar. From the Log Source Type list, select the Nortel Application Switch option.
   For more information about the Nortel Application Switch, see your vendor documentation.

Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Nortel Contivity
A QRadar Nortel Contivity DSM records all relevant Nortel Contivity events by using syslog.

About this task
Before you configure QRadar to integrate with a Nortel Contivity device, take the following steps:

Procedure
1. Log in to the Nortel Contivity command-line interface (CLI).
2. Type the following command:
   enable <password>
   Where <password> is the Nortel Contivity device administrative password.
3. Type the following command:
   config t
4. Configure the logging information:
   logging <IP address> facility-filter all level all
   Where <IP address> is the IP address of the QRadar.
5. Type the following command to exit the command-line:
   exit
   Next you will need to configure QRadar to receive events from a Nortel Contivity device.
6. You can now configure the log source in QRadar. From the Log Source Type list, select the Nortel Contivity VPN Switch
   For more information about your Nortel Contivity device, see your vendor documentation.
Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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

Nortel Ethernet Routing Switch 2500/4500/5500

The IBM QRadar Nortel Ethernet Routing Switch (ERS) 2500/4500/5500 DSM records all relevant routing switch events by using syslog.

About this task
Before configuring a Nortel ERS 2500/4500/5500 device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

Procedure
1. Log in to the Nortel ERS 2500/4500/5500 user interface.
2. Type the following commands to access global configuration mode:
   
   ena
   config term
3. Type informational as the severity level for the logs you want to send to the remote server.
   
   For example, logging remote level {critical|informational|serious|none}
   
   logging remote level informational
   
   Where a severity level of informational sends all logs to the syslog server.
4. Enable the host:
   
   host enable
5. Type the remote logging address:
   
   logging remote address <IP address>
   
   Where <IP address> is the IP address of the QRadar system.
6. Ensure that remote logging is enabled:
   
   logging remote enable
   
   You can now configure the log source in QRadar.
7. To configure to receive events from a Nortel ERS 2500/4500/5500 device: From the Log Source Type list, select the Nortel Ethernet Routing Switch 2500/4500/5500 option.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Nortel Ethernet Routing Switch 8300/8600

The IBM QRadar Nortel Ethernet Routing Switch (ERS) 8300/8600 DSM records all relevant events by using syslog.

About this task

Before you configure a Nortel ERS 8600 device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

Procedure

1. Log in to the Nortel ERS 8300/8600 command-line interface (CLI).
2. Type the following command:
   
   ```
   config sys syslog host <ID>
   ```
   
   Where `<ID>` is the ID of the host you wish to configure to send syslog events to QRadar.
   
   For the syslog host ID, the valid range is 1 - 10.
3. Type the IP address of your QRadar system:
   
   ```
   address <IP address>
   ```
   
   Where `<IP address>` is the IP address of your QRadar system.
4. Type the facility for accessing the syslog host:
   
   ```
   host <ID> facility local0
   ```
   
   Where `<ID>` is the ID specified in “Nortel Ethernet Routing Switch 8300/8600” on page 854.
5. Enable the host:
   
   ```
   host enable
   ```
6. Type the severity level for which syslog messages are sent:
   
   ```
   host <ID> severity info
   ```
   
   Where `<ID>` is the ID specified in “Nortel Ethernet Routing Switch 8300/8600” on page 854.
7. Enable the ability to send syslog messages:
   
   ```
   state enable
   ```
8. Verify the syslog configuration for the host:
   
   ```
   sylog host <ID> info
   ```
   
   For example, the output might resemble the following:

   ```
   ERS-8606:5/config/sys/syslog/host/1# info Sub-Context: Current Context:
   address : 192.0.2.1 create : 1 delete : N/A facility : local6 host : enable
   mapinfo : info mapwarning : warning maperror : error mapfatal : emergency
   severity : info|warning|error|fatal udp-port : 514 ERS-8606:5/config/sys/
   syslog/host/1#
   ```
   
   You can now configure the log source in QRadar.
9. To configure QRadar to receive events from a Nortel ERS 8300/8600 device: From the Log Source Type list, select the Nortel Ethernet Routing Switch 8300/8600 option.
Related tasks

“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Nortel Secure Router

The IBM QRadar Nortel Secure Router DSM records all relevant router events by using syslog.

About this task

Before you configure a Nortel Secure Router device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

Procedure

1. Log in to the Nortel Secure Router command line interface (CLI).
2. Type the following to access global configuration mode:
   ```
   config term
   ```
3. Type the following command:
   ```
   system logging syslog
   ```
4. Type the IP address of the syslog server (QRadar system):
   ```
   host_ipaddr <IP address>
   ```
   Where `<IP address>` is the IP address of the QRadar system.
5. Ensure that remote logging is enabled:
   ```
   enable
   ```
6. Verify that the logging levels are configured correctly:
   ```
   show system logging syslog
   ```
   The following code is an example of the output:
   ```
   ------------------------------------ Syslog Setting
   ------------------------------------
   Syslog: Enabled Host IP Address: <IP_address> Host UDP Port: 514
   Facility Priority Setting:
   facility priority
   ========= ========
   auth: info  
   bootp: warning  
   daemon: warning  
   domainname: warning  
   gated: warning  
   kern: info  
   mail: warning  
   ntp: warning
   ```
You can now configure the log source in QRadar.

7. To configure QRadar to receive events from a Nortel Secure Router device: From the Log Source Type list, select the Nortel Secure Router option.

**Related tasks**

“Adding a log source” on page 4

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

---

**Nortel Secure Network Access Switch**

The IBM QRadar Nortel Secure Network Access Switch (SNAS) DSM records all relevant switch events by using syslog.

**About this task**

Before you configure a Nortel SNAS device in QRadar, take the following steps:

**Procedure**

1. Log in to the Nortel SNAS user interface.
2. Select the Config tab.
   
   The Secure Access Domain window is displayed.
4. From the Secure Access Domain list, select the secure access domain. Click Refresh.
5. Click Add.
   
   The Add New Remote Server window is displayed.
6. Click Update.
   
   The server is displayed in the secure access domain table.
7. Using the toolbar, click Apply to send the current changes to the Nortel SNAS.
   
   You are now ready to configure the log source in QRadar.
8. To configure QRadar to receive events from a Nortel SNAS device: From the Log Source Type list, select the Nortel Secure Network Access Switch (SNAS) option.

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Nortel Switched Firewall 5100**

A IBM QRadar Nortel Switched Firewall 5100 DSM records all relevant firewall events by using either syslog or OPSEC.

Before you configure a Nortel Switched Firewall device in QRadar, you must configure your device to send events to QRadar.

See information about configuring a Nortel Switched Firewall by using one the following methods:

- “Integrating Nortel Switched Firewall by using syslog” on page 857
- “Integrate Nortel Switched Firewall by using OPSEC” on page 858

**Integrating Nortel Switched Firewall by using syslog**

This method ensures the IBM QRadar Nortel Switched Firewall 5100 DSM accepts events by using syslog.

**About this task**

To configure your Nortel Switched Firewall 5100:

**Procedure**

1. Log into your Nortel Switched Firewall device command-line interface (CLI).
2. Type the following command:

   /cfg/sys/log/syslog/add

3. Type the IP address of your QRadar system at the following prompt:

   Enter IP address of syslog server:

   A prompt is displayed to configure the severity level.

4. Configure **info** as the severity level.

   For example, Enter minimum logging severity

   (emerg | alert | crit | err | warning | notice | info | debug): info

   A prompt is displayed to configure the facility.

5. Configure **auto** as the local facility.

   For example, Enter the local facility (auto | local0-local7): auto

6. Apply the configuration:

   apply

7. Repeat for each firewall in your cluster.

   You are now ready to configure the log source in QRadar.

8. To configure QRadar to receive events from a Nortel Switched Firewall 5100 device by using syslog:

   From the Log Source Type list, select the **Nortel Switched Firewall 5100** option.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Integrate Nortel Switched Firewall by using OPSEC**

This method ensures the IBM QRadar Nortel Switched Firewall 5100 DSM accepts Check Point FireWall-1 events by using OPSEC.

Depending on your Operating System, the procedures for the Check Point SmartCenter Server can vary. The following procedures are based on the Check Point SecurePlatform Operating system.

To enable Nortel Switched Firewall and QRadar integration, take the following steps:

1. Reconfigure Check Point SmartCenter Server.
2. Configure the log source in QRadar.

**Configuring a log source**

Configure the log source in QRadar.

**Procedure**

1. To configure QRadar to receive events from a Nortel Switched Firewall 5100 device that uses OPSEC, you must select the **Nortel Switched Firewall 5100** option from the **Log Source Type** list.
2. To configure QRadar to receive events from a Check Point SmartCenter Server that uses OPSEC LEA, you must select the **LEA** option from the **Protocol Configuration** list when you configure your protocol configuration.

**Related concepts**

“OPSEC/LEA protocol configuration options” on page 76

To receive events on port 18184, configure a log source to use the OPSEC/LEA protocol.

**Related tasks**

“Adding a log source” on page 4

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

**Nortel Switched Firewall 6000**

A IBM QRadar Nortel Switched Firewall 6000 DSM records all relevant firewall events by using either syslog or OPSEC.

Before you configure a Nortel Switched Firewall device in QRadar, you must configure your device to send events to QRadar.

The following information is about configuring a Nortel Switched Firewall 6000 device with QRadar by using one of the following methods:

- “Configuring syslog for Nortel Switched Firewalls” on page 858
- “Configuring OPSEC for Nortel Switched Firewalls ” on page 859

**Configuring syslog for Nortel Switched Firewalls**

This method ensures the IBM QRadar Nortel Switched Firewall 6000 DSM accepts events by using syslog.

**About this task**

To configure your Nortel Switched Firewall 6000:

**Procedure**

1. Log into your Nortel Switched Firewall device command-line interface (CLI).
2. Type the following command:
   /cfg/sys/log/syslog/add
3. Type the IP address of your QRadar system at the following prompt:
   Enter IP address of syslog server:
   A prompt is displayed to configure the severity level.
4. Configure info as the severity level.
   For example, Enter minimum logging severity
   (emerg | alert | crit | err | warning | notice | info | debug): info
   A prompt is displayed to configure the facility.
5. Configure auto as the local facility.
   For example, Enter the local facility (auto | local0-local7): auto
6. Apply the configuration:
   apply
   You can now configure the log source in QRadar.
7. To configure QRadar to receive events from a Nortel Switched Firewall 6000 using syslog: From the Log Source Type list, select the Nortel Switched Firewall 6000 option.

Related tasks
“Adding a log source” on page 4
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 OPSEC for Nortel Switched Firewalls
This method ensures the IBM QRadar Nortel Switched Firewall 6000 DSM accepts Check Point FireWall-1 events by using OPSEC.

About this task
Depending on your Operating System, the procedures for the Check Point SmartCenter Server can vary. The following procedures are based on the Check Point SecurePlatform Operating system.

To enable Nortel Switched Firewall and QRadar integration, take the following steps:

Procedure
1. Reconfigure Check Point SmartCenter Server. See “Reconfiguring the Check Point SmartCenter Server” on page 860.
2. Configure the OPSEC LEA protocol in QRadar.
   To configure QRadar to receive events from a Check Point SmartCenter Server that uses OPSEC LEA, you must select the LEA option from the Protocol Configuration list when you configure LEA.
3. Configure the log source in QRadar.
   To configure QRadar to receive events from a Nortel Switched Firewall 6000 device using OPSEC you must select the Nortel Switched Firewall 6000 option from the Log Source Type list.

Related concepts
“OPSEC/LEA protocol configuration options” on page 76
To receive events on port 18184, configure a log source to use the OPSEC/LEA protocol.

Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Reconfiguring the Check Point SmartCenter Server**

In the Check Point SmartCenter Server, you can create a host object that represents the IBM QRadar system. The *leapipe* is the connection between the Check Point SmartCenter Server and QRadar.

**About this task**

To reconfigure the Check Point SmartCenter Server:

**Procedure**

1. To create a host object, open the Check Point SmartDashboard user interface and select **Manage > Network Objects > New > Node > Host**.
2. Type the Name, IP address, and type a comment for your host if you want.
3. Click **OK**.
4. Select **Close**.
5. To create the OPSEC connection, select **Manage > Servers and OPSEC applications > New > OPSEC Application Properties**.
6. Type the Name, and type a comment if you want.
7. From the **Host** drop-down menu, select the host object that you have created in “Reconfiguring the Check Point SmartCenter Server” on page 860.
8. From **Application Properties**, select **User Defined** as the vendor.
9. From **Client Entries**, select **LEA**.
10. Click **Communication** to generate a Secure Internal Communication (SIC) certificate and enter an activation key.
11. Click **OK** and then click **Close**.
12. To install the Security Policy on your firewall, select **Policy > Install > OK**.

   The configuration is complete.

**Nortel Threat Protection System (TPS)**

The IBM QRadar Nortel Threat Protection System (TPS) DSM records all relevant threat and system events by using syslog.

**About this task**

Before you configure a Nortel TPS device in QRadar, take the following steps:

**Procedure**

1. Log in to the Nortel TPS user interface.
2. Select **Policy & Response > Intrusion Sensor > Detection & Prevention**.
3. Click **Edit** next to the intrusion policy you want to configure alerting option.
4. Click **Alerting**.

The configuration is complete.
5. Under **Syslog Configuration**, select **on next to State** to enable **syslog alerting**.

6. From the list, select the facility and priority levels.

7. Optional: In the **Logging Host** field, type the IP address of your QRadar system. This configures your QRadar system to be your logging host. Separate multiple hosts with commas.

8. Click **Save**.

   The **syslog alerting** configuration is saved.

9. Apply the policy to your appropriate detection engines.

   You can now configure the log source in QRadar.

10. To configure QRadar to receive events from a Nortel TPS device: From the **Log Source Type** list, select the **Nortel Threat Protection System (TPS) Intrusion Sensor** option.

**Related tasks**

   “Adding a DSM” on page 4
   “Adding a log source” on page 4

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

### Nortel VPN Gateway

The IBM QRadar Nortel VPN Gateway DSM accepts events by using syslog.

**About this task**

QRadar records all relevant operating system (OS), system control, traffic processing, startup, configuration reload, AAA, and IPSec events. Before you configure a Nortel VPN Gateway device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

**Procedure**

1. Log in to the Nortel VPN Gateway command-line interface (CLI).
2. Type the following command:
   
   /cfg/sys/syslog/add

3. At the prompt, type the IP address of your QRadar system:
   
   Enter new syslog host: <IP address>
   
   Where <IP address> is the IP address of your QRadar system.
4. Apply the configuration:
   
   apply
5. View all syslog servers currently added to your system configuration:
   
   /cfg/sys/syslog/list
   
   You can now configure the log source in QRadar.
6. To configure QRadar to receive events from a Nortel VPN Gateway device: From the **Log Source Type** list, select the **Nortel VPN Gateway** option.

**Related tasks**

   “Adding a DSM” on page 4
   “Adding a log source” on page 4

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 108. Novell eDirectory

The Novell eDirectory DSM for IBM QRadar accepts audit events from Novell eDirectory using syslog. To use the Novell eDirectory DSM, you must have the following components installed:

- Novell eDirectory v8.8 with service pack 6 (sp6)
- Novell Audit Plug-in
- Novell iManager v2.7
- XDASv2

To configure Novell eDirectory with QRadar, you must:

1. Configure the XDASv2 property file to forward events to QRadar.
2. Load the XDASv2 module on your Linux or Windows Operating System.
3. Install the Novell Audit Plug-in on the Novell iManager.
4. Configure auditing using Novell iManager.
5. Configure QRadar.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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

Configure XDASv2 to forward events

By default, XDASv2 is configured to log events to a file. To forward events from XDASv2 to QRadar, you must edit the xdasconfig.properties.template and configure the file for syslog forwarding.

About this task
Audit events must be forwarded by syslog to QRadar, instead of being logged to a file.

To configure XDASv2 to forward syslog events:

Procedure

1. Log in to the server hosting Novell eDirectory.
2. Open the following file for editing:
   - Windows - C:\Novell\NDS\dasconfig.properties.template
   - Linux or Solaris - etc/opt/novell/eDirectory/conf/xdasconfig.properties.template
3. To set the root logger, remove the comment marker (#) from the following line:
   
```log4j.rootLogger=debug, S, R```
4. To set the appender, remove the comment marker (#) from the following line:
   
```log4j.appender.S=org.apache.log4j.net.SyslogAppender```
5. To configure the IP address for the syslog destination, remove the comment marker (#) and edit the following lines:
   
```log4j.appender.S.Host=<IP address> log4j.appender.S.Port=<Port>```

Where,

- `<IP address>` is the IP address or hostname of QRadar.
<Port> is the port number for the UDP or TCP protocol. The default port for syslog communication is port **514** for QRadar or Event Collectors.

6. To configure the syslog protocol, remove the comment marker (#) and type the protocol (UDP, TCP, or SSL) use in the following line:

   ```
   log4j.appender.S.Protocol=TCP
   ```
   
The encrypted protocol SSL is not supported by QRadar.

7. To set the severity level for logging events, remove the comment marker (#) from the following line:

   ```
   log4j.appender.S.Threshold=INFO
   ```
   
The default value of INFO is the correct severity level for events.

8. To set the facility for logging events, remove the comment marker (#) from the following line:

   ```
   log4j.appender.S.Facility=USER
   ```
   
The default value of USER is the correct facility value for events.

9. To set the facility for logging events, remove the comment marker (#) from the following line:

   ```
   log4j.appender.R.MaxBackupIndex=10
   ```

10. Save the `xdasconfig.properties.template` file.

     After you configure the syslog properties for XDASv2 events, you are ready to load the XDASv2 module.

---

**Load the XDASv2 Module**

Before you can configure events in Novell iManager, you must load the changes you made to the XDASv2 module.

**About this task**

To load the XDASv2 module, select your operating system.

- To load the XDASv2 in Linux, see “Loading the XDASv2 on a Linux Operating System” on page 864.
- To load the XDASv2 in Windows, see “Loading the XDASv2 on a Windows Operating System” on page 865.

**Important:** If your Novell eDirectory has Novell Module Authentication Service (NMAS) installed with NMAS auditing enabled, the changes made to XDASv2 modules are loaded automatically. If you have NMAS installed, you should configure event auditing. For information on configuring event auditing, see “Configure event auditing using Novell iManager” on page 865.

---

**Loading the XDASv2 on a Linux Operating System**

You can load XDASv2 on a Linux Operating System.

**Procedure**

1. Log in to your Linux server hosting Novell eDirectory, as a root user.
2. Type the following command:

   ```
   ndstrace -c "load xdasauditds"
   ```

**What to do next**

You are now ready to configure event auditing in Novell eDirectory. For more information, see “Configure event auditing using Novell iManager” on page 865.
Loading the XDASv2 on a Windows Operating System

You can load XDASv2 on a Windows Operating System.

**Procedure**

1. Log in to your Windows server hosting Novell eDirectory.
2. On your desktop, click **Start > Run**.
   The Run window is displayed.
3. Type the following:
   ```
   C:\Novell\NDS\ndscons.exe
   ```
   This is the default installation path for the Windows Operating System. If you installed Novell eDirectory to a different directory, then the correct path is required.
4. Click **OK**.
   The Novell Directory Service console displays a list of available modules.
5. From the **Services** tab, select **xdasauditds**.
6. Click **Start**.
   The xdasauditds service is started for Novell eDirectory.
7. Click **Startup**.
   The Service window is displayed.
8. In the **Startup Type** panel, select the **Automatic** check box.
9. Click **OK**.

**What to do next**

You are now ready to configure event auditing in Novell eDirectory. For more information, see “Configure event auditing using Novell iManager” on page 865.

Configure event auditing using Novell iManager

You can configure event auditing for XDASv2 in Novell iManager.

**Procedure**

1. Log in to your Novell iManager console user interface.
2. From the navigation bar, click **Roles and Tasks**.
3. In the left-hand navigation, click **eDirectory Auditing > Audit Configuration**.
   The Audit Configuration panel is displayed.
4. In the **NPC Server name** field, type the name of your NPC Server.
5. Click **OK**.
   The Audit Configuration for the NPC Server is displayed.
6. Configure the following parameters:
   a) On the **Components** panel, select one or both of the following:
      - **DS** - Select this check box to audit XDASv2 events for an eDirectory object.
      - **LDAP** - Select this check box to audit XDASv2 events for a Lightweight Directory Access Protocol (LDAP) object.
6. On the **Log Event’s Large Values** panel, select one of the following:
Log Large Values - Select this option to log events that are larger than 768 bytes.

Don’t Log Large Values - Select this option to log events less than 768 bytes. If a value exceeds 768 bytes, then the event is truncated.

8. On the XDAS Events Configuration, select the check boxes of the events you want XDAS to capture and forward to IBM QRadar.

9. Click Apply.

10. On the XDAS tab, click XDASRoles.

   The XDAS Roles Configuration panel is displayed.

11. Configure the following role parameters:

   a) Select a check box for each object class to support event collection.

12. From the Available Attribute(s) list, select any attributes and click the arrow to add these to the Selected Attribute(s) list.

13. Click OK after you have added the object attributes.

14. Click Apply.

15. On the XDAS tab, click XDASAccounts.

   The XDAS Accounts Configuration panel is displayed.

16. Configure the following account parameters:

   a) From the Available Classes list, select any classes and click the arrow to add these to the Selected Attribute(s) list.

17. Click OK after you have added the object attributes.

18. Click Apply.

What to do next
You are now ready to configure QRadar.

Configure a log source

IBM QRadar automatically detects syslog events from Novell eDirectory. This configuration step is optional.

Procedure

From the Log Source Type list, select Novell eDirectory.

For more information about Novell eDirectory, Novell iManager, or XDASv2, see your vendor documentation.
Chapter 109. Observe IT JDBC

The IBM QRadar DSM for ObserveIT JDBC collects JDBC events from ObserveIT. The following table identifies the specifications for the ObserveIT JDBC DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>ObserveIT</td>
</tr>
<tr>
<td>Product</td>
<td>ObserveIT JDBC</td>
</tr>
<tr>
<td>DSM RPM name</td>
<td>DSM-ObserveIT-QRadar_Version-Build_Number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V5.7</td>
</tr>
<tr>
<td>Protocol</td>
<td>ObserveIT JDBC</td>
</tr>
<tr>
<td></td>
<td>Log File Protocol</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>The following event types are supported by ObserveIT JDBC:</td>
</tr>
<tr>
<td></td>
<td>• Alerts</td>
</tr>
<tr>
<td></td>
<td>• User Activity</td>
</tr>
<tr>
<td></td>
<td>• System Events</td>
</tr>
<tr>
<td></td>
<td>• Session Activity</td>
</tr>
<tr>
<td></td>
<td>• DBA Activity</td>
</tr>
<tr>
<td></td>
<td>The Log File Protocol supports user activity in LEEF logs.</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>ObserveIT website (<a href="http://www.observeit-sys.com">http://www.observeit-sys.com</a>)</td>
</tr>
</tbody>
</table>

To collect ObserveIT JDBC events, 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:
   • ObserveIT JDBC DSM RPM
   • DSMCommon DSM RPM
   • ObserveIT JDBC PROTOCOL RPM
   • JDBC PROTOCOL RPM

2. Make sure that your ObserveIT system is installed and the SQL Server database is accessible over the network.

3. For each ObserveIT server that you want to integrate, create a log source on the QRadar Console. Configure all the required parameters. Use these tables to configure ObserveIT specific parameters:
### Table 476. ObserveIT JDBC log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>ObserveIT</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>ObserveIT JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database name</td>
<td>ObserveIT</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name of the ObserveIT system.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on the ObserveIT host. The default is 1433.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name that is required to connect to the ObserveIT MS SQL database</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is required to connect to the ObserveIT MS SQL database</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>Use the yyyy-MM-dd HH: mm format.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>The frequency by which to poll the database.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The event rate throttle in events per second.</td>
</tr>
</tbody>
</table>

### Table 477. Log file protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Configuration</td>
<td>Log file</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address for the log source. This value must match the value that is configured in the Remote IP or Hostname parameter. The Log Source Identifier value must be unique for the log source type.</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the list, select the protocol that 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 that retrieves 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.</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>The IP address or host name of the device that stores your event log files.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>If the remote host uses a non-standard port number, you must adjust the port value to retrieve events.</td>
</tr>
<tr>
<td>Remote User</td>
<td>The user name necessary to log in to the host that contains your event files. The user name can be up to 255 characters in Length.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>The password that is necessary to log in to the host.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirmation of the password that is necessary to log in to the host.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>The path to the SSH key, if the system is configured to use key authentication. When an SSH key file is used, the Remote Password field is ignored.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>For FTP, if the log files are in the remote user’s home directory, you can leave the remote directory blank. A blank remote directory field supports systems where a change in the working directory (CWD) command is restricted.</td>
</tr>
<tr>
<td>SCP Remote File</td>
<td>If you selected SCP as the Service Type, you must type the file name of the remote file.</td>
</tr>
<tr>
<td>Recursive</td>
<td>This option is ignored for SCP file transfers.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>The regular expression (regex) required to identify the files to download from the remote host.</td>
</tr>
<tr>
<td>FTP Transfer Mode</td>
<td>For ASCII transfers over FTP, you must select NONE in the Processor field and LINEBYLINE in the Event Generator field.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time of day when you want the processing to begin. For example, type 12:00 AM 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 12-hour clock, in the following format: HH:MM &lt;AM/PM&gt;.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The time interval to determine how frequently the remote directory is scanned for new event log files. The time interval can include values in hours (H), minutes (M), or days (D). For example, a recurrence of 2H scans the remote directory every 2 hours.</td>
</tr>
<tr>
<td>Run On Save</td>
<td>Starts the log file import immediately after you save the log source configuration. When selected, this check box clears the list of previously downloaded and processed files. After the first file import, the log file protocol follows the start time and recurrence schedule that is defined by the administrator.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The number of Events Per Second (EPS) that the protocol cannot exceed.</td>
</tr>
<tr>
<td>Processor</td>
<td>Processors allow QRadar to expand event file archives, and to process contents for events. QRadar processes files only after they are downloaded. QRadar can process files in zip, gzip, tar, or tar+gzip archive format.</td>
</tr>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>Tracks and ignores files that were processed by the log file protocol. QRadar examines the log files in the remote directory to determine whether a file was processed previously 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 were not processed previously are downloaded. This option applies only to FTP and SFTP Service Types.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>Changes the local directory on the Target Event Collector to store event logs before they are processed.</td>
</tr>
<tr>
<td>Local Directory</td>
<td>The local directory on the Target Event Collector. The directory must exist before the log file protocol attempts to retrieve events.</td>
</tr>
<tr>
<td>File Encoding</td>
<td>The character encoding that is used by the events in your log file.</td>
</tr>
</tbody>
</table>
### Table 477. Log file protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder Separator</td>
<td>The character that is used to separate folders for your operating system. Most configurations can use the default value in <strong>Folder Separator</strong> field. This field is intended for operating systems that use a different character to define separate folders. For example, periods that separate folders on mainframe systems.</td>
</tr>
</tbody>
</table>

**Related tasks**

Adding a DSM

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.
The IBM QRadar DSM for Okta collects events by using the Okta REST API.

The following table identifies the specifications for the Okta DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Okta</td>
</tr>
<tr>
<td>DSM name</td>
<td>Okta</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-OktaIdentityManagement-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>Okta REST API</td>
</tr>
<tr>
<td>Event format</td>
<td>JSON</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Okta website (<a href="https://www.okta.com/">https://www.okta.com/</a>)</td>
</tr>
</tbody>
</table>

To integrate Okta 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:
   - Protocol Common
   - Okta REST API Protocol RPM
   - Okta DSM RPM

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

2. Configure the required parameters by using the following table for the Okta log source specific parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Okta</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Okta REST API</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>Your personal Okta host name.</td>
</tr>
<tr>
<td>Authentication Token</td>
<td>A single authentication token that is generated by the Okta console and must be used for all API transactions.</td>
</tr>
</tbody>
</table>

© Copyright IBM Corp. 2005, 2019
### Table 479. Okta DSM log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Proxy</td>
<td>When a proxy is configured, all traffic for the log source travels through the proxy for QRadar to access Okta. Configure the Proxy IP or Hostname, 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.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificate(s)</td>
<td>If you select Yes from the list, QRadar downloads the certificate and begins trusting the target server.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The time interval to determine how frequently the remote directory is scanned for new event log files. The time interval can include values in hours (H), minutes (M), or days (D). For example, a recurrence of 2H scans the remote directory every 2 hours. The default is 1M.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The maximum limit for the number of events per second.</td>
</tr>
</tbody>
</table>

The following table provides a sample event message for the Okta DSM:

### Table 480. Okta sample message supported by the Okta device

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| Core-User Auth-Login Success     | User Login Success | ```json
{"eventId":"xxxxxxxxxxxxxxxxxxxxxxx-xxxxxxxxxxxxxxxxxxxx","sessionId":"xxxxxxxxxxxxxxxxxxxxxxx","requestId":"xxxxxxxxxxxxxxxxxxxxxxxxxxxxx","published":"2016-04-06T16:40:00Z","action":{"message":"Sign-in successful","categories": ["Sign-in Success"],"objectType":"core.user_auth.login_success","requestUri":"/api/v1/authn"},"actors": [ {"id":"xxxxxxxxxxxxxxxxxxxxxxx","displayName":"User","login":"username@example.com","objectType":"User"}, { "id": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0", "displayName":"FIREFOX","ipAddress":"<IP_address>" } ],"targets": [ { "id": "xxxxxxxxxxxxxxxxxxxxxxx","displayName":"User","login": "username@example.com","objectType":"User"} ]
```
### Table 480. Okta sample message supported by the Okta device (continued)

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| Core-User Auth-Login Failed     | User Login Failure          | ```{"eventId":"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx","sessionId":","requestId":"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx","published":"2015-08-19T17:08:37.000Z","action":
{"message":"Sign-in Failed - Not Specified","categories":["Sign-in Failure","Suspicious Activity"],
"objectType":"core.user_auth.login_failed","requestUri":"/login/do-login"},
"actors":[
{"id":"Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko","displayName":"x x","ipAddress":"<IP_address>"},
"objectType":"Client"],
"targets":[{"id":","objectType":"User"}]``` |

### Related concepts

“Okta REST API protocol configuration options” on page 76
To receive events from Okta, configure a log source to use the Okta REST API protocol.

### Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.
The IBM QRadar DSM for Onapsis Security Platform collects logs from an Onapsis Security Platform device.

The following table describes the specifications for the Onapsis Security Platform DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Onapsis</td>
</tr>
<tr>
<td>DSM name</td>
<td>Onapsis Security Platform</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-OnapsisIncOnapsisSecurityPlatform-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>1.5.8 and later</td>
</tr>
<tr>
<td>Event format</td>
<td>Log Event Extented Format (LEEF)</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Assessment, Attack signature, Correlation, Compliance</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Onapsis website (<a href="https://www.onapsis.com">https://www.onapsis.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Onapsis Security Platform 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:
   - Onapsis Security Platform DSM RPM
   - DSM Common RPM

2. Configure your Onapsis Security Platform device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add an Onapsis Security Platform log source on the QRadar Console. The following table describes the parameters that require specific values for Onapsis Security Platform event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Onapsis Security Platform</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Onapsis Security Platform to communicate with QRadar**

To collect events from Onapsis Security Platform, you must add a connector and an alarm profile.

**About this task**

Alarm profiles configure the Onapsis Security Platform to automatically take action when an incident is observed.

**Procedure**

1. Log in to Onapsis Security Platform.
2. Click the Gear icon.
3. Click Settings.
4. From Connectors Settings, click Add to include a new connector.
5. Click Respond > Alarm Profiles.
6. Add new alarm profile.
   a) Select Alarm Type and Severity.
   b) Type the name and the description.
   c) Select the target from the Assets List or Tags List.
      The lists are mutually exclusive.
   d) Add a condition for when the alarm is triggered
   e) To add an action that runs when the alarm is triggered, click Action.
   f) Select the QRadar connector that was created in step 4.
Chapter 112. OpenBSD

The OpenBSD DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant informational, authentication, and system level events that are forwarded from OpenBSD operating systems.

Configuring a log source

To integrate OpenBSD events with IBM QRadar, you must manually create a log source. QRadar does not automatically discover or create log sources for syslog events from OpenBSD operating systems.

About this task

To create a log source for OpenBSD:

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   - The Data Sources pane is displayed.
4. Click the Log Sources icon.
   - The Log Sources window is displayed.
5. Click Add.
   - The Add a log source window is displayed.
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 OpenBSD OS.
9. From the Protocol Configuration list, select Syslog.
   - The syslog protocol configuration is displayed.
10. Configure the following values:

    | Parameter        | Description                                                                 |
    |------------------|-----------------------------------------------------------------------------|
    | Log Source Identifier | Type the IP address or host name for the log source as an identifier for events from your OpenBSD appliance. |

11. Click Save.
12. On the Admin tab, click Deploy Changes.

What to do next

The log source is added to QRadar. You are now ready to configure your OpenBSD appliance to forward syslog events.
Configuring syslog for OpenBSD

You can configure OpenBSD to forward syslog events.

Procedure

1. Use SHH, to log in to your OpenBSD device, as a root user.
2. Open the `/etc/syslog.conf` file.
3. Add the following line to the top of the file. Make sure that all other lines remain intact:

   `*. @<IP address>`

   Where `<IP address>` is the IP address of your IBM QRadar.
4. Save and exit the file.
5. Send a hang-up signal to the syslog daemon to ensure that all changes are applied:

   `kill -HUP `cat /var/run/syslog.pid`

   **Note:** This command line uses the back quotation mark character (`'`), which is located to the left of the number one on most keyboard layouts.

The configuration is complete. Events that are forwarded to QRadar by OpenBSD are displayed on the Log Activity tab.
Chapter 113. Open LDAP

The Open LDAP DSM for IBM QRadar accepts UDP Multiline syslog events from Open LDAP installations that are configured to log stats events by using logging level 256.

Open LDAP events are forwarded to QRadar by using port 514. The events must be redirected to the port that is configured for the UDP Multiline syslog protocol. QRadar does not support UDP Multiline syslog on the standard listen port 514.

**Note:** UDP Multiline Syslog events can be assigned to any available port that is not in use, other than port 514. The default port that is assigned to the UDP Multiline Syslog protocol is port 517. If port 517 is already being used in your network, see the QRadar port usage topic in the IBM QRadar Administration Guide or the IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_adm_common_ports.html?pos=2) for a list of ports that are used by QRadar.

**Important:** Forward the UDP Multiline syslog events directly to the chosen port (default 517) from your Open LDAP device. If you can’t send events to this port directly, you can use the backup method of configuring IPtables for UDP Multiline Syslog events.

**Related concepts**
“UDP multiline syslog protocol configuration options” on page 96
To create a single-line syslog event from a multiline event, configure a log source to use the UDP multiline protocol. The UDP multiline syslog protocol uses a regular expression to identify and reassemble the multiline syslog messages into single event payload.

**Related tasks**
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 a log source

IBM QRadar does not automatically discover Open LDAP events that are forwarded in UDP multiline format. To complete the integration, you must manually create a log source for the UDP Multiline Syslog protocol by using the Admin tab in QRadar. Creating the log source allows QRadar to establish a listen port for incoming Open LDAP multiline events.

**About this task**
To configure an Open LDAP log source in QRadar:

**Procedure**
1. Log in to QRadar.
2. Click the Admin tab.
3. In the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 your log source.

8. From the **Log Source Type** list, select **Open LDAP Software**.

9. From the **Protocol Configuration** list, select **UDP Multiline Syslog**.

10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type the IP address or host name for the log source as an identifier for events from your Open LDAP server.</td>
</tr>
</tbody>
</table>
| **Listen Port**         | Type the port number that is used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65536. The default UDP Multiline Syslog listen port is 517. If you do not see the **Listen Port** field, you must restart Tomcat on QRadar. To edit the **Listen Port** number:
  
  Update IPtables on your QRadar Console or Event Collector with the new UDP Multiline Syslog port number. For more information, see “Configuring IPtables for UDP Multiline Syslog events” on page 882.
  
  a. In the **Listen Port** field, type the new port number for receiving UDP Multiline Syslog events.
  
  b. Click **Save**.
  
  The port update is complete and event collection starts on the new port number. |
| **Message ID Pattern**  | Type the regular expression (regex) that is needed to filter the event payload messages. All matching events are included when processing Open LDAP events. 
  The following regular expression is suggested for Open LDAP events:
  conn=(\d+) 
  For example, Open LDAP starts connection messages with the word `conn`, followed by the rest of the event payload. 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/](http://download.oracle.com/javase/tutorial/essential/regex/) |

11. Click **Save**.

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

---

### Configuring IPtables for UDP Multiline Syslog events

To collect UDP Multiline Syslog events in IBM QRadar, if you are unable to send the events directly to the standard UDP Multiline port of 517 or any other available port that is not already in use by QRadar, then you must redirect events from port 514 to the default port 517 or your chosen alternate port by using IPTables as outlined below. You must configure IPTables on your QRadar Console or for each QRadar Event Collector that receives UDP Multiline Syslog events from an Open LDAP server, and then complete the configuration for each Open LDAP server IP address that you want to receive logs from.
Before you begin

Important: Complete this configuration method only if you can’t send UDP Multiline Syslog events directly to the chosen UDP Multiline port on QRadar from your Open LDAP server, and you are restricted to only sending to the standard syslog port 514.

Procedure

1. Using SSH, log in to QRadar as the root user.
   
   Login: <root>
   
   Password: <password>

2. Type the following command to edit the IPtables file:
   
   vi /opt/qradar/conf/iptables-nat.post
   
   The IPtables NAT configuration file is displayed.

3. Type the following command to instruct QRadar to redirect syslog events from UDP port 514 to UDP port 517:
   
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port <new-port> -s <IP address>

   Where:
   
   <IP address> is the IP address of your Open LDAP server.
   
   <New port> is the port number that is configured in the UDP Multiline protocol for Open LDAP.

   You must include a redirect for each Open LDAP IP address that sends events to your QRadar Console or Event Collector. Example:
   
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s <IP_address>

4. Save your IPtables NAT configuration.

   You are now ready to configure IPtables on your QRadar Console or Event Collector to accept events from your Open LDAP servers.

5. Type the following command to edit the IPtables file:
   
   vi /opt/qradar/conf/iptables.post
   
   The IPtables configuration file is displayed.

6. Type the following command to instruct QRadar to allow communication from your Open LDAP servers:
   
   -I QChain 1 -m udp -p udp --src <IP_address> --dport <New port> -j ACCEPT

   Where:
   
   <IP address> is the IP address of your Open LDAP server.
   
   <New port> is the port number that is configured in the UDP Multiline protocol for Open LDAP.

   You must include a redirect for each Open LDAP IP address that sends events to your QRadar Console or Event Collector. Example:
   
   -I QChain 1 -m udp -p udp --src <IP_address> --dport 517 -j ACCEPT

7. Type the following command to update IPtables in QRadar:
   
   ./opt/qradar/bin/iptables_update.pl
Example
If you need to configure another QRadar Console or Event Collector that receives syslog events from an Open LDAP server, repeat these steps.

What to do next
Configure your Open LDAP server to forward events to QRadar.

Configuring event forwarding for Open LDAP
Configure syslog event forwarding for Open LDAP:

Procedure
1. Log in to the command line interface for your Open LDAP server.
2. Edit the following file:
   /etc/syslog.conf
3. Add the following information to the syslog configuration file:
   `<facility>@<IP address>`
   Where:
   `<facility>` is the syslog facility, for example local4.
   `<IP address>` is the IP address of your QRadar Console or Event Collector.
   For example,
   ```
   #Logging for SLAPD local4.debug /var/log/messages local4.debug @<IP_address>
   ```
   Note: If your Open LDAP server stores event messages in a directory other than /var/log/messages, you must edit the directory path.
4. Save the syslog configuration file.
5. Type the following command to restart the syslog service:
   ```
   /etc/init.d/syslog restart
   ```
The configuration for Open LDAP is complete. UDP Multiline Syslog events that are forwarded to QRadar are displayed on the Log Activity tab.
Chapter 114. Open Source SNORT

The Open Source SNORT DSM for IBM QRadar records all relevant SNORT events using syslog. The SourceFire VRT certified rules for registered SNORT users are supported. Rule sets for Bleeding Edge, Emerging Threat, and other vendor rule sets might not be fully supported by the Open Source SNORT DSM.

Configuring Open Source SNORT

To configure syslog on an Open Source SNORT device:

About this task

The following procedure applies to a system that runs Red Hat Enterprise. The following procedures can vary for other operating systems.

Procedure

1. Configure SNORT on a remote system.
2. Open the snort.conf file.
3. Uncomment the following line:

   output alert_syslog:LOG_AUTH LOG_INFO

4. Save and exit the file.
5. Open the following file:

   /etc/init.d/snortd

6. Add a -s to the following lines, as shown in the example:

   daemon /usr/sbin/snort $ALERTMODE
   $BINARY_LOG $NO_PACKET_LOG $DUMP_APP -D
   $PRINT_INTERFACE -i $i -s -u $USER -g
   $GROUP $CONF -i $LOGIR/$i $PASS_FIRST

   daemon /usr/sbin/snort $ALERTMODE
   $BINARY_LOG $NO_PACKET_LOG $DUMP_APP -D
   $PRINT_INTERFACE $INTERFACE -s -u $USER -g
   $GROUP $CONF -i $LOGDIR

7. Save and exit the file.
8. Restart SNORT by typing the following command:

   /etc/init.d/snortd restart

9. Open the syslog.conf file.
10. Update the file to reflect the following code:

    auth.info@<IP Address>

    Where <IP Address> is the system to which you want logs sent.
11. Save and exit the file.
12. Restart syslog:

    /etc/init.d/syslog restart

What to do next

You can now configure the log source in QRadar.
Configuring a log source

IBM QRadar automatically discovers and creates log sources for Open Source SNORT syslog events.

About this task

The following configuration steps are optional.

To create a log source in QRadar:

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 Open Source IDS.
   The syslog protocol configuration is displayed.
10. Configure the following values:

    | Parameter             | Description                                                                 |
    |-----------------------|-----------------------------------------------------------------------------|
    | Log Source Identifier | Type the IP address or host name for the log source as an identifier for your Open Source SNORT events. |

11. Click Save.
12. On the Admin tab, click Deploy Changes.
    The configuration is complete.

For more information about SNORT, see the SNORT documentation at http://www.snort.org/docs/. 886 IBM QRadar : QRadar DSM Configuration Guide
Chapter 115. OpenStack

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

The following table identifies the specifications for the OpenStack DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>OpenStack</td>
</tr>
<tr>
<td>DSM name</td>
<td>OpenStack</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-OpenStackCeilometer-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V2015.1</td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTP Receiver</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit event</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>OpenStack website (<a href="http://www.openstack.org/">http://www.openstack.org/</a>)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>OpenStack</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address of the OpenStack server, and not the host name.</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>HTTPReceiver</td>
</tr>
<tr>
<td>Communication Type</td>
<td>HTTP</td>
</tr>
<tr>
<td>Listen Port</td>
<td>The port number that OpenStack uses to communicate with QRadar.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong>: Do not use Port 514. Port 514 is used by the standard Syslog listener.</td>
</tr>
<tr>
<td>Message Pattern</td>
<td>^{&quot;typeURI</td>
</tr>
</tbody>
</table>

3. Configure your OpenStack device to communicate with QRadar.

The following table provides a sample event message for the OpenStack DSM:
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists details for all servers</td>
<td>Read activity</td>
<td>{&quot;typeURI&quot;: &quot;<a href="http://schemas.dmtf.org/cloud/audit/1.0/event">http://schemas.dmtf.org/cloud/audit/1.0/event</a>&quot;, &quot;eventTime&quot;: &quot;2014-12-09T00:18:52.063878+0000&quot;, &quot;target&quot;: {&quot;typeURI&quot;: &quot;service/compute/servers/detail&quot;, &quot;id&quot;: &quot;openstack:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx&quot;, &quot;name&quot;: &quot;nova&quot;, &quot;addresses&quot;: [{&quot;url&quot;: &quot;http://&lt;IP_address&gt;:8774/v2/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx&quot;, &quot;name&quot;: &quot;admin&quot;}, {&quot;url&quot;: &quot;http://&lt;IP_address&gt;:8774/v2/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx&quot;, &quot;name&quot;: &quot;private&quot;}, {&quot;url&quot;: &quot;http://&lt;IP_address&gt;:8774/v2/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx&quot;, &quot;name&quot;: &quot;public&quot;}], &quot;observer&quot;: {&quot;id&quot;: &quot;target&quot;}, &quot;tags&quot;: [{&quot;correlation_id?value=openstack:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx&quot;}], &quot;eventType&quot;: &quot;activity&quot;, &quot;initiator&quot;: {&quot;typeURI&quot;: &quot;service/security/account/user&quot;, &quot;name&quot;: &quot;admin&quot;, &quot;credential&quot;: {&quot;token&quot;: &quot;xxxx xxxxxxxx xxxx&quot;, &quot;identity_status&quot;: &quot;Confirmed&quot;}, &quot;host&quot;: {&quot;agent&quot;: &quot;python-novaclient&quot;, &quot;address&quot;: &quot;&lt;IP_address&gt;&quot;}, &quot;project_id&quot;: &quot;openstack:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx&quot;, &quot;id&quot;: &quot;openstack:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx&quot;, &quot;action&quot;: &quot;read/list&quot;, &quot;outcome&quot;: &quot;pending&quot;, &quot;id&quot;: &quot;openstack:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx&quot;},</td>
</tr>
</tbody>
</table>

Related tasks

Configuring OpenStack to communicate with QRadar
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.

Adding a DSM

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:
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.


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 116. Oracle

IBM QRadar supports a number of Oracle DSMs.

Oracle Acme Packet Session Border Controller

You can use IBM QRadar to collect events from Oracle Acme Packet Session Border Controller (SBC) installations in your network.

The Oracle Acme Packet SBC installations generate events from syslog and SNMP traps. SNMP trap events are converted to syslog and all events are forwarded to QRadar over syslog. QRadar does not automatically discover syslog events that are forwarded from Oracle Communications SBC. QRadar supports syslog events from Oracle Acme Packet SBC V6.2 and later.

To collect Oracle Acme Packet SBC events, you must complete the following tasks:

1. On your QRadar system, configure a log source with the Oracle Acme Packet Session Border Controller DSM.
2. On your Oracle Acme Packet SBC installation, enable SNMP and configure the destination IP address for syslog events.
3. On your Oracle Acme Packet SBC installation, enable syslog settings on the media-manager object.
4. Restart your Oracle Acme Packet SBC installation.
5. Optional. Ensure that firewall rules do not block syslog communication between your Oracle Acme Packet SBC installation and the QRadar Console or managed host that collects syslog events.

Supported Oracle Acme Packet event types that are logged by IBM QRadar

The Oracle Acme Packet SBC DSM for QRadar can collect syslog events from the authorization and the system monitor event categories.

Each event category can contain low-level events that describe the action that is taken within the event category. For example, authorization events can have low-level categories of login success or login failed.

Configuring an Oracle Acme Packet SBC log source

To collect syslog events from Oracle Acme Packet SBC, you must configure a log source in IBM QRadar. Oracle Acme Packet SBC syslog events do not automatically discover 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. In the Log Source Name field, type a name for your log source.
7. Optional: In the Log Source Description field, type a description for your log source.
8. From the Log Source Type list, select Oracle Acme Packet SBC.
9. From the Protocol Configuration list, select Syslog.
10. Configure the following values:
Table 489. Syslog protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name as an identifier for events from your Oracle Acme Packet SBC installation. The log source identifier must be unique value.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this check box to enable the log source. By default, the check box is selected.</td>
</tr>
<tr>
<td>Credibility</td>
<td>Select the Credibility of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>Select the Event Collector to use as the target for the log source.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the Coalescing Events list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td>Incoming Event Payload</td>
<td>From the list, select the incoming payload encoder for parsing and storing the logs.</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Store Event Payload list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

**What to do next**
You can now configure your Oracle Acme Packet SBC installation.

**Configuring SNMP to syslog conversion on Oracle Acme Packet SBC**
To collect events in a format compatible with IBM QRadar, you must enable SNMP to syslog conversion and configure a syslog destination.

**Procedure**
1. Use SSH to log in to the command-line interface of your Oracle Acme Packet SBC installation, as an administrator.
2. Type the following command to start the configuration mode:
   ```
   config t
   ```
3. Type the following commands to start the system configuration:
   ```
   (configure)# system (system)# (system)# system-config (system-config)# sel
   ```
The `sel` command is required to select a single-instance of the system configuration object.

4. Type the following commands to configure your QRadar system as a syslog destination:

```
(system-config)# syslog-servers (syslog-config)# address <QRadar IP address>
(syslog-config)# done
```

5. Type the following commands to enable SNMP traps and syslog conversion for SNMP trap notifications:

```
(system-config)# enable-snmp-auth-traps enabled (system-config)
# enable-snmp-syslog-notify enabled (system-config)
# enable-snmp-monitor-traps enabled (system-config)
# ids-syslog-facility 4 (system-config)# done
```

6. Type the following commands to return to configuration mode:

```
(system-config)# exit (system)# exit (configure)#
```

### Enabling syslog settings on the media manager object

The media-manager object configuration enables syslog notifications when the Intrusion Detection System (IDS) completes an action on an IP address. The available action for the event might depend on your firmware version.

**Procedure**

1. Type the following command to list the firmware version for your Oracle Acme Packet SBC installation:

```
(configure)# show ver
ACME Net-Net OSVM Firmware SCZ 6.3.9 MR-2 Patch 2 (Build 465) Build Date=03/12/13
```

You may see underlined text which shows the major and minor version number for the firmware.

2. Type the following commands to configure the media-manager object:

```
(configure)# media-manager (media-manager)# (media-manager)# media-manager (media-manager)# sel (media-manager-config)#
```

The `sel` command is used to select a single-instance of the media-manager object.

3. Type the following command to enable syslog messages when an IP is demoted by the Intrusion Detection System (IDS) to the denied queue.

```
(media-manager-config)# syslog-on-demote-to-deny enabled
```

4. For firmware version C6.3.0 and later, type the following command to enable syslog message when sessions are rejected.

```
(media-manager-config)# syslog-on-call-reject enabled
```

5. For firmware version C6.4.0 and later, type the following command to enable syslog messages when an IP is demoted to the untrusted queue.

```
(media-manager-config)# syslog-on-demote-to-untrusted enabled
```

6. Type the following commands to return to configuration mode:

```
(media-manager-config)# done (media-manager-config)# exit (media-manager)#
```

7. Type the following commands to save and activate the configuration:

```
# save Save complete # activate
```

8. Type `reboot` to restart your Oracle Acme Packet SBC installation.

After the system restarts, events are forwarded to IBM QRadar and displayed on the **Log Activity** tab.
Oracle Audit Vault

The IBM QRadar DSM for Oracle Audit Vault collects events from an Oracle Audit Vault server.

The following table describes the specifications for the Oracle Audit Vault DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Oracle</td>
</tr>
<tr>
<td>DSM name</td>
<td>Oracle Audit Vault</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-OracleAuditvault-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>10.3 and 12.2</td>
</tr>
<tr>
<td>Protocol</td>
<td>JDBC</td>
</tr>
<tr>
<td>Event format</td>
<td>name-value pair (NVP)</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All audit records from the AVSYS.AV $ALERT_STORE table for V10.3, or from the custom AVSYS.AV_ALERT_STORE_V view for V12.2. For more information about audit records, see Configuring Oracle Audit Vault to communicate with QRadar.</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate Oracle Audit Vault 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:
   - JDBC Protocol RPM
   - DSMCommon RPM
   - Oracle Audit Vault DSM RPM

2. Obtain the database information for your Oracle Audit Vault server and then configure your Oracle Audit Vault database to allow incoming TCP connections.

3. For each instance of Oracle Audit Vault, add an Oracle Audit Vault log source on the QRadar Event Collector. The following table describes the parameters that require specific values to collect events from Oracle Audit Vault:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Oracle Audit Vault</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
</tbody>
</table>
Table 491. Oracle Audit Vault JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol.</td>
</tr>
<tr>
<td></td>
<td>If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the <strong>Log Source Identifier</strong> value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the <strong>Log Source Identifier</strong> value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td><strong>Database Type</strong></td>
<td>Oracle</td>
</tr>
<tr>
<td><strong>Database Name</strong></td>
<td>The name of the Oracle Audit Vault database.</td>
</tr>
<tr>
<td><strong>IP or Hostname</strong></td>
<td>The IP address or host name of the Oracle Audit Vault server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port from where the Oracle Audit Vault database is listening.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Any user with the AV_AUDITOR permission. For example, AVAUDITOR.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for the database user.</td>
</tr>
<tr>
<td><strong>Predefined Query</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Table Name</strong></td>
<td>For Oracle Audit Vault Version 10.3, the <strong>Table Name</strong> value is AVSYS.AV$ALERT_STORE.</td>
</tr>
<tr>
<td></td>
<td>For Oracle Audit Vault Version 12.2, the <strong>Table Name</strong> value is AVSYS.AV_ALERT_STORE_V.</td>
</tr>
<tr>
<td><strong>Select List</strong></td>
<td>The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the <strong>Compare Field</strong>.</td>
</tr>
<tr>
<td><strong>Compare Field</strong></td>
<td>For Oracle Audit Vault Version 10.3, the <strong>Compare Field</strong> value is ALERT_SEQUENCE</td>
</tr>
<tr>
<td></td>
<td>For Oracle Audit Vault Version 12.2, the <strong>Compare Field</strong> value is RECORD_ID.</td>
</tr>
<tr>
<td><strong>Use Prepared Statements</strong></td>
<td>You must select the <strong>Use Prepared Statements</strong> option.</td>
</tr>
<tr>
<td><strong>Start Date and Time</strong></td>
<td>The initial date and time for the JDBC retrieval.</td>
</tr>
</tbody>
</table>
Table 491. Oracle Audit Vault JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Oracle Encryption</td>
<td>Oracle Encryption and Data Integrity settings is also known as Oracle Advanced Security. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC protocol parameters, see c_logsource_JDBCprotocol.dita.

4. Verify that QRadar is configured correctly.

The following table shows a sample parsed audit event message from Oracle Audit Vault:

Table 492. Oracle Audit Vault sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGON-success</td>
<td>3075</td>
<td>ALERT_SEQUENCE: &quot;25&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AW_ALERT_TIME: &quot;2010-01-11 13:02:13.30702&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACTUAL_ALERT_TIME: &quot;2010-01-11 12:19:36.0&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TIME_CLEARED: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALERT_NAME: &quot;testing2&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TARGET_OWNER: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TARGET_OBJECT: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSOCIATED_OBJECT_OWNER: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSOCIATED_OBJECT_NAME: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALERT_SEVERITY: &quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLIENT_HOST: &quot;host.domain.lab&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLIENT_HOSTIP: &quot;&lt;client_host_IP_address&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOURCE_HOST: &quot;&lt;source_host_IP_address&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOURCE_HOSTIP: &quot;&lt;source_host_IP_address&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PROCESS#: &quot;3428&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSUSER_NAME: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>USERNAME: &quot;&lt;os_user_name&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INSTANCE_NAME: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INSTANCE_NUMBER: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVENT_STATUS: &quot;0&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONTEXTID: &quot;1561&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUB_CONTEXTID: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PARENT_CONTEXTID: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOURCE_NAME: &quot;XE&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RECORD_ID: &quot;23968&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSG_NUMBER: &quot;0&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CAT_ID: &quot;2&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVENT_ID: &quot;95&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSG_ARG_1: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSG_ARG2: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSG_ARG3: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSG_ARG4: &quot;null&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSG_ARG5: &quot;null&quot;</td>
</tr>
</tbody>
</table>

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Oracle Audit Vault to communicate with QRadar” on page 897
If you are using Oracle Audit Vault V12.2, you must create a database view. If you are using Oracle Audit Vault V10.3, no further configuration is required.

**Configuring Oracle Audit Vault to communicate with QRadar**

If you are using OracleAudit Vault V12.2, you must create a database view. If you are using Oracle Audit Vault V10.3, no further configuration is required.

**Procedure**

1. Log in to your Oracle Audit Vault V12.2 database as the AVSYS user.

2. To create the database view, type the following query:

   ```sql
   create or replace view AVSYS.AV_ALERT_STORE_V as select RECORD_ID,
   USER_NAME, SECURED_TARGET_ID, SECURED_TARGET_NAME, SECURED_TARGET_TYPE,
   EVENT_TIME, OSUSER_NAME, COMMAND_CLASS,
   nvl(to_number(decode(EVENT_STATUS,'SUCCESS','0','FAILURE','1','1')),'1'),
   EVENT_STATUS, EVENT_NAME, EVENT_ID,
   nvl(ERROR_CODE,0) ERROR_CODE,
   ERROR_MESSAGE, AV_TIME, TARGET_TYPE, TARGET_OBJECT, TARGET_OWNER,
   CLIENT_HOST_NAME, CLIENT_IP, AUDIT_TRAIL_ID, MONITORING_POINT_ID, MARKER,
   ALERT_RAISED, ACTION_TAKEN, NETWORK_CONNECTION, LOGFILE_ID, SERVICE_NAME,
   POLICY_NAME, THREAT_SEVERITY, LOG_CAUSE, CLUSTER_ID, CLUSTER_TYPE,
   GRAMMAR_VERSION, CLIENT_PROGRAM, COMMAND_TEXT, COMMAND_PARAM, EXTENSION,
   SECURED_TARGET_CLASS, LOCATION, TERMINAL, CLIENT_ID from avsys.EVENT_LOG el
   where el.alert_raised = 1;
   ```

3. To allow a user that has AV_AUDITOR permission to read the view that you created, type the following query:

   ```sql
   grant select on AVSYS.AV_ALERT_STORE_V to AV_AUDITOR;
   ```

---

**Oracle BEA WebLogic**

The Oracle BEA WebLogic DSM allows IBM QRadar to retrieve archived server logs and audit logs from any remote host, such as your Oracle BEA WebLogic server.

**About this task**

QRadar uses the log file protocol to retrieve events from your Oracle BEA WebLogic server and provides information on application events that occur in your domain or on a single server.

To integrate Oracle BEA WebLogic events, take the following steps:

1. Enable auditing on your Oracle BEA WebLogic server.

2. Configure domain logging on your Oracle BEA WebLogic server.

3. Configure application logging on your Oracle BEA WebLogic server.

4. Configure an audit provider for Oracle BEA WebLogic.

5. Configure QRadar to retrieve log files from Oracle BEA WebLogic.

**Enabling event logs**

By default, Oracle BEA WebLogic does not enable event logging.

**About this task**

To enable event logging on your Oracle WebLogic console:

**Procedure**

1. Log in to your Oracle WebLogic console user interface.
2. Select **Domain > Configuration > General**.
3. Click **Advanced**.
4. From the **Configuration Audit Type** list, select **Change Log and Audit**.
5. Click **Save**.

**What to do next**
You can now configure the collection of domain logs for Oracle BEA WebLogic.

**Configuring domain logging**
Oracle BEA WebLogic supports multiple instances. Event messages from instances are collected in a single domain-wide log for the Oracle BEA WebLogic server.

**About this task**
To configure the log file for the domain:

**Procedure**
1. From your Oracle WebLogic console, select **Domain > Configuration > Logging**.
2. From the **Log file name** parameter, type the directory path and file name for the domain log.
   
   For example, `OracleDomain.log`.
3. Optional: Configure any additional domain log file rotation parameters.
4. Click **Save**.

**What to do next**
You can now configure **application logging** for the server.

**Configuring application logging**
You can configure application logging for Oracle BEA WebLogic:

**Procedure**
1. From your Oracle WebLogic console, select **Server > Logging > General**.
2. From the **Log file name** parameter, type the directory path and file name for the application log.
   
   For example, `OracleDomain.log`.
3. Optional: Configure any additional application log file rotation parameters.
4. Click **Save**.

**What to do next**
You can now configure an audit provider for Oracle BEA WebLogic.

**Configuring an audit provider**
You can configure an audit provider:

**Procedure**
1. Select **Security Realms > Realm Name > Providers > Auditing**.
2. Click **New**.
3. Configure an audit provider by typing a name for the audit provider that you are creating.
4. From the **Type** list, select **DefaultAuditor**.
5. Click **OK**.

   The **Settings** window is displayed.
6. Click the auditing provider that you created in “Configuring an audit provider” on page 898.
7. Click the Provider Specific tab.
8. Add any Active Context Handler Entries that are needed.
9. From the Severity list, select Information.
10. Click Save.

What to do next
You can now configure IBM QRadar to pull log files from Oracle BEA WebLogic.

Configuring a log source
You can configure IBM QRadar to retrieve log files from Oracle BEA WebLogic.

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. From the Log Source Type list, select Oracle BEA WebLogic.
7. Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source. This value must match the value that is configured in the Remote Host IP or Hostname parameter. The log source identifier must be unique for the log source type.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the list, select the File Transfer Protocol (FTP) you want to use for retrieving files. You can choose: SSH File Transfer Protocol (SFTP), File Transfer Protocol (FTP), or Secure Copy (SCP). The default is SFTP.</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>Type the IP address or host name of the host from which you want to receive files.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>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.</td>
</tr>
<tr>
<td>Remote User</td>
<td>Type the user name necessary to log in to the host that runs the selected Service Type. The user name can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Type the password necessary to log in to the host that runs the selected Service Type.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the <strong>Remote Password</strong> to log in to the host that runs the selected <strong>Service Type</strong>.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>If you select <strong>SCP</strong> or <strong>SFTP</strong> as the <strong>Service Type</strong>, this parameter gives the option to define an SSH private key file. Also, when you provide an SSH Key File, the <strong>Remote Password</strong> option is ignored.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>Type the directory location on the remote host from which the files are retrieved.</td>
</tr>
<tr>
<td>Recursive</td>
<td>Select this check box if you want the file pattern to also search sub folders. The <strong>Recursive</strong> parameter is not used if you configure <strong>SCP</strong> as the <strong>Service Type</strong>. By default, the check box is clear.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>If you select <strong>SFTP</strong> or <strong>FTP</strong> as the <strong>Service Type</strong>, this gives the option to configure the regular expression (regex) that is needed to filter the list of files that are specified in the <strong>Remote Directory</strong>. All matching files are included in the processing. For example, if you want to list all files that start with the word server, followed by one or more digits and ending with <code>.log</code>, use the following entry: <code>server[0-9]+\..log</code>. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: <a href="http://docs.oracle.com/javase/tutorial/essential/regex/">http://docs.oracle.com/javase/tutorial/essential/regex/</a></td>
</tr>
</tbody>
</table>
| FTP Transfer Mode        | This option appears only if you select **FTP** as the **Service Type**. The **FTP Transfer Mode** parameter gives the option to define the file transfer mode when log files are retrieved over FTP. From the list, select the transfer mode that you want to apply to this log source:  
  - **Binary** - Select a binary FTP transfer mode for log sources that require binary data files or compressed `.zip`, `.gzip`, `.tar`, or `.tar+gz` archive files.  
  - **ASCII** - Select **ASCII** for log sources that require an ASCII FTP file transfer. You must select **None** for the Processor parameter and **LineByLine** the **Event Generator** parameter when you use ASCII as the FTP 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. |
| 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. |
Table 493. Log file parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run On Save</td>
<td>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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.</td>
</tr>
<tr>
<td>Processor</td>
<td>If the files on the remote host are stored in a .zip, .gzip, .tar, or .tar.gz archive format, select the processor that allows the archives to be expanded and contents that are processed.</td>
</tr>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>Select this check box to track files that are already processed and you do not want these files to be processed a second time. This applies only to FTP and SFTP Service Types.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>Select this check box to define the local directory on your QRadar system that you want to use for storing downloaded files during processing. It is suggested that you leave the check box clear. When the check box is selected, the Local Directory field is displayed, and this gives you the option to configure the local directory for storing files.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the Event Generator list, select Oracle BEA WebLogic.</td>
</tr>
</tbody>
</table>

8. Click Save.

The configuration is complete.

Oracle DB Audit

The IBM QRadar DSM for Oracle DB Audit collects logs from an Oracle database.

The following table describes the specifications for the Oracle DB Audit DSM:

Table 494. Oracle DB Audit DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Oracle</td>
</tr>
<tr>
<td>DSM name</td>
<td>Oracle DB Audit</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-OracleDbAudit-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>9i, 10g, 11g, 12c (includes unified auditing)</td>
</tr>
<tr>
<td>Protocol</td>
<td>JDBC, Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Name-Value Pair</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit records</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 494. Oracle DB Audit DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Oracle website (<a href="https://www.oracle.com">https://www.oracle.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Oracle DB Audit 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:
   - Protocol JDBC RPM
   - DSMCommon RPM
   - Oracle DB Audit DSM RPM

2. Configure your Oracle DB Audit device to write audit logs.

3. If QRadar does not automatically detect the log source, add an Oracle DB Audit log source on the QRadar Console. The following tables describe the parameters that require specific values to collect audit events from Oracle DB Audit:

Table 495. Oracle DB Audit Syslog log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Oracle RDBMS Audit Record</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>

Table 496. Oracle DB Audit JDBC log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Oracle RDBMS Audit Record</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>Oracle</td>
</tr>
<tr>
<td>Database Name</td>
<td>The name of the database from where you collect audit logs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP or host name of the Oracle database.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are:</td>
</tr>
<tr>
<td></td>
<td>• MSDE - 1433</td>
</tr>
<tr>
<td></td>
<td>• Postgres - 5432</td>
</tr>
<tr>
<td></td>
<td>• MySQL - 3306</td>
</tr>
<tr>
<td></td>
<td>• Sybase - 1521</td>
</tr>
<tr>
<td></td>
<td>• Oracle - 1521</td>
</tr>
<tr>
<td></td>
<td>• Informix - 9088</td>
</tr>
<tr>
<td></td>
<td>• DB2 - 50000</td>
</tr>
<tr>
<td></td>
<td>If a database instance is used with the MSDE database type, you must leave the Port field blank.</td>
</tr>
<tr>
<td>Username</td>
<td>A user account to connect to the database. The user must have AUDIT_ADMIN or AUDIT_VIEWER permissions.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is required to connect to the database.</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the none option.</td>
</tr>
<tr>
<td>Table Name</td>
<td>The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td>Select List</td>
<td>The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the Compare Field.</td>
</tr>
<tr>
<td>Compare Field</td>
<td>For Oracle 9i or Oracle 10g Release 1, type Qradar_time.</td>
</tr>
<tr>
<td></td>
<td>For Oracle 10g Release 2, Oracle 11g, or Oracle 12c (non-unified auditing), type extended_timestamp.</td>
</tr>
<tr>
<td></td>
<td>For Oracle 12c (unified auditing), type event_timestamp.</td>
</tr>
</tbody>
</table>
Table 496. Oracle DB Audit JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Oracle Encryption</td>
<td>Oracle Encryption and Data Integrity settings is also known as Oracle Advanced Security. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC parameters, see `c_logsource_JDBCprotocol.dita`

4. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Oracle Db Audit:

**Table 497. Oracle Db Audit sample message**

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| SELECT succeeded    | System Action Allow | **OS_USERNAME**: "os_username" **USERNAME**: "username" **USERHOST**: "userhost" **TERMINAL**: "terminal" **TIMESTAMP**: "2017-04-05 21:04:02.0" **OWNER**: "owner" **OBJ_NAME**: "PARTIAL_ALERT" **ACTION**: "3" **ACTION_NAME**: "SELECT" **NEW_OWNER**: "null" **NEW_NAME**: "null" **OBJ_PRIVILEGE**: "null" **SYS_PRIVILEGE**: "null" **ADMIN_OPTION**: "null" **GRANTEE**: "null" **AUDIT_OPTION**: "null" **SES_ACTIONS**: "null" **LOGOFF_TIME**: "null" **LOGOFF_READ**: "null" **LOGOFF_WRITE**: "null" **LOGOFF_DLOCK**: "null" **COMMENT_TEXT**: "null" **SESSIONID**: "xxxxxx" **ENTRYID**: "2" **STATEMENTID**: "2" **RETCODE**: "0" **PRIV_USED**: "null" **CLIENT_ID**: "null" **ECONTEXT_ID**: "null" **SESSION_CPU**: "null" **EXTENDED_TIMESTAMP**: "2017-04-05 21:04:02.318133 America/Halifax" **PROXY_SESSIONID**: "null" **GLOBAL_UID**: "null" **INSTANCE_NUMBER**: "0" **OS_PROCESS**: "9276" **TRANSACTIONID**: "null" **SCN**: "3842851" **SQL_BIND**: "null" **SQL_TEXT**: "null" **OBJ_EDITION_NAME**: "null" **DBID**: "xxxxxxxxxx"
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Enabling Unified Auditing in Oracle 12c**

To enable Unified Auditing in Oracle 12c, you must shut down the Oracle database, stop the Oracle listener service and then restart the Oracle database and Oracle Listener service.

**Before you begin**

You must have the AUDIT_SYSTEM system privilege or the AUDIT_ADMIN role to complete the following steps.

**Procedure**

1. Shut down the Oracle database by connecting to the database with SQLplus, and then type the following command:
   
   shutdown immediate

2. Stop the Oracle listener service by typing the following command:

   lsnrctl stop

3. If applicable, stop the Enterprise Manager by typing the following commands:
   
   cd /u01/app/oracle/product/middleware/oms
   export OMS_HOME=/u01/app/oracle/product/middleware/oms
   $OMS_HOME/bin/emctl stop oms

4. Relink Oracle DB with the uniaud option by typing the following commands:
   
   cd $ORACLE_HOME/rdbms/lib
   make -f ins_rdbms.mk uniaud_on ioracle

5. Restart the Oracle database by connecting to the database with SQLplus, and then type the following command:

   startup

6. Restart the Oracle listener service by typing the following command:

   lsnrctl start

7. If applicable, restart the Enterprise Manager by typing the following commands:

   cd /u01/app/oracle/product/middleware/oms
   export OMS_HOME=/u01/app/oracle/product/middleware/oms
   $OMS_HOME/bin/emctl start oms

8. To verify that unified auditing is enabled, connect to the Oracle database with SQLplus, and then type the following command:

   select * from v$option where PARAMETER = 'Unified Auditing';

   Verify that the command returns one row with **VALUE equal to "TRUE"**.

**Configuring an Oracle database server to send syslog audit logs to QRadar**

Configure your Oracle device to send syslog audit logs to IBM QRadar.

**Procedure**

1. Log in to the Oracle host as an Oracle user.

2. Ensure that the **ORACLE_HOME** and **ORACLE_SID** environment variables are configured properly for your deployment.

3. Open the following file:
4. Choose one of the following options:
   a) For database audit trails, type the following command:
      
      ```
      *.audit_trail='DB'
      ```
   
b) For syslog, type the following commands:
      
      ```
      *.audit_trail='os'
      *.audit_syslog_level='local0.info'
      ```
      You must ensure that the syslog daemon on the Oracle host is configured to forward the audit log to QRadar. For systems that run Red Hat Enterprise, the following line in the `/etc/syslog.conf` file affects the forwarding:
      
      ```
      local0.info @ qradar.domain.tld
      ```
      Where `qradar.domain.tld` is the host name of QRadar that receives the events. The syslog configuration must be reloaded for the command to be recognized. On a system that runs Red Hat Enterprise, type the following line to reload the syslog configuration:
      
      ```
      kill -HUP /var/run/syslogd.pid
      ```
      
5. Save and exit the file.
6. To restart the database, connect to SQLplus and log in as sysdba:

   **Example:** Enter `user-name: sys as sysdba`

7. Shut down the database by typing the following line:

   ```
   shutdown immediate
   ```
8. Restart the database by typing the following line:

   ```
   startup
   ```
9. If you are using Oracle v9i or Oracle v10g Release 1, you must create a view that uses SQLplus to enable the QRadar integration. If you are using Oracle 10g Release 2 or later, you can skip this step:

   ```
   CREATE VIEW qradar_audit_view
   AS SELECT CAST(dba_audit_trail.timestamp AS TIMESTAMP)
   AS qradar_time, dba_audit_trail.* FROM dba_audit_trail;
   ```

   If you are using the JDBC protocol, when you configure the JDBC protocol within QRadar, use the following specific parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Oracle v9i or 10g Release 1 Values</th>
<th>Oracle v10g Release 2 and v11g Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table Name</td>
<td>QRadar_audit_view</td>
<td>dba_audit_trail</td>
</tr>
<tr>
<td>Select List</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Compare Field</td>
<td>QRadar_time</td>
<td>extended_timestamp</td>
</tr>
<tr>
<td>Database Name</td>
<td>For all supported versions of Oracle, the Database Name must be the exact service name that is used by the Oracle listener. You can view the available service names by running the following command on the Oracle host: <code>lsnrctl status</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Ensure that the database user that QRadar uses to query events from the audit log table has the appropriate permissions for the Table Name object.
10. You can now configure QRadar to receive events from an Oracle database: From the Log Source Type list, select the Oracle RDBMS Audit Record option.

**Related tasks**

“Adding a log source” on page 4

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

**Oracle DB Listener**

The Oracle Database Listener application stores logs on the database server.

To integrate IBM QRadar with Oracle DB Listener, select one of the following methods for event collection:

- “Collecting events by using the Oracle Database Listener Protocol” on page 908
- “Collecting Oracle database events by using Perl ” on page 910

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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 events by using the Oracle Database Listener Protocol**

The Oracle Database Listener protocol source allows IBM QRadar to monitor log files that are generated from an Oracle Listener database. Before you configure the Oracle Database Listener protocol to monitor log files for processing, you must obtain the directory path to the Oracle Listener database log files.

**Before you begin**

Samba services must be running on the destination server to properly retrieve events when using the Oracle Database Listener protocol.

**About this task**

To configure QRadar to monitor log files from Oracle Database Listener:

**Procedure**

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   
   The Log Sources window is displayed.
5. From the Log Source Type list, select Oracle Database Listener.
6. Using the Protocol Configuration list, select Oracle Database Listener.
7. Configure the following parameters:

<table>
<thead>
<tr>
<th>Table 499. Oracle Database Listener parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Server Address</td>
</tr>
<tr>
<td>Domain</td>
</tr>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Confirm Password</td>
</tr>
<tr>
<td>Log Folder Path</td>
</tr>
</tbody>
</table>
| File Pattern            | Type the regular expression (regex) that is needed to filter the file names. All matching files are included in the processing. The default is listener\.log  
This parameter does not accept wildcard or globbing patterns in the regular expression. For example, if you want to list all files that start with the word log, followed by one or more digits and ending with tar.gz, use the following entry: log[0-9]+\.tar\.gz. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://docs.oracle.com/javase/tutorial/essential/regex/ |
| Force File Read         | Select this check box to force the protocol to read the log file when the timing of the polling interval specifies.                     |
|                         | When the check box is selected, the log file source is always examined when the polling interval specifies, regardless of the last modified time or file size attribute. |
|                         | When the check box is not selected, the log file source is examined at the polling interval if the last modified time or file size attributes changed. |
| Recursive               | Select this check box if you want the file pattern to also search sub folders. By default, the check box is selected.                  |
| Polling Interval (in seconds) | Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The minimum polling interval is 10 seconds, with a maximum polling interval of 3,600 seconds. The default is 10 seconds. |
| Throttle Events/Sec     | Type the maximum number of events the Oracle Database Listener protocol forwards per second. The minimum value is 100 EPS and the maximum is 20,000 EPS. The default is 100 EPS. |

8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.
Collecting Oracle database events by using Perl

The Oracle Database Listener application stores logs on the database server. To forward these logs from the Oracle server to IBM QRadar, you must configure a Perl script on the Oracle server. The Perl script monitors the listener log file, combines any multi-line log entries into a single log entry, and sends the logs, by using syslog (UDP), to QRadar.

About this task

Before the logs are sent to QRadar, they are processed and reformatted so that they are not forwarded line-by-line, as they are in the log file. All of the relevant information is retained.

Note: Perl scripts that are written for Oracle DB listener work on Linux/UNIX servers only. Windows Perl script is not supported. You must make sure Perl 5.8 is installed on the device that hosts the Oracle server.

To install and configure the Perl script:

Procedure

1. Go to the following website to download the files that you need:
   http://www.ibm.com/support
2. From the Downloads list, click Fix Central.
3. Click Select product tab.
4. Select IBM Security from the Product Group list.
5. Select IBM Security QRadar SIEM from the Select from IBM Security list.
7. Select Linux from the Platform list and click Continue.
8. Select Browse for fixes and click Continue.
9. Select Script.
10. Click `<QRadar_version>-oracle_dblistener_fwdr-<version_number>.pl.tar.gz` to download the Oracle DB Listener Script.
11. Copy the Oracle DB Listener Script to the server that hosts the Oracle server.
12. Log in to the Oracle server by using an account that has read/write permissions for the listener.log file and the /var/run directory.
13. Extract the Oracle DB Listener Script file by typing the following command:
   ```
tar -xvzf oracle_dblistener_fwdr-<version_number>.pl.tar.gz
```
14. Type the following command and include any additional command parameters to start monitoring the Oracle DB Listener log file:
   ```
oracle_dblistener_fwdr.pl -h `<IP address>` -t "tail -F <absolute_path_to_listener_log>/listener.log"
   ```
   where `<IP address>` is the IP address of your QRadar Console or Event Collector, and `<absolute_path_to_listener_log>` is the absolute path of the listener log file on the Oracle server.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-D</code></td>
<td>The <code>-D</code> parameter defines that the script is to run in the foreground. Default is to run as a daemon and log all internal messages to the local syslog service.</td>
</tr>
</tbody>
</table>
# Table 500. Command parameters (continued)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t</td>
<td>The <code>-t</code> parameter defines that the command-line is used to tail the log file (monitors any new output from the listener). The location of the log file might be different across versions of the Oracle database. For examples, Oracle 9i: <code>&lt;install_directory&gt;/product/9.2/network/log/listener.log</code> Oracle 10g: <code>&lt;install_directory&gt;/product/10.2.0/db_1/network/log/listener.log</code> Oracle 11g: <code>&lt;install_directory&gt;/diag/tnslsnr/qaoracle11/listener/trace/listener.log</code></td>
</tr>
<tr>
<td>-f</td>
<td>The <code>-f</code> parameter defines the <strong>syslog facility.priority</strong> to be included at the beginning of the log. If nothing is specified, <code>user.info</code> is used.</td>
</tr>
<tr>
<td>-g</td>
<td>The <code>-g</code> parameter defines the language pack file. For example, <code>./oracle_dblistener_fwdr.pl -h &lt;IP_address&gt; -g /root/OracleDBListener/languagepacks/localization.french -t &quot;tail -f /root/smbtest/listener_vali.log&quot;</code> This parameter is optional.</td>
</tr>
<tr>
<td>-H</td>
<td>The <code>-H</code> parameter defines the host name or IP address for the syslog header. It is suggested that is the IP address of the Oracle server on which the script is running.</td>
</tr>
<tr>
<td>-h</td>
<td>The <code>-h</code> parameter defines the receiving syslog host (the Event Collector host name or IP address that is used to receive the logs).</td>
</tr>
<tr>
<td>-p</td>
<td>The <code>-p</code> parameter defines the receiving UDP syslog port. If a port is not specified, 514 is used.</td>
</tr>
<tr>
<td>-r</td>
<td>The <code>-r</code> parameter defines the directory name where you want to create the .pid file. The default is <code>/var/run</code>. This parameter is ignored if <code>-D</code> is specified.</td>
</tr>
<tr>
<td>-l</td>
<td>The <code>-l</code> parameter defines the directory name where you want to create the lock file. The default is <code>/var/lock</code>. This parameter is ignored if <code>-D</code> is specified.</td>
</tr>
</tbody>
</table>

For example, to monitor the listener log on an Oracle 9i server with an IP address of 192.0.2.10 and forward events to QRadar with the IP address of 192.0.2.20, type the following code:

`oracle_dblistener_fwdr.pl -t tail -f <install_directory>/product/9.2/network/log/listener.log -f user.info -H 192.0.2.10 -h 192.0.2.20 -p 514`

A sample log from this setup would appear as follows:

```markdown
<14>Apr 14 13:23:37 192.0.2.10 AgentDevice=OracleDBListener Command=SERVICE_UPDATE DeviceTime=18-AUG-2006 16:51:43 Status=0 SID=qora9
```

**Note:** The **kill** command can be used to stop the script if you need to reconfigure a script parameter or stop the script from sending events to QRadar. For example, `kill -QUIT `cat /var/run/oracle_dblistener_fwdr.pl.pid`
The example command uses the backquote character (``), which is located to the left of the number one on most keyboard layouts.

**What to do next**
You can now configure the Oracle Database Listener within QRadar.

**Configuring the Oracle Database Listener within QRadar.**
You can configure the Oracle Database Listener within IBM QRadar.

**Procedure**
1. From the Log Source Type list, select Oracle Database Listener.
2. From the Protocol Configuration list, select syslog.
3. In the Log Source Identifier field, type the IP address of the Oracle Database you specified using the -H option in “Collecting Oracle database events by using Perl ” on page 910.
   The configuration of the Oracle Database Listener protocol is complete. For more information on Oracle Database Listener, see your vendor documentation.

**Oracle Directory Server overview**
Oracle Directory Server is formerly known as Sun ONE LDAP.

**Related concepts**
“Sun ONE LDAP” on page 1059

**Oracle Enterprise Manager**
The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Oracle</td>
</tr>
<tr>
<td>DSM name</td>
<td>Oracle Enterprise Manager</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-OracleEnterpriseManager-QRadar_version-Buildbuild_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>Oracle Enterprise Manager Cloud Control 12c</td>
</tr>
<tr>
<td>Protocol</td>
<td>JDBC</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>(Optional) Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source type</td>
<td>Oracle Enterprise Manager</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Database Type</td>
<td>Oracle</td>
</tr>
<tr>
<td>Database Name</td>
<td>The Service Name of Oracle Enterprise Manager database.</td>
</tr>
<tr>
<td></td>
<td>To view the available service names, run the lsnrctl status command on the Oracle host.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name of the Oracle Enterprise Manager database server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that is used by the Oracle Enterprise Manager database.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name of the account that has rights to access the sysman.mgmt$ccc_all_observations table.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is required to connect to the database.</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>(Optional) none</td>
</tr>
<tr>
<td>Table Name</td>
<td>sysman.mgmt$ccc_all_observations</td>
</tr>
<tr>
<td>Select List</td>
<td>*</td>
</tr>
</tbody>
</table>

Table 502. Oracle Enterprise Manager JDBC log source parameters
### Table 502. Oracle Enterprise Manager JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Compare Field</strong></td>
<td>ACTION_TIME</td>
</tr>
<tr>
<td><strong>Use Prepared Statements</strong></td>
<td>True</td>
</tr>
<tr>
<td><strong>Start Date and Time</strong> (Optional)</td>
<td>Type the start date and time for database polling in the following format: 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.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value. The maximum polling interval is one week.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000.</td>
</tr>
<tr>
<td><strong>Use Oracle Encryption</strong></td>
<td>Oracle Encryption and Data Integrity settings is also known as Oracle Advanced Security. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC parameters, see `c_logsourc_JDBCprotocol.dita`

**Related tasks**

Adding a DSM

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.

“Adding a DSM” on page 4

“Adding a log source” on page 4

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

---

### Oracle Fine Grained Auditing

The Oracle Fine Grained Auditing DSM can poll for database audit events from Oracle 9i and later by using the Java Database Connectivity (JDBC) protocol.

To collect events, administrators must enable fine grained auditing on their Oracle databases. Fine grained auditing provides events on select, update, delete, and insert actions that occur in the source database and the records that the data changed. The database table `dba_fga_audit_trail` is updated with a new row each time a change occurs on a database table where the administrator enabled an audit policy.

To configure Oracle fine grained auditing, administrators can complete the following tasks:

1. Configure on audit on any tables that require policy monitoring in the Oracle database.
2. Configure a log source for the Oracle Fine Grained Auditing DSM to poll the Oracle database for events.
3. Verify that the events polled are collected and displayed on the Log Activity tab of IBM QRadar.

**Configuring a log source in QRadar to collect events from Oracle Fine Grained Auditing**

After the database administrator has configured database policies, you can configure a log source to access the Oracle database with the JDBC protocol.

**Procedure**

1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.
5. Configure the parameters:

<table>
<thead>
<tr>
<th>Table 503. Oracle Fine Grained Auditing JDBC parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Database Type</td>
</tr>
<tr>
<td>Database Name</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>IP or Hostname</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
</tbody>
</table>
| Port            | Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535.  
                      The defaults are:  
                      • MSDE - 1433  
                      • Postgres - 5432  
                      • MySQL - 3306  
                      • Sybase - 1521  
                      • Oracle - 1521  
                      • Informix - 9088  
                      • DB2 - 50000  
                      If a database instance is used with the MSDE database type, you must leave the **Port** field blank. |
| Username        | A user account for QRadar in the database.  
                      The user name can be up to 255 alphanumeric characters in length. The user name can also include underscores (_). |
| Password        | Type the database password that is required to connect to the database.  
                      The password can be up to 255 characters in length. |
| Confirm Password| Confirm the password to connect to the database. |
| Predefined Query| From the list, select **None**. |
| Table Name      | Type dba_fga_audit_trail as the name of the table that includes the event records. If you change the value of this field from the default, events cannot be properly collected by the JDBC protocol. |
| Select List     | Type * to include all fields from the table or view.  
                      You can use a comma-separated list to define specific fields from tables or views, if this is needed for your configuration. The list must contain the field that is defined in the **Compare Field** parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.). |
| Compare Field   | Type extended_timestamp to identify new events added between queries to the table by their time stamp. |
Table 503. Oracle Fine Grained Auditing JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Prepared Statements</td>
<td>Select the <strong>Use Prepared Statements</strong> check box. Prepared statements allow the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>Optional. Configure the start date and time for database polling.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Type the polling interval in seconds, which is the amount of time between queries to the database table. The default polling interval is 30 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 without an H or M designator poll in seconds.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td>Use Oracle Encryption</td>
<td><strong>Oracle Encryption and Data Integrity settings</strong> is also known as <strong>Oracle Advanced Security</strong>. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.</td>
</tr>
</tbody>
</table>

6. Click **Save**.
7. On the **Admin** tab, click **Deploy Changes**.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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

**Oracle OS Audit**

The Oracle OS Audit DSM for IBM QRadar allows monitoring of the audit records that are stored in the local operating system file.

**About this task**

When audit event files are created or updated in the local operating system directory, a Perl script detects the change, and forwards the data to QRadar. The Perl script monitors the Audit log file, and combines any multi-line log entries into a single log entry to make sure that the logs are not forwarded line-by-line, because this is the format in the log file. Then, the logs are sent by using syslog to QRadar. Perl scripts that are written for Oracle OS Audit work on Linux/UNIX servers only. Windows based Perl installations are not supported.

To integrate the Oracle OS Audit DSM with QRadar:
Procedure

1. Go to the following websites to download the files that you need:
2. From the **Software** tab, select **Scripts**.
3. Download the Oracle OS Audit script:
   `oracle_osauditlog_fwdr_5.3.tar.gz`
4. Type the following command to extract the file:
   `tar -zxvf oracle_osauditlog_fwdr_5.3.tar.gz`
5. Copy the Perl script to the server that hosts the Oracle server.
6. Log in to the Oracle host as an Oracle user that has SYS or root privilege.
7. Make sure the **ORACLE_HOME** and **ORACLE_SID** environment variables are configured properly for your deployment.
8. Open the following file:
   `$ORACLE_HOME/dbs/init$ORACLE_SID.ora`
9. For syslog, add the following lines to the file:
   `*.audit_trail=os *.audit_syslog_level=local0.info`
10. Verify account has read/write permissions for the following directory:
    `/var/lock/ /var/run/`
11. Restart the Oracle database instance.
12. Start the OS Audit DSM script:
    `oracle_osauditlog_fwdr_5.3.pl -t target_host -d logs_directory`

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-t</code></td>
<td>The <code>-t</code> parameter defines the remote host that receives the audit log files.</td>
</tr>
</tbody>
</table>
| `-d`       | The `-d` parameter defines directory location of the DDL and DML log files.  
The directory location that you specify should be the absolute path from the root directory. |
| `-H`       | The `-H` parameter defines the host name or IP address for the syslog header. It is suggested that is the IP address of the Oracle server on which the script is running. |
| `-D`       | The `-D` parameter defines that the script is to run in the foreground.  
Default is to run as a daemon (in the background) and log all internal messages to the local syslog service. |
| `-n`       | The `-n` parameter processes new logs, and monitors existing log files for changes to be processed.  
If the `-n` option string is absent all existing log files are processed during script execution. |
| `-u`       | The `-u` parameter defines UDP. |
### Table 504. Oracle OS Audit command parameters (continued)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
</table>
| -f         | The `-f` parameter defines the **syslog facility.priority** to be included at the beginning of the log.  
If you do not type a value, `user.info` is used. |
| -r         | The `-r` parameter defines the directory name where you want to create the `.pid` file.  
The default is `/var/run`. This parameter is ignored if `-D` is specified. |
| -l         | The `-l` parameter defines the directory name where you want to create the lock file.  
The default is `/var/lock`. This parameter is ignored if `-D` is specified. |
| -h         | The `-h` parameter displays the help message. |
| -v         | The `-v` parameter displays the version information for the script. |

If you restart your Oracle server you must restart the script:

```
oracle_osauditlog_fwdr.pl -t target_host -d logs_directory
```

### What to do next

You can now configure the log sources within QRadar.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 the log sources within QRadar for Oracle OS Audit

You can configure the log sources within IBM QRadar.

**Procedure**

1. From the **Log Source Type** list, select **Oracle RDBMS OS Audit Record**.
2. From the **Protocol Configuration** list, select **syslog**.
3. From the **Log Source Identifier** field, type the address that is specified by using the `-H` option in “Oracle OS Audit” on page 917.

   For more information about your Oracle Audit Record, see your vendor documentation.
Chapter 117. OSSEC

The OSSEC DSM for IBM QRadar accepts events that are forwarded from OSSEC installations by using syslog.

OSSEC is an open source Host-based Intrusion Detection System (HIDS) that can provide intrusion events to QRadar. If you have OSSEC agents that are installed, you must configure syslog on the OSSEC management server. If you have local or stand-alone installations of OSSEC, then you must configure syslog on each stand-alone OSSEC to forward syslog events to QRadar.

Configuring OSSEC

You can configure syslog for OSSEC on a stand-alone installation or management server:

Procedure

1. Use SSH to log in to your OSSEC device.
2. Edit the OSSEC configuration ossec.conf file.
   `<installation directory>/ossec/etc/ossec.conf`
3. Add the following syslog configuration:
   
   **Note:** Add the syslog configuration after the alerts entry and before the localfile entry.
   ```
   </alerts>
   <syslog_output> <server>(QRadar IP Address)</server> <port>514</port> </syslog_output>
   <localfile>
   
   For example,
   ```
   <syslog_output> <server><IP_address></server> <port>514</port> </syslog_output>
   <localfile>
```
4. Save the OSSEC configuration file.
5. Type the following command to enable the syslog daemon:
   ```
   <installation directory>/ossec/bin/ossec-control enable client-syslog
   ```
6. Type the following command to restart the syslog daemon:
   ```
   <installation directory>/ossec/bin/ossec-control restart
   ```

The configuration is complete. The log source is added to IBM QRadar as OSSEC events are automatically discovered. Events that are forwarded to QRadar by OSSEC are displayed on the Log Activity tab of QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from OSSEC.

About this task

The following configuration steps are optional.

To manually configure a log source for OSSEC:
Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 OSSEC.
   The syslog protocol configuration is displayed.
10. Configure the following values:
   
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your OSSEC installation.</td>
</tr>
</tbody>
</table>
11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.
Chapter 118. Palo Alto Networks

IBM QRadar supports a range of Palo Alto Network devices.

Palo Alto Endpoint Security Manager

The IBM QRadar DSM for Palo Alto Endpoint Security Manager (Traps) collects events from a Palo Alto Endpoint Security Manager (Traps) device.

The following table describes the specifications for the Palo Alto Endpoint Security Manager DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Palo Alto Networks</td>
</tr>
<tr>
<td>DSM name</td>
<td>Palo Alto Endpoint Security Manager</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-PaloAltoEndpointSecurityManager-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>3.4.2.17401</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Log Event Extended Format (LEEF)</td>
</tr>
<tr>
<td></td>
<td>Common Event Format (CEF)</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td>Config</td>
</tr>
<tr>
<td></td>
<td>Policy</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Threat</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Palo Alto Networks website (<a href="https://www.paloaltonetworks.com">https://www.paloaltonetworks.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Palo Alto Endpoint Security Manager with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs, in the order that they are listed, on your QRadar Console:
   - DSMCommon RPM
   - Palo Alto Endpoint Security Manager DSM RPM
2. Configure your Palo Alto Endpoint Security Manager device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Palo Alto Endpoint Security Manager log source on the QRadar Console. The following table describes the parameters that require specific values for Palo Alto Endpoint Security Manager event collection:
Table 507. Palo Alto Endpoint Security Manager log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Palo Alto Endpoint Security Manager</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>A unique identifier</td>
</tr>
</tbody>
</table>

4. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

The following table shows a sample event message for Palo Alto Endpoint Security Manager:

Table 508. Palo Alto Endpoint Security Manager sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| New Hash Added   | Successful Configuration Modification| LEEF:1.0|Palo Alto Networks|Traps ESM|3.4.2.17401| New Hash Added|cat=Policy subtype=New Hash Added devTimeFormat=
|                  |                                     | MMM dd yyyy HH:mm:ss devTime=Nov 03 2016 18:43:57 fileHash= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx NewVerdict=Benign msg=New hash added sev=6 |

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 Palo Alto Endpoint Security Manager to communicate with QRadar

Before IBM QRadar can collect events from Palo Alto Endpoint Security Manager, you must configure Palo Alto Endpoint Security Manager to send events to QRadar.

Procedure

1. Log in to the Endpoint Security Manager (ESM) Console.
2. Click **Settings > ESM**.
3. Click **Syslog**, and then select **Enable Syslog**.
4. Configure the syslog parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Server</td>
<td>Host name or IP address of the QRadar server.</td>
</tr>
<tr>
<td>Syslog Port</td>
<td>514</td>
</tr>
<tr>
<td>Syslog Protocol</td>
<td>LEEF</td>
</tr>
<tr>
<td>Keep-alive-timeout</td>
<td>0</td>
</tr>
<tr>
<td>Send reports interval</td>
<td>Frequency (in minutes), in which Traps sends logs from the endpoint. The default is 10. The range is 1 - 2,147,483,647.</td>
</tr>
</tbody>
</table>
Parameter | Value
--- | ---
Syslog Communication Protocol | Transport layer protocol that the ESM Console uses to send syslog reports by using UDP, TCP, or TCP with SSL.

5. In the **Logging Events** area, select the types of events that you want to send to QRadar.

6. Click **Check Connectivity**. The ESM Console sends a test communication to the syslog server by using the information on the **Syslog** page. If the test message is not received, verify that the settings are correct, and then try again.

**Palo Alto Networks PA Series**

Use the IBM QRadar DSM for Palo Alto PA Series to collect events from Palo Alto PA Series devices.

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 from the IBM support website (https://www-945.ibm.com/support/fixcentral).

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 the 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:

   **Table 509. Palo Alto PA Series log source parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the Palo Alto Series device</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>Palo Alto PA Series</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4

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

**Palo Alto PA DSM specifications**

The following table identifies the specifications for the Palo Alto PA Series DSM:

**Table 510. DSM specifications for Palo Alto PA Series**

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Palo Alto Networks</td>
</tr>
<tr>
<td>DSM name</td>
<td>Palo Alto PA Series</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-PaloAltoPaSeries-QRadar_version-&lt;build number&gt;.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>PAN-OS v3.0 to v8.1</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF for PAN-OS v3.0 to v8.1</td>
</tr>
<tr>
<td></td>
<td>CEF for PAN-OS v4.0 to v6.1</td>
</tr>
</tbody>
</table>
**Table 510. DSM specifications for Palo Alto PA Series (continued)**

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRadar recorded log types</td>
<td>Traffic</td>
</tr>
<tr>
<td></td>
<td>Threat</td>
</tr>
<tr>
<td></td>
<td>Config</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>HIP Match</td>
</tr>
<tr>
<td></td>
<td>Data</td>
</tr>
<tr>
<td></td>
<td>WildFire</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Tunnel Inspection</td>
</tr>
<tr>
<td></td>
<td>Correlation</td>
</tr>
<tr>
<td></td>
<td>URL Filtering</td>
</tr>
<tr>
<td></td>
<td>User-ID</td>
</tr>
<tr>
<td></td>
<td>SCTP</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Palo Alto Networks website (<a href="http://www.paloaltonetworks.com">http://www.paloaltonetworks.com</a>)</td>
</tr>
</tbody>
</table>

**Creating a Syslog destination on your Palo Alto PA Series device**

To send Palo Alto PA Series events to IBM QRadar, create a Syslog destination (Syslog or LEEF) 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.
6. Configure LEEF events:

   **Note**: Palo Alto can only send one format to all Syslog devices. By modifying the Syslog format, any other device that requires Syslog will be required to support that same format.

   **Attention**: If you are using Syslog, set the **Custom Format** column to **Default** for all Log Types. If you are using LEEF, use the following substeps:
   a) Click the **Custom Log Format** tab in the **Syslog Server Profile** dialogue.
Important: Due to PDF formatting, do not copy and paste the message formats directly into the PAN-OS web interface. Instead, paste into a text editor, remove any carriage return or line feed characters, and then copy and paste into the web interface.

b) Click **Config**, copy the following text, and paste it in the **Config Log Format** text box for the **Config** log type.

**PAN-OS v3.0 - v6.1**

```
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
```

**PAN-OS v7.1 - v8.0**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$result|configTime=$receive_time|serialNumber=$serial|cat=$type|devTime=$cef-formatted-receive_time|virtualSystem=$vsys|filename=$object|module=$module|sequence=$seqno|actionFlags=$actionflags|beforeChangeDetail=$before-change-detail|afterChangeDetail=$after-change-detail|deviceGroupName1=$dg_hier_level_1|deviceGroupName2=$dg_hier_level_2|deviceGroupName3=$dg_hier_level_3|deviceGroupName4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name
```

c) Click **System**, copy the following text, and paste it in the **System Log Format** text box for the **System** log type.

**PAN-OS v3.0 - v6.1**

```
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
```

**PAN-OS v7.1 - v8.0**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$eventid|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive_time|VirtualSystem=$vsys|Filename=$object|Module=$module|sequence=$seqno|ActionFlags=$actionflags|beforeChangeDetail=$before-change-detail|afterChangeDetail=$after-change-detail|deviceGroupName1=$dg_hier_level_1|deviceGroupName2=$dg_hier_level_2|deviceGroupName3=$dg_hier_level_3|deviceGroupName4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name
```

d) Click **Threat**, copy the following text, and paste it in the **Threat Log Format** text box for the **Threat** log type.

**PAN-OS v3.0 - v6.1**

```
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=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=$flags|proto=$proto|action=$action|Miscellaneous=$misc
```

**PAN-OS v7.1**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$threatid|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|subtype=$subtype|devTime=$cef-formatted-receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|usrName=$srcuser|SourceUser=$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=$flags|proto=$proto|action=$action|Miscellaneous=$misc|URLCategory=$category|Severity=$number-of-severity|Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=$srcloc|DestinationLocation=$dstloc|ContentType=$contenttype|PCAP_ID=$pcap_id|FileDigest=$fileDigest|Cloud=$cloud|URLIndex=$url_idx|UserAgent=$user_agent|FileType=$filetype|identSrc=$xff|Referer=$referer|Sender=$sender|Subject=$subject|Recipient=$recipient|ReportID=$reportid|DeviceGroupName1=$dg_hier_level_1|DeviceGroupName2=$dg_hier_level_2|DeviceGroupName3=$dg_hier_level_3|DeviceGroupName4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name
```

**PAN-OS v8.0**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$threatid|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|subtype=$subtype|devTime=$cef-formatted-receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|usrName=$srcuser|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|SourceZone=$from
```

Chapter 118. Palo Alto Networks 927
e) Click **Traffic**, copy the following text, and paste it in the **Traffic Log Format** text box for the **Traffic log type**.

**PAN-OS v3.0 - v6.1**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$action|cat=$type|src=$src
|dst=$dst|proto=$proto|usn=$username|serialNumber=$serial|logType=$logType
|RuleName=$rule|SourceUser=$username|SourceIP=$sourceIp|destinationIP=$destinationIp
|ActionFlags=$actionFlags|UserDefinedFields=$userDefinedFields
|LogForwardingProfileLogsetId=$logsetId|SessionId=$sessionId
|RepeatCount=$repeatCount|flags=$flags
|totalBytes=$totalBytes|totalPackets=$totalPackets
|startTime=$startTime|sessionStart=$sessionStart
|ActionSource=$actionSource|SourceLocation=$sourceLocation
|DestinationLocation=$destinationLocation
```

**PAN-OS v7.1**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$action|cat=$type|src=$src
|dst=$dst|proto=$proto|usn=$username|serialNumber=$serial|logType=$logType
|RuleName=$rule|SourceUser=$username|SourceIP=$sourceIp|destinationIP=$destinationIp
|ActionFlags=$actionFlags|UserDefinedFields=$userDefinedFields
|LogForwardingProfileLogsetId=$logsetId|SessionId=$sessionId
|RepeatCount=$repeatCount|flags=$flags
|totalBytes=$totalBytes|totalPackets=$totalPackets
|startTime=$startTime|sessionStart=$sessionStart
|ActionSource=$actionSource|SourceLocation=$sourceLocation
|DestinationLocation=$destinationLocation
```

**PAN-OS v8.0**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$action|cat=$type|receiveTime=$receiveTime|serialNumber=$serial|logType=$logType
|RuleName=$rule|SourceUser=$username|SourceIP=$sourceIp|destinationIP=$destinationIp
|ActionFlags=$actionFlags|UserDefinedFields=$userDefinedFields
|LogForwardingProfileLogsetId=$logsetId|SessionId=$sessionId
|RepeatCount=$repeatCount|flags=$flags
|totalBytes=$totalBytes|totalPackets=$totalPackets
|startTime=$startTime|sessionStart=$sessionStart
|ActionSource=$actionSource|SourceLocation=$sourceLocation
|DestinationLocation=$destinationLocation
```

f) Click **HIP Match**, copy the following text, and paste it in the **HIP Match Log Format** text box for the **HIP Match log type**. Omit this step if you are using PAN-OS v3.0 - v6.1.

**PAN-OS v7.1**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$action|cat=$type|receiveTime=$receiveTime|serialNumber=$serial|logType=$logType
|RuleName=$rule|SourceUser=$username|SourceIP=$sourceIp|destinationIP=$destinationIp
|ActionFlags=$actionFlags|UserDefinedFields=$userDefinedFields
|LogForwardingProfileLogsetId=$logsetId|SessionId=$sessionId
|RepeatCount=$repeatCount|flags=$flags
|totalBytes=$totalBytes|totalPackets=$totalPackets
|startTime=$startTime|sessionStart=$sessionStart
|ActionSource=$actionSource|SourceLocation=$sourceLocation
|DestinationLocation=$destinationLocation
```
g) Copy the following text and paste it in the **Custom Format** column for the **URL Filtering** log type.

**PAN-OS v8.0**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$threatid|
ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=cef-formatted-receive-time|usrName=$srcuser|VirtualSystem=$vsys|identHostName=$machine_name|OS=$os|identsrc=$src|
HIP=$matchname|RepeatCount=|sourceName=$src|ActionFlags=|sequence=$seqno|ActionFlags=|
DeviceGroupHierarchy1=$dg_hier_level_1|DeviceGroupHierarchy2=$dg_hier_level_2|DeviceGroupHierarchy3=$dg_hier_level_3|DeviceGroupHierarchy4=$dg_hier_level_4|
srcName=$vsys_name|DeviceName=$device_name|VirtualSystemID=$vsys_id|srcipv6=$srcipv6|
startTime=cef-formatted-time-generated
```

h) Copy the following text and paste it in the **Custom Format** column for the **Data** log type.

**PAN-OS v8.0**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$threatid|
ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=cef-formatted-receive-time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|usrName=$srcuser|
SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|
LogForwardingProfile=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|
srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=$flags|proto=$proto|action=$action|
Miscellaneous=$misc|ThreatID=$threatid|URLCategory=$category|
```

i) Copy the following text and paste it in the **Custom Format** column for the **Wildfire** log type.

**PAN-OS v8.0**

```
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$threatid|
ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=cef-formatted-receive-time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|usrName=$srcuser|
SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|
LogForwardingProfile=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|
srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=$flags|proto=$proto|action=$action|
Miscellaneous=$misc|ThreatID=$threatid|URLCategory=$category|
```

Chapter 118. Palo Alto Networks 929
j) Copy the following text and paste it in the Custom Format column for the Authentication log type.

PAN-OS v8.0

LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$event|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|subtype=$subtype|devtime=$cef-formatted-receive-time|ServerProfile=$serverprofile|LogForwardingProfile=$logset|VirtualSystem=$vsys|AuthPolicy=$authpolicy|ClientType=$clienttype|NormalizeUser=$normalizeuser|ObjectName=$object|FactorNumber=$factor|AuthenticationID=$authhid|src=$ip|RepeatCount=$repeatcnt|usrName=$username|Vendor=$vendor|m=$msg|event=$event|sequence=$sequence|DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|LogSource=$logsource|ActionFlag=$actionflags|AdditionalAuthInfo=$desc|ActionFlags=$actionflags

k) Copy the following text and paste it in the Custom Format column for the User-ID log type.

PAN-OS v8.0

LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$subtype|DataSource=$datasource|DataSourceType=$datasourcetype|FactorNumber=$factorno|DataSourceName=$datasourcename|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive-time|TimeoutThreshold=$timeout|src=$ip|srcPort=$beginport|dstPort=$endport|RepeatCount=$repeatcnt|vsys_id=$vsys_id

l) Copy the following text and paste it in the Custom Format column for the Tunnel Inspection log type.

PAN-OS v8.0

LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$event|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|subtype=$subtype|devtime=$cef-formatted-receive-time|starttime=$cef-formatted-starttime|time=$time|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|SessionTime=$sessiontime|RepeatCount=$repeatcnt|SourcePort=$sport|DestinationPort=$dport|TimeoutThreshold=$timeout|Logs|LogForwardingProfile=$logset|DataSource=$datasource|DataSourceType=$datasourcetype|DataSourceName=$datasourcename|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive-time|TimeoutThreshold=$timeout|src=$ip|srcPort=$beginport|dstPort=$endport|RepeatCount=$repeatcnt|vsys_id=$vsys_id

m) Copy the following text and paste it in the Custom Format column for the Correlation log type.

PAN-OS v8.0

LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$category|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|device=$device|time=$time|SourceUser=$srcuser|DestinationUser=$dstuser|VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|SessionID=$sessionid|SessionTime=$sessiontime|RepeatCount=$repeatcnt|SourcePort=$sport|DestinationPort=$dport|TimeoutThreshold=$timeout|SctpFragment=$sctp_fragment|SctpSessionsCreated=$sctp_sessions_created|SctpSessionsClosed=$sctp_sessions_closed|SctpSessionEndReason=$sctp_session_end_reason|ActionSource=$action_source|startTime=$start|ElapsedTime=$elapsed

n) Copy the following text, and paste it in the Custom Format column for the SCTP log type.

PAN-OS v8.1

LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$event|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|time=$time|SourceUser=$srcuser|DestinationUser=$dstuser|VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|SessionID=$sessionid|SessionTime=$sessiontime|RepeatCount=$repeatcnt|SourcePort=$sport|DestinationPort=$dport|TimeoutThreshold=$timeout|SctpFragment=$sctp_fragment|SctpSessionsCreated=$sctp_sessions_created|SctpSessionsClosed=$sctp_sessions_closed|SctpSessionEndReason=$sctp_session_end_reason|ActionSource=$action_source|startTime=$start|ElapsedTime=$elapsed

930 IBM QRadar : QRadar DSM Configuration Guide
7. Click OK.

8. Specify the severity of events that are contained in the Syslog messages.
   a) Click Log Settings.
   b) In the System pane, choose whether each severity should be contained in the Syslog message.
      1) Click the Severity name to edit each severity.
      2) Select the desired Syslog destination from the Syslog drop-down menu.
      3) Click OK.

9. Click Commit.

What to do next
To enable communication between your Palo Alto Networks device and QRadar, create a forwarding policy. See “Creating a forwarding policy on your Palo Alto PA Series device” on page 931.

Creating a forwarding policy on your Palo Alto PA Series device
If your IBMQRadar 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. Click Policies > Policy Based Forwarding.
3. Click Add.
4. Configure the parameters. For descriptions of the policy-based forwarding values, see your Palo Alto Networks Administrator’s Guide.

Creating ArcSight CEF formatted Syslog events on your Palo Alto PA Series Networks Firewall device
Configure your Palo Alto Networks firewall to send ArcSight CEF formatted Syslog events to IBM QRadar.

Procedure
1. Log in to the Palo Alto Networks interface.
2. Click the Device tab.
4. Click Add.
5. Specify the name, server IP address, port, and facility of the QRadar system that you want to use as a Syslog server:
   a) The Name is the Syslog server name.
   b) The Syslog Server is the IP address for the Syslog server.
   c) The Transport default is UDP.
   d) The Port default is 514.
   e) The Facility default is LOG_USER.
6. To select any of the listed log types that define a custom format, based on the ArcSight CEF for that log type, complete the following steps:
   a) Click the Custom Log Format tab and select any of the listed log types to define a custom format based on the ArcSight CEF for that log type. The listed log types are Config, System, Threat, Traffic, and HIP Match.
   b) Click OK twice to save your entries, then click Commit.
7. To define your own CEF-style formats that use the event mapping table that is provided in the ArcSight document, *Implementing ArcSight CEF*, you can use the following information about defining CEF style formats:

   a) The **Custom Log Format** tab supports escaping any characters that are defined in the CEF as special characters. For example, to use a backslash to escape the backslash and equal characters, enable the **Escaping** check box, specify `\=` as the **Escaped Characters** and `\` as the **Escape Character**.

   b) The following list displays the CEF-style format that was used during the certification process for each log type. These custom formats include all of the fields, in a similar order, that the default format of the Syslogs display.

   **Important:** Due to PDF formatting, do not copy and paste the message formats directly into the PAN-OS web interface. Instead, paste into a text editor, remove any carriage return or line feed characters, and then copy and paste into the web interface.

### Traffic

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$type  
|1|rt=$cef-formatted-receive_time deviceExternalId=$serial src=$src dst=$dst sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule user=$srcuser duser=$dstuser app=$sapp cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags proto=$proto act=$action flexNumber1Label=Total bytes flexNumber1=$bytes in=$bytes_sent out=$bytes_received cn2Label=Packets cn2=$packets PanOSPacketsReceived=$pkts_received PanOSPacketsSent=$pkts_sent start=$cef-formatted-time_generated cn3Label=Elapsed time in seconds cn3=$elapsed cs2Label=URL Category cs2=$category externalId=$seqno
```

### Threat

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$type
$number-of-severity|rt=$cef-formatted-receive_time
deviceExternalId=$serial src=$src dst=$dst sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule user=$srcuser duser=$dstuser app=$sapp cs3Label=Virtual System cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags proto=$proto act=$action request=$misc cs2Label=URL Category cs2=$category flexString2Label=Direction flexString2=$direction externalId=$seqno requestContext=$contenttype cat=$threatid filePath=$cloud fileId=$pcap_id fileHash=$filedigest
```

### Config

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$result|$type|1|rt=$cef-formatted-receive_time deviceExternalId=$serial dvchost=$host cs3Label=Virtual System cs3=$vsys act=$cmd duser=$admin destinationServiceName=$client msg=$path externalId=$seqno
```

### Optional:

```
cs1Label=Before Change Detail cs1=$before-change-detail
cs2Label=After Change Detail cs2=$after-change-detail
```
What to do next
For more information about Syslog configuration, see the PAN-OS Administrator's Guide on the Palo Alto Networks website (https://www.paloaltonetworks.com).

Sample event message
Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when using the Syslog protocol for the Palo Alto PA Series DSM:
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Denied</td>
<td>Firewall Deny</td>
<td>&lt;182&gt;Sep 28 14:31:56 paloalto.paseries.test</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 119. Pirean Access: One

The Pirean Access: One DSM for IBM QRadar collects events by polling the DB2 audit database for access management, and authentication events.

QRadar supports Pirean Access: One software installations at v2.2 that use a DB2 v9.7 database to store access management and authentication events.

Before you begin

Before you configure QRadar to integrate with Pirean Access: One, you can create a database user account and password for QRadar. Creating a QRadar account is not required, but is beneficial as it secures your access management and authentication event table data for the QRadar user.

Your QRadar user needs read permission access for the database table that contains your events. The JDBC protocol allows QRadar to log in and poll for events from the database based on the time stamp to ensure that the most recent data is retrieved.

Note: Ensure that firewall rules do not block communication between your Pirean Access: One installation and the QRadar Console or managed host responsible for event polling with JDBC.

Configuring a log source in QRadar to collect events from Pirean Access: One

To collect events, you must configure a log source in IBM QRadar to poll your Access: One installation database with the JDBC protocol.

Procedure

1. Click the Admin tab.
2. Click the Log Sources icon.
3. Click Add.
4. Configure the parameter values. The following table describes the parameters that require specific values to collect events from Pirean Access: One:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>(Optional)</td>
<td></td>
</tr>
<tr>
<td>Log Source Type</td>
<td>Pirean Access: One</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
</tbody>
</table>

© Copyright IBM Corp. 2005, 2019
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Log Source Identifier | Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol.  
If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2. |
| Database Type      | DB2                                                                                                                                              |
| Database Name      | Type the name of the database to which you want to connect. The default database name is LOGINAUD.                                                |
| IP or Hostname     | Type the IP address or host name of the database server.                                                                                       |
| Port               | Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535.  
The defaults are:  
• MSDE - 1433  
• Postgres - 5432  
• MySQL - 3306  
• Sybase - 1521  
• Oracle - 1521  
• Informix - 9088  
• DB2 - 50000  
If a database instance is used with the MSDE database type, you must leave the Port field blank. |
| Username           | A user account for QRadar in the database.                                                                                                       |
| Password           | The password that is required to connect to the database.                                                                                       |
| Confirm Password   | The password that is required to connect to the database.                                                                                       |
| Table Name         | Type AUDITDATA as the name of the table or view that includes the event records.                                                             
The table name can be up to 255 alphanumeric characters in length. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.). |
Table 512. Pirean Access: One JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select List</strong></td>
<td>Type * to include all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if it is needed for your configuration. The list must contain the field that is defined in the <strong>Compare Field</strong> parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.)</td>
</tr>
<tr>
<td><strong>Compare Field</strong></td>
<td>Type TIMESTAMP to identify new events added between queries to the table. The compare field can be up to 255 alphanumeric characters in length. The list can include the special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.)</td>
</tr>
<tr>
<td><strong>Use Prepared Statements</strong></td>
<td>Select this check box to use prepared statements, which allows the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clear this check box to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
<tr>
<td><strong>Start Date and Time (Optional)</strong></td>
<td>Optional. Configure the start date and time for database polling. The <strong>Start Date and Time</strong> 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.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Type the polling interval, which 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 without an H or M designator poll in seconds.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td><strong>Security Mechanism</strong></td>
<td>From the list, select the security mechanism that is supported by your DB2 server. If you don’t want to select a security mechanism, select <strong>None</strong>. The default is <strong>None</strong>. For more information about security mechanisms that are supported by DB2 environments, see the IBM Support website (<a href="https://www.ibm.com/support/knowledgelcenter/en/SSEPCC_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvcjsec.html">https://www.ibm.com/support/knowledgelcenter/en/SSEPCC_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvcjsec.html</a>)</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>Select this check box to enable the Pirean Access: One log source.</td>
</tr>
</tbody>
</table>

For more information about configuring a log source by using the JDBC protocol, see c_logsource_JDBCprotocol.dita

5. Click **Save**.

6. On the **Admin** tab, click **Deploy Changes**.
The configuration is complete. Access Management and authentication events for Pirean Access: One are displayed on the Log Activity tab of QRadar.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.
IBM QRadar can collect and categorize syslog mail events from PostFix Mail Transfer Agents (MTA) installed in your network.

To collect syslog events, you must configure PostFix MTA installation to forward syslog events to QRadar. QRadar does not automatically discover syslog events that are forwarded from PostFix MTA installations as they are multiline events. QRadar supports syslog events from PostFix MTA V2.6.6.

To configure PostFix MTA, complete the following tasks:

1. On your PostFix MTA system, configure syslog.conf to forward mail events to QRadar.
2. On your QRadar system, create a log source for PostFix MTA to use the UDP multiline syslog protocol.
3. On your QRadar system, configure IPtables to redirect events to the port defined for UDP multiline syslog events.
4. On your QRadar system, verify that your PostFix MTA events are displayed on the Log Activity tab.

If you have multiple PostFix MTA installations where events go to different QRadar systems, you must configure a log source and IPtables for each QRadar system that receives PostFix MTA multiline UDP syslog events.

### Configuring syslog for PostFix Mail Transfer Agent

To collect events, you must configure syslog on your PostFix MTA installation to forward mail events to IBM QRadar.

**Procedure**

1. Use SSH to log in to your PostFix MTA installation as a root user.
2. Edit the following file:
   `/etc/syslog.conf`
3. To forward all mail events, type the following command to change `-/var/log/maillog/` to an IP address. Make sure that all other lines remain intact:
   ```
   mail.*@<IP address>
   ```
   Where `<IP address>` is the IP address of the QRadar Console, Event Processor, or Event Collector, or all-in-one system.
4. Save and exit the file.
5. Restart your syslog daemon to save the changes.

### Configuring a PostFix MTA log source

To collect syslog events, you must configure a log source for PostFix MTA to use the UDP Multiline Syslog 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 log source.
5. From the **Log Source Type** list, select PostFix Mail Transfer Agent.
6. From the **Protocol Configuration** list, select **UDP Multiline Syslog**.

7. Configure the following parameter values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type the IP address, host name, or name to identify your PostFix MTA installation.</td>
</tr>
<tr>
<td><strong>Listen Port</strong></td>
<td>Type 517 as the port number used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65535.</td>
</tr>
<tr>
<td></td>
<td>To edit a saved configuration to use a new port number:</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Listen Port</strong> field, type the new port number for receiving UDP Multiline Syslog events.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>c. On the <strong>Admin</strong> tab toolbar, click <strong>Deploy Changes</strong> to make this change effective.</td>
</tr>
<tr>
<td></td>
<td>The port update is complete and event collection starts on the new port number.</td>
</tr>
<tr>
<td><strong>Message ID Pattern</strong></td>
<td>Type the following regular expression (regex) needed to filter the event payload messages.</td>
</tr>
<tr>
<td></td>
<td>postfix/.*?[ []\d+[ ]](?:- -</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>Select this check box to enable the log source.</td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
<td>Select the credibility of the log source. The range is 0 - 10.</td>
</tr>
<tr>
<td></td>
<td>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. The default is 5.</td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
<td>Select the <strong>Target Event Collector</strong> to use as the target for the log source.</td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
<td>Select this check box to enable the log source to coalesce (bundle) events.</td>
</tr>
<tr>
<td></td>
<td>By default, automatically discovered log sources inherit the value of the <strong>Coalescing Events</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
<td>Select this check box to enable the log source to store event payload information.</td>
</tr>
<tr>
<td></td>
<td>By default, automatically discovered log sources inherit the value of the <strong>Store Event Payload</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

8. Click **Save**.

9. On the **Admin** tab, click **Deploy Changes**.
Configuring IPtables for multiline UDP syslog events

To collect events, you must redirect events from the standard PostFix MTA port to port 517 for the UDP multiline protocol.

Procedure

1. Use SSH to log in to IBM QRadar as the root user.
2. To edit the IPtables file, type the following command:
   ```bash
   vi /opt/qradar/conf/iptables-nat.post
   ```
3. To instruct QRadar to redirect syslog events from UDP port 514 to UDP port 517, type the following command:
   ```bash
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port <new-port> -s <IP address>
   ```
   Where:
   - `<IP address>` is the IP address of your PostFix MTA installation.
   - `<New port>` is the port number that is configured in the UDP Multiline protocol for PostFix MTA.
   
   For example, if you had three PostFix MTA installations that communicate to QRadar, you can type the following code:
   ```bash
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s <IP_address1>
   -A PREROUTING -p udp --dport 517 -s <IP_address2> -j REDIRECT --to-port 517 -s <IP_address3>
   ```
4. Save your IPtables NAT configuration.

   You are now ready to configure IPtables on your QRadar Console or Event Collector to accept events from your PostFix MTA installation.
5. Type the following command to edit the IPtables file:
   ```bash
   vi /opt/qradar/conf/iptables.post
   ```
6. Type the following command to instruct QRadar to allow communication from your PostFix MTA installations:
   ```bash
   -I QChain 1 -m udp -p udp --src <IP address> --dport <New port> -j ACCEPT
   ```
   Where:
   - `<IP address>` is the IP address of your PostFix MTA installation.
   - `<New port>` is the port number that is configured in the UDP Multiline protocol.
   
   For example, if you had three PostFix MTA installations that communicate with an Event Collector, you can type the following code:
   ```bash
   -I QChain 1 -m udp -p udp --src <IP_address1> --dport 517 -j ACCEPT
   -I QChain 1 -m udp -p udp --src <IP_address2> --dport 517 -j ACCEPT
   -I QChain 1 -m udp -p udp --src <IP_address3> --dport 517 -j ACCEPT
   ```
7. To save the changes and update IPtables, type the following command:
   ```bash
   ./opt/qradar/bin/iptables_update.pl
   ```
Chapter 121. ProFTPd

IBM QRadar can collect events from a ProFTP server through syslog.

By default, ProFTPd logs authentication related messages to the local syslog using the `auth` (or `authpriv`) facility. All other logging is done using the daemon facility. To log ProFTPd messages to QRadar, use the SyslogFacility directive to change the default facility.

Configuring ProFTPd

You can configure syslog on a ProFTPd device:

**Procedure**

1. Open the `/etc/proftd.conf` file.
2. Below the LogFormat directives add the following line:
   
   ```
   SyslogFacility <facility>
   ```
   
   Where `<facility>` is one of the following options: `AUTH` (or `AUTHPRIV`), `CRON`, `DAEMON`, `KERN`, `LPR`, `MAIL`, `NEWS`, `USER`, `UUCP`, `LOCAL0`, `LOCAL1`, `LOCAL2`, `LOCAL3`, `LOCAL4`, `LOCAL5`, `LOCAL6`, or `LOCAL7`.
3. Save the file and exit.
4. Open the `/etc/syslog.conf` file
5. Add the following line at the end of the file:
   
   ```
   <facility> @<QRadar host>
   ```
   
   Where:

   - `<facility>` matches the facility that is chosen in “Configuring ProFTPd” on page 943. The facility must be typed in lowercase.
   - `<QRadar host>` is the IP address of your QRadar Console or Event Collector.

6. Restart syslog and ProFTPd:
   
   ```
   /etc/init.d/syslog restart
   /etc/init.d/proftpd restart
   ```

**What to do next**

You can now configure the log source in QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from ProFTPd. The following configuration steps are optional.

**About this task**

To manually configure a log source for ProFTPd:

**Procedure**

1. Log in to QRadar.
2. Click the `Admin` tab.
3. On the navigation menu, click `Data Sources`. 
The Data Sources pane is displayed.

4. Click the Log Sources icon.

The Log Sources window is displayed.

5. Click Add.

The Add a log source window is displayed.

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 ProFTPD Server.


The syslog protocol configuration is displayed.

10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 514. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.

12. On the Admin tab, click Deploy Changes.

The configuration is complete.
Chapter 122. Proofpoint Enterprise Protection and Enterprise Privacy

The IBM QRadar DSM for Proofpoint Enterprise Protection and Enterprise privacy can collect events from your Proofpoint Enterprise Protection and Enterprise Privacy DSM servers.

The following table identifies the specifications for the Proofpoint Enterprise Protection and Enterprise Privacy DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Proofpoint</td>
</tr>
<tr>
<td>DSM name</td>
<td>Proofpoint Enterprise Protection/Enterprise Privacy</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-Proofpoint_Enterprise_Protection/Enterprise_Privacy-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V7.02, V7.1, V7.2, V7.5, V8.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog, Log File</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>System, Email security threat classification, Email audit and encryption</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To integrate the Proofpoint Enterprise Protection and Enterprise Privacy DSM with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Proofpoint Enterprise Protection and Enterprise Privacy DSM RPM on your QRadar Console.
2. For each instance of Proofpoint Enterprise Protection and Enterprise Privacy, configure your Proofpoint Enterprise Protection and Enterprise Privacy DSM appliance to enable communication with QRadar.
3. Add a Proofpoint Enterprise Protection and Enterprise Privacy log source on your QRadar Console.

Related tasks
“Adding a DSM” on page 4
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 Proofpoint Enterprise Protection and Enterprise Privacy DSM to communicate with IBM QRadar**

To collect all audit logs and system events from your Proofpoint Enterprise Protection and Enterprise Privacy DSM, you must add a destination that specifies IBM QRadar as the Syslog server.

**Procedure**

1. Log in to the Proofpoint Enterprise interface.
2. Click **Logs and Reports**.
3. Click **Log Settings**.
4. From the **Remote Log Settings** pane, configure the following options to enable Syslog communication:
   a) Select **Syslog** as the communication protocol.
5. Type the IP address of the QRadar Console or Event Collector.
6. In the **Port** field, type 514 as the port number for Syslog communication.
7. From the **Syslog Filter Enable** list, select **On**.
8. From the **Facility** list, select **local1**.
9. From the **Level** list, select **Information**.
10. From the **Syslog MTA Enable** list, select **On**.
11. Click **Save**

**Configuring a Proofpoint Enterprise Protection and Enterprise Privacy log source**

You can manually add a log source in IBM QRadar for Proofpoint Enterprise Protection and Enterprise Privacy by using the Syslog or the Log File protocol.

**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 **Proofpoint Enterprise Protection/Enterprise Privacy**.
9. Configure the protocol:
   a) If you want to configure the **Syslog** protocol, select it from the **Protocol Configuration** list and configure the following values:
### Table 516. Syslog parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name for the log source as an identifier for events from Proofpoint Enterprise Protection and Enterprise Privacy 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.</td>
</tr>
</tbody>
</table>

**Note:** A Proofpoint Remote Syslog Forwarding subscription is required for Syslog support.

b) If you want to configure a **Log File** protocol, select it from the **Protocol Configuration** list and configure the following values:

### Table 517. Log file parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name for the log source as an identifier for events from Proofpoint Enterprise Protection and Enterprise Privacy 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.</td>
</tr>
</tbody>
</table>
| Service Type            | From the list, select the protocol that 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 that is used to retrieve log files for the SCP and SFTP service types requires that the server has specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled. |
<p>| Remote IP or Hostname   | Type the IP address or host name of the Proofpoint Enterprise Protection and Enterprise Privacy 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.                                      |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote User</td>
<td>Type the user name necessary to log in to your Proofpoint Enterprise Protection and Enterprise Privacy system. The user name can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Type the password necessary to log in to your Proofpoint Enterprise Protection and Enterprise Privacy system.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the Remote Password to log in to your Proofpoint Enterprise Protection and Enterprise Privacy system.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>If you select SCP or SFTP from the <strong>Service Type</strong> 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.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>Type the directory location on the remote host from which the files are retrieved.</td>
</tr>
<tr>
<td>Recursive</td>
<td>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.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>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 &quot;_filter&quot; in the file name, use the following entry: .<em>_filter.</em> .syslog. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: <a href="http://download.oracle.com/javase/tutorial/essential/regex/">http://download.oracle.com/javase/tutorial/essential/regex/</a></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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. |
| 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. |
Table 517. Log file parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>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.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>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.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the Event Generator list, select LINEBYLINE.</td>
</tr>
</tbody>
</table>

10. Click **Save**.

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

The log source is added to QRadar. Events that are forwarded to QRadar by Proofpoint Enterprise Protection and Enterprise Privacy are displayed on the **Log Activity** tab.
Chapter 123. Pulse Secure Pulse Connect Secure


The following table describes the specifications for the Pulse Secure Pulse Connect Secure DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Pulse Secure</td>
</tr>
<tr>
<td>DSM name</td>
<td>Pulse Secure Pulse Connect Secure</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-PulseSecurePulseConnectSecure-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>8.2R5</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog, TLS Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Admin, Authentication, System, Network, Error</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td>Pulse Secure website (<a href="https://www.pulsesecure.net">https://www.pulsesecure.net</a>)</td>
</tr>
</tbody>
</table>

To integrate Pulse Secure Pulse Connect Secure with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the Pulse Secure Pulse Connect Secure DSM RPM on your QRadar Console.

2. Configure your Pulse Secure Pulse Connect Secure device to send WebTrends Enhanced Log File (WELF) formatted events to QRadar.

3. Configure your Pulse Secure Pulse Connect Secure device to send syslog events to QRadar.

4. If QRadar does not automatically detect the log source, add a Pulse Secure Pulse Connect Secure log source on the QRadar Console. The following tables describe the parameters that require specific values to collect Syslog events from Pulse Secure Pulse Connect Secure:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Pulse Secure Pulse Connect Secure</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>
5. Optional. To add a Pulse Secure Pulse Connect Secure log source to receive syslog events from network devices that support TLS Syslog event forwarding, configure the log source on the QRadar Console to use the TLS Syslog protocol.

The following table describes the parameters that require specific values to collect TLS Syslog events from Pulse Secure Pulse Connect Secure:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Pulse Secure Pulse Connect Secure</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>TLS Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
<tr>
<td>TLS Protocols</td>
<td>Select the version of TLS that is installed on the client.</td>
</tr>
</tbody>
</table>

Related concepts
“TLS syslog protocol configuration options” on page 93
Configure a TLS Syslog protocol log source to receive encrypted syslog events from up to 1000 network devices that support TLS Syslog event forwarding.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 a Pulse Secure Pulse Connect Secure device to send WebTrends Enhanced Log File (WELF) events to IBM QRadar

Before you can send WebTrends Enhanced Log File (WELF) formatted events to QRadar, you must configure syslog server information for events, user access, administrator access and client logs on your Pulse Secure Pulse Connect Secure device.

Procedure
1. Log in to your Pulse Secure Pulse Connect Secure device administration user interface on the web:
   https://<IP_address>/admin
2. Configure syslog server information for events.
   a) Click System > Log/Monitoring > Events > Settings.
   b) From the Select Events to Log pane, select the events that you want to log.
   c) In the Server name/IP field, type the name or IP address of the syslog server.
   d) From the Facility list, select a syslog server facility level.
   e) From the Filter list, select WELF:WELF.
   f) Click Add, and then click Save Changes.
3. Configure syslog server information for user access.
   a) Click System > Log/Monitoring > User Access > Settings.
   b) From the Select Events to Log pane, select the events that you want to log.
   c) In the Server name/IP field, type the name or IP address of the syslog server.
   d) From the Facility list, select the facility.
4. Configure syslog server information for Administrator access.
a) Click System > Log/Monitoring > Admin Access > Settings.
b) From the Select Events to Log pane, select the events that you want to log.
c) In the Server name/IP field, type the name or IP address of the syslog server.
d) From the Facility list, select the facility.
e) From the Filter list, select WELF:WELF.
f) Click Add, then click Save Changes.

5. Configure syslog server information for client logs.
   a) Click System > Log/Monitoring > Client Logs > Settings.
   b) From the Select Events to Log pane, select the events that you want to log.
   c) In the Server name/IP field, type the name or IP address of the syslog server.
   d) From the Facility list, select the facility.
   e) From the Filter list, select WELF:WELF.
   f) Click Add, then click Save Changes.

Results
You are now ready to configure a log source in QRadar.

Configuring a Pulse Secure Pulse Connect Secure device to send syslog events to QRadar

To forward syslog events to QRadar, you need to configure syslog server information for events, user access, administrator access and client logs on your Pulse Secure Pulse Connect Secure device.

Procedure

1. Log in to your Pulse Secure Pulse Connect Secure device administration user interface on the web:
   https://<IP_address>/admin

2. Configure syslog server information for events.
   a) Click System > Log/Monitoring > Events > Settings.
   b) From the Select Events to Log section, select the events that you want to log.
   c) In the Server name/IP field, type the name or IP address of the syslog server.
   d) Click Add, and then click Save Changes.

3. Configure syslog server information for user access.
   a) Click System > Log/Monitoring > User Access > Settings.
   b) From the Select Events to Log section, select the events that you want to log.
   c) In the Server name/IP field, type the name or IP address of the syslog server.
   d) Click Add, and then click Save Changes.

4. Configure syslog server information for Administrator access.
   a) Click System > Log/Monitoring > Admin Access > Settings.
   b) From the Select Events to Log section, select the events that you want to log.
   c) In the Server name/IP field, type the name or IP address of the syslog server.
   d) Click Add, and then click Save Changes.

5. Configure syslog server information for client logs.
   a) Click System > Log/Monitoring > Client Logs > Settings.
   b) From the Select Events to Log section, select the events that you want to log.
   c) In the Server name/IP field, type the name or IP address of the syslog server.
d) Click **Add**, and then click **Save**.

**Results**
You are now ready to configure a log source in QRadar.

**Sample event message**

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message for the Pulse Secure Pulse Connect Secure DSM:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>VlanAssigned</td>
<td>Information</td>
<td>(\text{id=firewall time= 2009-10-01 22:26:39} \text{ pri=6 fw= &lt;IP_address&gt; vpn=ic user=user} \text{ realm=&lt;Domain&gt;} \text{ roles=Employee, Remediation} \text{ proto=} \text{ src=&lt;Source_IP_address&gt;} \text{ dst= dstname= type=vpn op=} \text{ arg=} \text{ result=} \text{ sent= rcvd= agent=} \text{ duration=} \text{ msg=EAM24459: User assigned to vlan (VLAN='16')})</td>
</tr>
</tbody>
</table>
IBM QRadar supports a range of Radware devices.

**Radware AppWall**

The IBM QRadar DSM for Radware AppWall collects logs from a Radware AppWall appliance. The following table describes the specifications for the Radware AppWall DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Radware</td>
</tr>
<tr>
<td>DSM name</td>
<td>Radware AppWall</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-RadwareAppWall-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V6.5.2 V8.2</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Vision Log</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Administration Audit Learning Security System</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Radware website (<a href="http://www.radware.com">http://www.radware.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Radware AppWall with QRadar, complete the following steps:

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Radware AppWall</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>
Note: Your RadWare AppWall device might have event payloads that are longer than the default maximum TCP Syslog payload length of 4096 bytes. This overage can result in the event payload being split into multiple events by QRadar. To avoid this behavior, increase the maximum TCP Syslog payload length. To optimize performance, start by configuring the value to 8192 bytes. The maximum length for RadWare AppWall events is 14019 bytes.

You can verify that QRadar is configured to receive events from your Radware AppWall device when you complete Step 6 of the Configuring Radware AppWall to communicate with QRadar procedure.

Related tasks
 “Adding a DSM” on page 4
 “Adding a log source” on page 4
 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 Radware AppWall to communicate with QRadar” on page 956
 Configure your Radware AppWall device to send logs to IBM QRadar. You integrate AppWall logs with QRadar by using the Vision Log event format.
 “Increasing the maximum TCP Syslog payload length for Radware AppWall” on page 956
 Increase the maximum TCP Syslog payload length for your RadWare AppWall appliance in IBM QRadar.

Configuring Radware AppWall to communicate with QRadar
 Configure your Radware AppWall device to send logs to IBM QRadar. You integrate AppWall logs with QRadar by using the Vision Log event format.

Procedure
 1. Log in to your Radware AppWall Console.
 2. Select Configuration View from the menu bar.
 3. In the Tree View pane on the left side of the window, click appwall Gateway > Services > Vision Support.
 4. From the Server List tab on the right side of the window, click the add icon (+) in the Server List pane.
 5. In the Add Vision Server window, configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The IP address for the QRadar Console.</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
<tr>
<td>Version</td>
<td>Select the most recent version from the list. It is the last item in the list.</td>
</tr>
</tbody>
</table>

6. Click Check to verify that the AppWall can successfully connect to QRadar.
7. Click Submit and Save.
8. Click Apply > OK.

Increasing the maximum TCP Syslog payload length for Radware AppWall
 Increase the maximum TCP Syslog payload length for your RadWare AppWall appliance in IBM QRadar.

Before you begin
 Note: Your RadWare AppWall device might have event payloads that are longer than the default maximum TCP Syslog payload length of 4096 bytes. This overage can result in the event payload being split into multiple events by QRadar. To avoid this behavior, increase the maximum TCP Syslog payload length. To optimize performance, start by configuring the value to 8192 bytes. The maximum length for RadWare AppWall events is 14019 bytes.
Procedure

1. If you want to increase the maximum TCP Syslog payload length for QRadar V7.2.6, follow these steps:
   a) Log in to the QRadar Console as an administrator.
   b) From the Admin tab, click System Settings.
   c) Click Advanced.
   d) In the Max TCP Syslog Payload Length field, type 8192.
   e) Click Save.
   f) From the Admin tab, click Deploy Changes.

2. If you want to increase the maximum TCP Syslog payload length for QRadar V7.2.5 and earlier, follow these steps:
   a) Use SSH to log in to the QRadar Console.
   b) Go to the /opt/qradar/conf/templates/configservice/pluggablesources/ directory, and edit the TCPSyslog.vm file.
   c) Type 8192 for the value for the MaxPayload parameter.
      For example, <parameter type=MaxPayload>8192</parameter>.
   d) Save the TCPSyslog.vm file.
   e) Log in to the QRadar Console as an administrator.
   f) From the Admin tab, click Advanced > Deploy Full Configuration.

Radware DefensePro

The Radware DefensePro DSM for IBM QRadar accepts events by using syslog. Event traps can also be mirrored to a syslog server.

Before you configure QRadar to integrate with a Radware DefensePro device, you must configure your Radware DefensePro device to forward syslog events to QRadar. You must configure the appropriate information by using the Device > Trap and SMTP option.

Any traps that are generated by the Radware device are mirrored to the specified syslog server. The current Radware Syslog server gives you the option to define the status and the event log server address.

You can also define more notification criteria, such as Facility and Severity, which are expressed by numerical values:

- **Facility** is a user-defined value that indicates the type of device that is used by the sender. This criteria is applied when the device sends syslog messages. The default value is 21, meaning Local Use 6.
- **Severity** indicates the importance or impact of the reported event. The Severity is determined dynamically by the device for each message sent.

In the Security Settings window, you must enable security reporting by using the connect and protect/security settings. You must enable security reports to syslog and configure the severity (syslog risk).

You are now ready to configure the log source in QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Radware DefensePro. The following configuration steps are optional.

About this task

To manually configure a log source for Radware DefensePro:
Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 Radware DefensePro.
   The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Radware DefensePro installation.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.
IBM QRadar collects and parses Log Event Extended Format (LEEF) events that are forwarded from Raz-Lee iSecurity installations on IBM i. The events are parsed and categorized by the IBM i DSM.

QRadar supports events from Raz-Lee iSecurity installations for iSecurity Firewall V15.7 and iSecurity Audit V11.7.

The following table describes the specifications for the IBM i DSM for Raz-Lee iSecurity installations:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>IBM</td>
</tr>
<tr>
<td>DSM name</td>
<td>IBM i</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-IBMi-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>iSecurity Firewall V15.7, iSecurity Audit V11.7</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All security, compliance, and audit events.</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>IBM website (<a href="http://www.ibm.com">http://www.ibm.com</a>)</td>
</tr>
</tbody>
</table>

Configuring Raz-Lee iSecurity to communicate with QRadar

To collect security, compliance, and audit events, configure your Raz-Lee iSecurity installation to forward Log Event Extended Format (LEEF) syslog events to IBM QRadar.

**Procedure**

1. Log in to the IBM i command-line interface.
2. From the command line, type STRAUD to access the **Audit** menu options.
3. From the **Audit** menu, select **81. System Configuration**.
4. From the **iSecurity/Base System Configuration** menu, select **32. SIEM 1**.
5. Configure the **32.SIEM 1** parameter values.

**Learn more about 32. SIEM 1 parameter values:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIEM 1 name</td>
<td>Type QRadar.</td>
</tr>
</tbody>
</table>
Table 526. 32.SIEM 1 parameter values (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Type the port that is used to send syslog messages. The default port is 514, which is the syslog standard.</td>
</tr>
<tr>
<td>SYSLOG type</td>
<td>Type 1 for UDP.</td>
</tr>
<tr>
<td>Destination address</td>
<td>Type the IP address for QRadar.</td>
</tr>
<tr>
<td>Severity range to auto send</td>
<td>Type a severity message level in the range of 0 - 7. For example, type 7 to send all syslog messages.</td>
</tr>
<tr>
<td>Facility to use</td>
<td>Type a syslog facility level in the range of 0 - 23.</td>
</tr>
<tr>
<td>Message structure</td>
<td>Type *LEEF.</td>
</tr>
<tr>
<td>Convert data to CCSID</td>
<td>Type 0 in the Convert data to CCSID field. This is the default character conversion.</td>
</tr>
<tr>
<td>Maximum length</td>
<td>Type 1024.</td>
</tr>
</tbody>
</table>

6. From the iSecurity/Base System Configuration menu, select 31. Main Control.

7. Configure the 31. Main Control parameter values.

Learn more about 31. Main Control parameter values:

Table 527. 31. Main Control parameter values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run rules before sending</td>
<td>To process the events that you want to send, type Y. To send all events, type N.</td>
</tr>
<tr>
<td>SIEM 1: QRadar</td>
<td>Type Y.</td>
</tr>
<tr>
<td>Send JSON messages (for DAM)</td>
<td>Type N.</td>
</tr>
<tr>
<td>As only operation</td>
<td>Type N.</td>
</tr>
</tbody>
</table>

8. From the command line, to configure the Firewall options, type STRFW to access the menu options.


10. From the iSecurity (part 1) Global Parameters: menu, select 72. SIEM 1.

11. Configure the 72.SIEM 1 parameter values.

Learn more about 72. SIEM 1 parameter values:

Table 528. 72.SIEM 1 parameter values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIEM 1 name</td>
<td>Type QRadar.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port that is used to send syslog messages. The default port is 514, which is the Syslog standard.</td>
</tr>
<tr>
<td>SYSLOG type</td>
<td>Type 1 for UDP syslog type.</td>
</tr>
<tr>
<td>Send in FYI mode</td>
<td>Type N.</td>
</tr>
</tbody>
</table>
Table 528. 72.SIEM 1 parameter values (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination address</td>
<td>Type the IP address for the QRadar console.</td>
</tr>
<tr>
<td>Severity range to auto send</td>
<td>Type a severity level in the range 0 - 7.</td>
</tr>
<tr>
<td>Facility to use</td>
<td>Type a facility level.</td>
</tr>
<tr>
<td>Message structure</td>
<td>Type *LEEF.</td>
</tr>
<tr>
<td>Convert data to CCSID</td>
<td>Type 0.</td>
</tr>
<tr>
<td>Maximum length</td>
<td>Type 1024.</td>
</tr>
</tbody>
</table>

12. From the **iSecurity (part 1) Global Parameters** menu, select **71. Main Control**.
13. Configure the **71. Main Control** parameter values.

Learn more about **71. Main Control** parameter values:

Table 529. 71. Main Control parameter values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIEM 1: QRadar</td>
<td>Type 2.</td>
</tr>
<tr>
<td>Send JSON messages (for DAM)</td>
<td>Type 0.</td>
</tr>
</tbody>
</table>

Results
Syslog LEEF events that are forwarded by Raz-Lee iSecurity are automatically discovered by the QRadar DSM for IBM i. In most cases, the log source is automatically created in QRadar after a few events are detected.

If the event rate is low, you can manually configure a log source for Raz-Lee iSecurity in QRadar. Until the log source is automatically discovered and identified, the event type displays as Unknown on the **Log Activity** tab. View automatically discovered log sources on the **Admin** tab by clicking the **Log Sources** icon.

**Configuring a log source for Raz-Lee iSecurity**

IBM QRadar automatically discovers and creates a log source for Syslog LEEF events that are forwarded from Raz-Lee iSecurity. If the log source isn't automatically discovered, you can manually create it.

**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. In the **Log Source Description** field, type a description for the log source.
6. From the **Log Source Type** list, select **IBM i**.
7. From the **Protocol Configuration** list, select **Syslog**.
8. Configure the syslog protocol values.

Learn more about syslog protocol parameters:
Table 530. Syslog protocol parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the log source that sends events from the Raz-Lee iSecurity device.</td>
</tr>
<tr>
<td>Enabled</td>
<td>By default, the check box is selected.</td>
</tr>
<tr>
<td>Credibility</td>
<td>The Credibility of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>By default, automatically discovered log sources inherit the value of the Coalescing Events list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td>Incoming Payload Encoding</td>
<td>Select Incoming Payload Encoder for parsing and storing the logs.</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>By default, automatically discovered log sources inherit the value of the Store Event Payload list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

9. Click Save.
10. On the Admin tab, click Deploy Changes.
Chapter 126. Redback ASE

The Redback ASE DSM for IBM QRadar accepts events by using syslog.
The Redback ASE device can send log messages to the Redback device console or to a log server that is integrated with QRadar to generate deployment-specific reports. Before you configure a Redback ASE device in QRadar, you must configure your device to forward syslog events.

Configuring Redback ASE

You can configure the device to send syslog events to IBM QRadar.

Procedure

1. Log in to your Redback ASE device user interface.
2. Start the CLI configuration mode.
3. In global configuration mode, configure the default settings for the security service:
   asp security default
4. In ASP security default configuration mode, configure the IP address of the log server and the optional transport protocol:
   log server <IP address> transport udp port 9345
   Where <IP address> is the IP address of the QRadar.
5. Configure the IP address that you want to use as the source IP address in the log messages:
   log source <source IP address>
   Where <source IP address> is the IP address of the loopback interface in context local.
6. Commit the transaction.

   For more information about Redback ASE device configuration, see your vendor documentation.

   For example, if you want to configure:
   - Log source server IP address <IP_address>
   - Default transport protocol: UDP
   - Default server port: 514

   The source IP address that is used for log messages is <IP_address>. This address must be an IP address of a loopback interface in context local.

   asp security default log server <IP_address1> log source <IP_address2>

What to do next

You can now configure the log sources in QRadar.

Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events from Redback ASE. The following configuration steps are optional.

About this task

To manually configure a log source for Redback ASE:
Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
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 Redback ASE.
   The syslog protocol configuration is displayed.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 531. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
   The configuration is complete.
Chapter 127. Resolution1 CyberSecurity

Resolution1 CyberSecurity is formerly known as AccessData InSight. The Resolution1 CyberSecurity DSM for IBM QRadar collects event logs from your Resolution1 CyberSecurity device.

The following table identifies the specifications for the Resolution1 CyberSecurity DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Resolution1</td>
</tr>
<tr>
<td>DSM name</td>
<td>Resolution1 CyberSecurity</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-Resolution1CyberSecurity-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V2</td>
</tr>
<tr>
<td>Event format</td>
<td>Log file</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Volatile Data, Memory Analysis Data, Memory Acquisition Data, Collection Data, Software Inventory, Process Dump Data, Threat Scan Data, Agent Remediation Data</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Included identity?</td>
<td>No</td>
</tr>
</tbody>
</table>

To send events from Resolution1 CyberSecurity to QRadar, use the following steps:

1. If automatic updates are not enabled, download the most recent versions of the following RPMs.
   - LogFileProtocol
   - DSMCommon
   - Resolution1 CyberSecurity DSM

2. Configure your Resolution1 CyberSecurity device to communicate with QRadar.

3. Create a Resolution1 CyberSecurity log source on the QRadar Console.

Related tasks
Adding a DSM
Configuring your Resolution1 CyberSecurity device to communicate with QRadar
To collect Resolution1 CyberSecurity events, you must configure your third-party device to generate event logs in LEEF format. You must also create an FTP site for Resolution1 CyberSecurity to transfer the LEEF files. QRadar can then pull the logs from the FTP server.

Resolution1 CyberSecurity log source on your QRadar Console
QRadar does not automatically discover the Resolution1 CyberSecurity log source. You must manually add the log source.

**Configuring your Resolution1 CyberSecurity device to communicate with QRadar**

To collect Resolution1 CyberSecurity events, you must configure your third-party device to generate event logs in LEEF format. You must also create an FTP site for Resolution1 CyberSecurity to transfer the LEEF files. QRadar can then pull the logs from the FTP server.

**Procedure**

1. Log in to your Resolution1 CyberSecurity 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:
   ```xml
   <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 Resolution1 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.

**Resolution1 CyberSecurity log source on your QRadar Console**

QRadar does not automatically discover the Resolution1 CyberSecurity 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 Resolution1 CyberSecurity device.
7. From the Log Source Type list, select Resolution1 CyberSecurity.
8. From the Protocol Configuration list, select Log File.
9. Configure the remaining parameters.
10. Click Save.
IBM QRadar supports a number of Riverbed DSMs:

**Riverbed SteelCentral NetProfiler (Cascade Profiler) Audit**

The IBM QRadar DSM for Riverbed SteelCentral NetProfiler Audit collects audit 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Riverbed</td>
</tr>
<tr>
<td>DSM name</td>
<td>SteelCentral NetProfiler Audit</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-RiverbedSteelCentralNetProfilerAudit-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Event format</td>
<td>Log file protocol</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Audit Events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Riverbed website (<a href="http://www.riverbed.com/">http://www.riverbed.com/</a>)</td>
</tr>
</tbody>
</table>

To integrate Riverbed SteelCentral NetProfiler Audit 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-LogFile RPM
   - Riverbed SteelCentral NetProfiler Audit RPM
2. Create an audit report template on your Riverbed host and then configure a third-party host to use the template to generate the audit file. See “Creating a Riverbed SteelCentral NetProfiler report template and generating an audit file” on page 968.
3. Create a log source on the QRadar Console. The log source allows QRadar to access the third-party host to retrieve the audit file. Use the following table to define the Riverbed-specific parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Riverbed SteelCentral NetProfiler Audit</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>LogFile</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>The IP address or host name of the third-party host that stores the generated audit file</td>
</tr>
<tr>
<td>Remote User</td>
<td>The user name for the account that can access the host.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>The password for the user account.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>The absolute file path on the third-party host that contains the generated audit file.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>A regex pattern that matches the name of the audit file.</td>
</tr>
</tbody>
</table>
### Related tasks

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 Riverbed SteelCentral NetProfiler report template and generating an audit file

To prepare for Riverbed SteelCentral NetProfiler integration with QRadar, create a report template on the Riverbed SteelCentral NetProfiler and then use a third-party host to generate an audit file. The third-party host must be a system other than the host you use for Riverbed SteelCentral NetProfiler or QRadar.

#### Before you begin

Ensure that the following items are installed on a third-party host that you use to run the audit report:

- **Python**
  
  Download and install Python from the Python website (https://www.python.org/download/).

- **SteelScript for Python**
  
  Download and install the SteelScript for Python SDK from the Riverbed SteelScript for Python website (https://support.riverbed.com/apis/steelscript/index.html). The script generates and downloads an audit file in CSV format. You must periodically run this script.

#### Procedure

1. Define the audit file report template.
   
   a) Log in to your Riverbed SteelCentral NetProfiler host user interface.
   
   b) Select **System > Audit Trail**.
   
   c) Select the criteria that you want to include in the audit file.
   
   d) Select a time frame.
   
   e) On the right side of the window, click **Template**.
   
   f) Select **Save As/Schedule**.
   
   g) Type a name for the report template.

2. To run the report template and generate an audit file, complete the following steps
   
   a) Log in to the third-party host on which you installed Python.
   
   b) Type the following command:

   ```
   $ python ./get_template_as_csv.py <riverbed_host_name> -u admin -p admin -t "<report_template_name>" -o <absolute_path_to_target_file>
   ```

   **Tip:** Record the report template name and file path. You need to use the name to run the report template and when you configure a log source in the QRadar interface.
Riverbed SteelCentral NetProfiler (Cascade Profiler) Alert

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Riverbed</td>
</tr>
<tr>
<td>DSM name</td>
<td>SteelCentral NetProfiler</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-RiverbedSteelCentralNetProfiler-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Event format</td>
<td>JDBC</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Alert Events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Riverbed website (<a href="http://www.riverbed.com/">http://www.riverbed.com/</a>)</td>
</tr>
</tbody>
</table>

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 JDBC parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Riverbed SteelCentral NetProfiler</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>Postgres</td>
</tr>
<tr>
<td>Database Name</td>
<td>You can type the actual name of the Riverbed database. For most configurations, the database name is mazu. <strong>Tip:</strong> Confirm the actual name of the Riverbed database.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name of the database server.</td>
</tr>
</tbody>
</table>
Table 536. Riverbed SteelCentral NetProfiler JDBC log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port                | Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535.  
                     | The defaults are:  
                     | • MSDE - 1433  
                     | • Postgres - 5432  
                     | • MySQL - 3306  
                     | • Sybase - 1521  
                     | • Oracle - 1521  
                     | • Informix - 9088  
                     | • DB2 - 50000  
                     | If a database instance is used with the MSDE database type, you must leave the Port field blank. |
| Table Name          | events.export_csv_view                                                                                                                      |
| Select List         | The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the Compare Field. |
| Username            | The user name for the account that is configured to access the PostgreSQL database on the Riverbed SteelCentral NetProfiler system.          |
| Password            | The password that is required to connect to the database.                                                                                  |
| Compare Field       | start_time                                                                                                                                  |
| Use Prepared Statements | Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements. |
| Start Date and Time (Optional) | Type the start date and time for database polling in the following format: 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. |
| Polling Interval    | 5M                                                                                                                                           |
| EPS Throttle        | The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000.                           |

For more information about configuring JDBC protocol parameters, see [c_logsource_JDBCprotocol.dita](#).

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4
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 129. RSA Authentication Manager

You can use an RSA Authentication Manager DSM to integrate IBM QRadar with an RSA Authentication Manager 6.x or 7.x by using syslog or the log file protocol. RSA Authentication Manager 8.x uses syslog only.

Before you configure QRadar to integrate with RSA Authentication Manager, select your configuration preference:

• “Configuration of syslog for RSA Authentication Manager 6.x, 7.x and 8.x” on page 973
• “Configuring the log file protocol for RSA Authentication Manager 6.x and 7.x” on page 974

Note: You must apply the most recent hot fix on RSA Authentication Manager 7.1 primary, replica, node, database, and radius installations before you configure syslog.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Configuration of syslog for RSA Authentication Manager 6.x, 7.x and 8.x

The procedure to configure your RSA Authentication Manager 6.x, 7.x and 8.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” on page 973.

If you are using RSA Authentication Manager on Windows, see “Configuring Windows” on page 974.

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 one of the following files for editing based on your version of RSA Authentication Manager:
   - Versions earlier than version 8
     /usr/local/RSASecurity/RSAAuthenticationManager/utils/resources/ims.properties
   - Version 8
     /opt/rsa/am/utils/resources/ims.properties
3. Add the following entries to the ims.properties file:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ims.logging.audit.admin.syslog_host</td>
<td>&lt;IP address&gt;</td>
</tr>
<tr>
<td>ims.logging.audit.admin.use_os_logger</td>
<td>true</td>
</tr>
<tr>
<td>ims.logging.audit.runtime.syslog_host</td>
<td>&lt;IP address&gt;</td>
</tr>
<tr>
<td>ims.logging.audit.runtime.use_os_logger</td>
<td>true</td>
</tr>
<tr>
<td>ims.logging.system.syslog_host</td>
<td>&lt;IP address&gt;</td>
</tr>
<tr>
<td>ims.logging.system.use_os_logger</td>
<td>true</td>
</tr>
</tbody>
</table>

Where <IP address> is the IP address or host name of IBM QRadar.
4. Save the ims.properties file.
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 host name of QRadar.

7. Type the following command to restart the syslog services for Linux.
   
   `service syslog restart`

   For more information on configuring syslog forwarding, see your RSA Authentication Manager documentation.

What to do next

Configure the log source and protocol in QRadar. To receive events from RSA Authentication Manager, from the Log Source Type list, select the RSA Authentication Manager option.

Configuring Windows

To configure RSA Authentication Manager for syslog using Microsoft Windows.

Procedure

1. Log in to the system that hosts 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 entries 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 host name of QRadar.
4. Save the ims.properties files.
5. Restart RSA services.

   You are now ready to configure the log source in QRadar.
6. To configure QRadar to receive events from your RSA Authentication Manager: From the Log Source Type list, select the RSA Authentication Manager option.

   For more information on configuring syslog forwarding, see your RSA Authentication Manager documentation.

Configuring the log file protocol for RSA Authentication Manager 6.x and 7.x

The log file protocol allows IBM 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 v6.x, see “Configuring RSA Authentication Manager 6.x” on page 975.
- If you are using RSA Authentication Manager v7.x, see “Configuring RSA Authentication Manager 7.x” on page 975.
Configuring RSA Authentication Manager 6.x

You can configure your RSA Authentication Manager 6.x device.

Procedure
1. Log in to the RSA Security Console.
2. Log in to the RSA Database Administration tool.
3. Click the Advanced tool.
   The system prompts you to log in again.
4. Click Database Administration.
   For complete information on using SecurID, see your vendor documentation.
5. From the Log list, select Automate Log Maintenance.
   The Automatic Log Maintenance window is displayed.
7. Select Delete and Archive.
8. Select Replace files.
9. Type an archive file name.
10. In the Cycle Through Version(s) field, type a value.
11. For example 1, Select Select all Logs.
12. Select a frequency.
13. Click OK.
14. You are now ready to configure the log sources and protocol in IBM 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.

Related tasks
“Adding a log source” on page 4
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 RSA Authentication Manager 7.x

You can configure your RSA Authentication Manager 7.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 from 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.

**Related concepts**

“Log File protocol configuration options” on page 62

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

**Related tasks**

“Adding a log source” on page 4

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 130. SafeNet DataSecure

The IBM QRadar DSM for SafeNet DataSecure collects syslog events from a SafeNet DataSecure device. DataSecure maintains activity, such as, record administrative actions, network activity, and cryptography requests. QRadar supports SafeNet DataSecure V6.3.0.

SafeNet DataSecure creates the following event logs:

**Activity Log**
Contains a record of each request that is received by the key server.

**Audit Log**
Contains a record of all configuration changes and user input errors that are made to SafeNet KeySecure, whether through the management console or the command-line interface.

**Client Event Log**
Contains a record of all client requests that have the `<RecordEventRequest>` element.

**System Log**
Contains a record of all system events, such as the following events:

- Service starts, stops, and restarts
- SNMP traps
- Hardware failures
- Successful or failed cluster replication and synchronization
- Failed log transfers

To integrate SafeNet DataSecure with QRadar, complete the following steps:

1. Enable syslog on the SafeNet DataSecure device.
2. QRadar automatically discovers SafeNet DataSecure after your system receives 25 events and configures a log source. If QRadar does not automatically discover SafeNet DataSecure, add a log source.

Related tasks

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 SafeNet DataSecure to communicate with QRadar

Before you add the DSM for SafeNet DataSecure, enable syslog on your SafeNet DataSecure device.

**Procedure**

1. Log in to the SafeNet DataSecure management console as an administrator with logging access control.
2. Select **Device > Log Configuration**.
3. Select the **Rotation & Syslog** tab.
4. Select a log in the **Syslog Settings** section and click **Edit**.
5. Select **Enable Syslog**.
6. Configure the following parameters:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Server #1 IP</td>
<td>The IP address or host name of the target QRadar. Event Collector.</td>
</tr>
<tr>
<td>Syslog Server #1 Port</td>
<td>The listening port for QRadar. Use Port 514.</td>
</tr>
<tr>
<td>Syslog Server #1 Proto</td>
<td>QRadar can receive syslog messages by using either UDP or TCP.</td>
</tr>
</tbody>
</table>

7. Optional. Type an IP address port, and protocol for a Syslog Server #2. When two servers are configured, SafeNet DataSecure sends messages to both servers.

8. Type the Syslog Facility or accept the default value of local1.

9. Click **Save**.
Chapter 131. Salesforce

IBM QRadar supports a range of Salesforce DSMs.

Salesforce Security

The IBM QRadar DSM for Salesforce Security can collect Salesforce Security Auditing audit trail logs and Salesforce Security Monitoring event logs from your Salesforce console by using a RESTful API in the cloud.

The following table identifies the specifications for the Salesforce Security DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Salesforce</td>
</tr>
<tr>
<td>DSM</td>
<td>Salesforce Security</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-SalesforceSecurity-QRadar_Version-Build_Number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>Salesforce REST API Protocol</td>
</tr>
<tr>
<td>Automatically discovered</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity</td>
<td>Yes</td>
</tr>
<tr>
<td>More information</td>
<td>Salesforce website (<a href="http://www.salesforce.com/">http://www.salesforce.com/</a>)</td>
</tr>
</tbody>
</table>

Salesforce Security DSM integration process

To integrate Salesforce Security 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.
   - Protocol Common RPM
   - SalesforceRESTAPI Protocol RPM
   - DSMCommon RPM
   - Salesforce Security Auditing RPM
   - Salesforce Security RPM
2. Configure the Salesforce Security server to communicate with QRadar.
3. Obtain and install a certificate to enable communication between Salesforce Security 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, 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 isn’t enabled on your Salesforce server, contact Salesforce support.

**Procedure**

1. Configure and collect information that is generated by the Connected App.
   a) Log in to your Salesforce Security Monitoring server.
   b) Click the **Setup** button.
   c) In the navigation pane, click **Create > Apps > New**.
   d) Type the name of your application.
   e) Type the contact email information.
   f) Select **Enable OAuth Settings**.
   g) From the **Selected OAuth Scopes** list, select **Access and manage your data (api)**.
   h) In the **Info URL** field, type a URL where the user can go for more information about your application.
   i) Configure the remaining optional parameters.
   j) Click **Save**.

2. Turn on **Entitlement History**.
   a) Click the **Setup** button.
   b) In the navigation pane, select **Build > Customize > Entitlement Management > Enablement Settings**.
   c) From the **Entitlement Management Settings** window, select the **Enable Entitlement Management** check box.
   d) 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. Don’t 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 log source in QRadar**
To collect Salesforce Security events, configure a log source in QRadar.

**Before you begin**
When you configured a Connected App on the Salesforce Security server, the following information was generated:

- Consumer Key
• Consumer Secret
• Security token

This information is required to configure a Salesforce Security log source in QRadar.

Ensure that the trusted certificate from the Salesforce Security instance is copied to the `/opt/qradar/conf/trusted_certificates` folder in .DER format on QRadar system.

**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**.
7. From the **Protocol Configuration** list, select **Salesforce Rest API**.
8. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login URL</td>
<td>The URL of the Salesforce security console.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name of the Salesforce security console.</td>
</tr>
<tr>
<td>Security Token</td>
<td>The security token that was sent to the email address configured as the contact email for the Connected App on the Salesforce security console.</td>
</tr>
<tr>
<td>Client ID</td>
<td>The Consumer Key that was generated when you configured the Connected App on the Salesforce security console.</td>
</tr>
<tr>
<td>Secret ID</td>
<td>The Consumer Secret that was generated when you configured the Connected App on the Salesforce security console.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>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 <strong>Proxy Server</strong>, <strong>Proxy Port</strong>, <strong>Proxy Username</strong>, and <strong>Proxy Password</strong> fields. If the proxy does not require authentication, you can leave the <strong>Proxy Username</strong> and <strong>Proxy Password</strong> fields blank.</td>
</tr>
<tr>
<td>Advanced Options</td>
<td>By default the Salesforce Rest API collects Audit Trail and Security Monitoring events. Configure available options as required.</td>
</tr>
</tbody>
</table>

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

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Salesforce</td>
</tr>
<tr>
<td>DSM</td>
<td>Salesforce Security Auditing</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-SalesforceSecurityAuditing-QRadar_Version-Build_Number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>Log File</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>Setup Audit Records</td>
</tr>
<tr>
<td>Automatically discovered</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Salesforce web site (<a href="http://www.salesforce.com/">http://www.salesforce.com/</a>)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Generator</td>
<td>RegEx Based Multiline</td>
</tr>
<tr>
<td>Start Pattern</td>
<td>(d{1,2}/d{1,2}/d{4} \d{1,2}:\d{2}:\d{2}\ w+)</td>
</tr>
<tr>
<td>End Pattern</td>
<td>Ensure that this parameter remains empty.</td>
</tr>
<tr>
<td>Date Time RegEx</td>
<td>(d{1,2}/d{1,2}/d{4} \d{1,2}:\d{2}:\d{2}\ w+)</td>
</tr>
<tr>
<td>Date Time Format</td>
<td>dd/MM/yyyy hh:mm:ss z</td>
</tr>
</tbody>
</table>

⚠️ 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 132. Samhain Labs

The Samhain Labs Host-Based Intrusion Detection System (HIDS) monitors changes to files on the system.

The Samhain HIDS DSM for IBM QRadar supports Samhain version 2.4 when used for File Integrity Monitoring (FIM).

You can configure the Samhain HIDS DSM to collect events by using syslog or JDBC.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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 syslog to collect Samhain events

Before you configure IBM QRadar to integrate with Samhain HIDS using syslog, you must configure the Samhain HIDS system to forward logs to your QRadar system.

About this task
The following procedure is based on the default samhainrc file. If the samhainrc file is modified, some values might be different, such as the syslog facility.

Procedure
1. Log in to Samhain HIDS from the command-line interface.
2. Open the following file:
   /etc/samhainrc
3. Remove the comment marker (#) from the following line:
   SetLogServer=info
4. Save and exit the file.
   Alerts are sent to the local system by using syslog.
5. Open the following file:
   /etc/syslog.conf
6. Add the following line:
   local2.* @<IP Address>
   Where <IP Address> is the IP address of your QRadar.
7. Save and exit the file.
8. Restart syslog:
   /etc/init.d/syslog restart
   Samhain sends logs by using syslog to QRadar.
   You are now ready to configure Samhain HIDS DSM in QRadar.
9. From the Log Source Type list, select the Samhain HIDS option.

Related tasks
“Adding a log source” on page 4
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 Samhain events by using the JDBC protocol

You can configure Samhain HIDS to send log alerts to a database. Oracle, PostgreSQL, and MySQL are natively supported by Samhain. Configure IBM QRadar to collect events from these databases by using the JDBC protocol.

### Before you begin

**Note:** IBM QRadar does not include a MySQL driver for JDBC. If you are using a DSM or protocol that requires a MySQL JDBC driver, you must download and install the *platform* independent MySQL Connector/J from the MySQL website ([https://dev.mysql.com/downloads/connector/j/](https://dev.mysql.com/downloads/connector/j/)).

### Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Click **Add**.
4. Configure the parameters.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>(Optional)</td>
<td></td>
</tr>
<tr>
<td>Log Source Type</td>
<td>Samhain HIDS</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be</td>
</tr>
<tr>
<td></td>
<td>unique among all log sources of the log source type that is configured to</td>
</tr>
<tr>
<td></td>
<td>use the JDBC protocol.</td>
</tr>
<tr>
<td></td>
<td>If the log source collects events from a single appliance that has a static</td>
</tr>
<tr>
<td></td>
<td>IP address or host name, use the IP address or host name of the appliance</td>
</tr>
<tr>
<td></td>
<td>as all or part of the Log Source Identifier value; for example, 192.168.1.1</td>
</tr>
<tr>
<td></td>
<td>or JDBC192.168.1.1. If the log source doesn't collect events from a single</td>
</tr>
<tr>
<td></td>
<td>appliance that has a static IP address or host name, you can use any unique</td>
</tr>
<tr>
<td></td>
<td>name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>Select Oracle, PostgreSQL, or MySQL</td>
</tr>
<tr>
<td>Database Name</td>
<td><code>&lt;Samhain SetDBName&gt;</code></td>
</tr>
<tr>
<td>IP or Hostname</td>
<td><code>&lt;Samhain SetDBHost&gt;</code></td>
</tr>
<tr>
<td></td>
<td>The IP address or host name of the database server.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Port              | Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are:  
  - MSDE - 1433  
  - Postgres - 5432  
  - MySQL - 3306  
  - Sybase - 1521  
  - Oracle - 1521  
  - Informix - 9088  
  - DB2 - 50000  
  If a database instance is used with the MSDE database type, you must leave the Port field blank. |
| Username          | <Samhain SetDBUser>  
  A user account for QRadar in the database. |
| Password          | <Samhain SetDBPassword>  
  The password that is required to connect to the database. |
| Confirm Password  | The password that is required to connect to the database. |
| Predefined Query  | Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the none option. |
| Table Name        | <Samhain SetDBTable>  
  The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.). |
| Select List       | Type * to select all fields.  
  The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the Compare Field. |
| Compare Field     | Type log_index.  
  A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. Enables the protocol to identify events that were previously polled by the protocol to ensure that duplicate events are not created. |
<p>| Use Prepared Statements | Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start Date and Time</strong></td>
<td>Type the start date and time for database polling in the following format: 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.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value. The maximum polling interval is one week.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000.</td>
</tr>
</tbody>
</table>
| **Use Oracle Encryption** | Oracle Encryption and Data Integrity settings is also known as Oracle Advanced Security.  
If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.                                                                 |

Where:
- `<Samhain Database Type>` is the database type that is used by Samhain (see your Samhain system administrator).
- `<Samhain SetDBName>` is the database name that is specified in the samhainrc file.
- `<Samhain SetDBTable>` is the database table that is specified in the samhainrc file.
- `<Samhain SetDBHost>` is the database host that is specified in the samhainrc file.
- `<Samhain SetDBUser>` is the database user who is specified in the samhainrc file.
- `<Samhain SetDBPassword>` is the database password that is specified in the samhainrc file.

For more information about configuring the JDBC protocol, see c_logsource_JDBCprotocol.dita

5. Click **Save**.
6. On the **Admin** tab, click **Deploy Changes**.

**Related tasks**
- “Adding a log source” on page 4
- 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 133. SAP Enterprise Threat Detection

Overview

The IBM QRadar DSM for SAP Enterprise Threat Detection collects events from an SAP Enterprise Threat Detection server. SAP Enterprise Threat Detection enables real-time security intelligence to help protect against cybersecurity threats and help ensure data loss prevention.

To integrate SAP Enterprise Threat Detection 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:
   - Protocol-Common RPM
   - SAP ETD Alert API Protocol RPM
   - SAP Enterprise Threat Detection DSM RPM

2. Configure QRadar to receive events from SAP Enterprise Threat Detection. See “Configuring QRadar to collect events from your SAP Enterprise Threat Detection system” on page 990.


4. If QRadar does not automatically detect the log source, add an SAP Enterprise Threat Detection log source on the QRadar Console.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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

Related reference
“SAP Enterprise Threat Detection DSM specifications” on page 989

The following table describes the specifications for the SAP Enterprise Threat Detection DSM.

SAP Enterprise Threat Detection DSM specifications

The following table describes the specifications for the SAP Enterprise Threat Detection DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>SAP</td>
</tr>
<tr>
<td>DSM name</td>
<td>SAP Enterprise Threat Detection</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-SAPEnterpriseThreatDetection-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>SAP ETD version sp6</td>
</tr>
<tr>
<td>Protocol</td>
<td>SAP Enterprise Threat Detection Alert API</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Alerts</td>
</tr>
</tbody>
</table>
Table 540. SAP Enterprise Threat Detection DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

**Configuring QRadar to collect events from your SAP Enterprise Threat Detection system**

Configure IBM QRadar to collect events from your SAP Enterprise Threat Detection (ETD) server.

**Before you begin**

To connect to the SAP Enterprise Threat Detection server by using the SAP Enterprise Threat Detection Alert API, the following requirements must be met:

- The SAP Enterprise Threat Detection server must be configured to generate alert events.
- You need the user name and password that is used to connect to the SAP Enterprise Threat Detection server.
- Check that the server port is not blocked by a firewall.

**Procedure**

1. Log in to QRadar and click the **Admin** tab.
2. In the navigation menu, click **Data Sources > Log Sources**.
3. In the **Log Sources** window, click **Add**.
4. Give the log source a name and description.
5. From the **Log Source Type** list, select **SAP Enterprise Threat Detection**.
6. From the **Protocol Configuration** list, select **SAP Enterprise Threat Detection Alert API**.
7. Complete the log source parameters for SAP Enterprise Threat Detection with the parameter information from the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source type</strong></td>
<td>SAP Enterprise Threat Detection</td>
</tr>
<tr>
<td><strong>Protocol Configuration</strong></td>
<td>SAP Enterprise Threat Detection Alert API</td>
</tr>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>A unique identifier for the log source. The Log Source Identifier can be any valid value, including the same value as the Log Source Name, and doesn't need to reference a specific server. If you configured multiple SAP Enterprise Threat Detection Alert API log sources, you might want to identify the first log source as SAPETD-1, the second log source as SAPETD-2, and the third log source as SAPETD-3.</td>
</tr>
<tr>
<td><strong>Server URL</strong></td>
<td>Specify the URL used to access the SAP Enterprise Threat Detection Alert API, including</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>the port. For example, “<a href="http://192.0.2.1:8003%E2%80%9D">http://192.0.2.1:8003”</a> or “<a href="https://192.0.2.1:9443%E2%80%9D">https://192.0.2.1:9443”</a>.</td>
<td></td>
</tr>
<tr>
<td>Username/Password</td>
<td>Enter the user name and password that are required to access the SAP ETD server, and then confirm that you entered the password correctly. The confirmation password must be identical to the password you typed for the password parameter. <strong>Important:</strong> SAP Enterprise Threat Detection has a login attempt limit of three attempts. If your account is locked because of multiple login attempts, you cannot connect QRadar to the SAP Enterprise Threat Detection Server until the account is unlocked. Contact SAP Support for assistance.</td>
</tr>
<tr>
<td>Use Pattern Filter</td>
<td>Select this option to limit the query to only a specific pattern filter. Leave the field cleared to query for all the events.</td>
</tr>
<tr>
<td>Pattern Filter Id</td>
<td>The pattern filter Id that is used to filter the query. The field accepts a UUID that is created when a pattern filter is made. The <strong>Filter Id</strong> is the UUID mentioned in the protocol parameters table for parameter Pattern Filter Id.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses the SAP Enterprise Threat Detection Alert API by using a proxy, enable Use Proxy. If the proxy requires authentication, configure the <strong>Proxy Hostname or IP</strong>, <strong>Proxy Port</strong>, <strong>Proxy Username</strong>, and <strong>Proxy</strong> fields. If the proxy does not require authentication, configure the <strong>Proxy Hostname or IP</strong> and <strong>Proxy Port</strong>.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificates</td>
<td>If you choose <strong>Yes</strong> from the list, QRadar automatically downloads the certificate and begins trusting the target server. If <strong>No</strong> is selected, QRadar does not attempt to retrieve any server certificates. <strong>Note:</strong> If the SAP Enterprise Threat Detection Server is configured for HTTPS, a valid certificate is required. Either set this value to <strong>Yes</strong> or manually retrieve a certificate for the Log Source.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The time interval between log source queries to the SAP Enterprise Threat Detection Alert API for new events. The time interval can be in hours (H), minutes (M), or days (D). The default is 5 minutes (5M).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
</tr>
<tr>
<td>Throttle</td>
<td>The maximum number of events per second. The default is 5000.</td>
</tr>
</tbody>
</table>

8. Click **Save**.

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

**Related concepts**

“Sample event messages” on page 993

Use these sample event messages as a way of verifying a successful integration with QRadar. Replace the sample IP addresses, and so on with your own content.

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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 pattern filter on the SAP server**

A **Pattern Filter** is a user configured setting that can be used to limit queries to specific events. When a **Pattern Filter** is generated on the SAP server, a **Filter Id** is provided. The **Filter Id** can then be entered into the **Pattern Filter Id** field of the QRadar log source to filter the patterns that are retrieved.

**Procedure**

1. To create the **Pattern Filter** on the SAP Server, use the following steps:
   a) Log in into the SAP server by using the administrator user name and password.
   b) Go to **Administration > Settings**.
   c) Select **Pattern Filter** and click **Add**.
   d) Enter a name for the **Pattern Filter**. This name is only used for identification purposes.
      
      **Note:** The name appears in the **Name Column** with a corresponding **Filter Id** (UUID). Record the **Filter Id** for future reference.
   e) Click the pattern filter name to see a new table with **Namespace** as a column header.
   f) To add patterns to the **Pattern Filter**, click **Add**.
      
      **Note:** A new window appears called **Pattern**.
   g) Select any **Pattern** you want to filter on and click **OK**.
   h) Refresh the page and ensure that the **Pattern** was added to the table with the **Namespace** header.

2. To use a **Pattern Filter** with QRadar, use the following steps:
   a) Either select or create an SAP ETD Alert API log source.
   b) Find the **Use Pattern Filter Id** check box and select it.
   c) Enter the **Filter Id** obtained in step 1d and enter it in the **Pattern Filter Id** field.
   d) Save the log source.

   **Note:** If you receive a 500 Internal Server Error after you save the log source with the **Filter Id**, double check that there is at least one pattern that is being filtered for.
Troubleshooting the SAP Enterprise Threat Detection Alert API

The SAP Enterprise Threat Detection DSM relies on the default pattern names of alerts to identify the events. Modifying the default patterns might result in events that appear as "Unknown".

**Procedure**

1. Verify that the SAP Enterprise Threat Detection server login credentials are valid by following these steps:
   a) In a Web browser, enter the IP address or domain name of your SAP Enterprise Threat Detection server. For example, http://192.0.2.1:8003.
   b) Enter your user name and password.

2. Query the SAP Enterprise Threat Detection server to verify that QRadar can receive events. Use the following example as a starting point to create your query:

   ```
   <Server_URL>/sap/secmon/services/Alerts.xsjs?$query=AlertCreationTimestamp%20ge%20<Date>T15:00:00.00Z&$format=LEEF&$batchSize=10
   ```

   In the example, replace the following parameters with your own values:

   - `<Server_URL>`: The address of the SAP Enterprise Threat Detection server you are trying to access.
   - `<Date>`: The current day's date in the YYYY-MM-DD format. Choose a date where you know that events came in; for example, 2017-10-15.

   The resulting query might look like this example:

   ```
   http://192.0.2.1:8003/sap/secmon/services/Alerts.xsjs?$query=AlertCreationTimestamp%20ge%202017-10-15T15:00:00.00Z&$format=LEEF&$batchSize=10
   ```

   If a problem exists with the query, it's unlikely that QRadar can successfully connect with SAP Enterprise Threat Detection.

3. Check that the server port is not blocked by a firewall.

   **Note:** If the port is blocked, contact your security or network administrator to open the port.

**Related concepts**

- "Sample event messages" on page 993
  Use these sample event messages as a way of verifying a successful integration with QRadar. Replace the sample IP addresses, and so on with your own content.

**Related reference**

- "SAP Enterprise Threat Detection DSM specifications" on page 989
  The following table describes the specifications for the SAP Enterprise Threat Detection DSM.

**Sample event messages**

Use these sample event messages as a way of verifying a successful integration with QRadar. Replace the sample IP addresses, and so on with your own content.

The following table provides sample event messages for the SAP Enterprise Threat Detection DSM.
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklisted function modules</td>
<td>Potential Misc. Exploit</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event name</td>
<td>Low-level category</td>
<td>Sample log message</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Brute force attack</td>
<td>Brute force attack</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Data Exchange by System ID with Third-Party Systems</td>
<td>Suspicious Activity</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event name</td>
<td>Low-level category</td>
<td>Sample log message</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data Exchange by Technical User</td>
<td>Suspicious Activity</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Debugging in systems assigned to critical roles</td>
<td>Suspicious Activity</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event name</td>
<td>Low-level category</td>
<td>Sample log message</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event name</td>
<td>Low-level category</td>
<td>Sample log message</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Generic access to critical database tables</td>
<td>Database Exploit</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Log Volume by System Group</td>
<td>Suspicious Activity</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event name</td>
<td>Low-level category</td>
<td>Sample log message</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logon and Communication by System ID</td>
<td>Suspicious Activity</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event name</td>
<td>Low-level category</td>
<td>Sample log message</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>New Service Calls by Technical Users</td>
<td>Suspicious Activity</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event name</td>
<td>Low-level category</td>
<td>Sample log message</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security relevant configuration changes</td>
<td>Suspicious Activity</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Service Calls by System ID</td>
<td>Suspicious Activity</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>

Chapter 133. SAP Enterprise Threat Detection Overview 1001
<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>User acts under created user</td>
<td>User Activity</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>
Chapter 134. Seculert

The IBM QRadar DSM for Seculert collects events from the Seculert cloud service. The following table describes the specifications for the Seculert DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Seculert</td>
</tr>
<tr>
<td>DSM name</td>
<td>Seculert</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-Seculert-&lt;qradar_version&gt;-&lt;build_number&gt;.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>v1</td>
</tr>
<tr>
<td>Protocol</td>
<td>Seculert Protection REST API Protocol</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All malware communication events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Seculert website (<a href="http://www.seculert.com">http://www.seculert.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Seculert with QRadar, complete the following steps:

1. Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol-Common
   - DSM-DSMCommon
   - Seculert DSM RPM
   - SeculertProtectionRESTAPI PROTOCOL RPM

2. Add a Seculert log source on the QRadar Console. The following table describes the parameters that require specific values for Seculert event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Seculert</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Seculert Protection REST API</td>
</tr>
<tr>
<td>API Key</td>
<td>32 character UUID For more information about obtaining an API key, see Obtaining an API key</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Obtaining an API key**

Before you can collect events from Seculert, you must copy your API key from the Seculert cloud service user interface to QRadar.

**Procedure**

1. Log in to the Seculert web portal.
2. On the dashboard, click the **API** tab.
3. Copy the value for **Your API Key**.

**What to do next**

You will need the API key that you copied when you configure a log source for Seculert in QRadar.
Chapter 135. Sentrigo Hedgehog

You can integrate a Sentrigo Hedgehog device with IBM QRadar.

About this task
A Sentrigo Hedgehog device accepts LEEF events by using syslog. Before you configure QRadar to integrate with a Sentrigo Hedgehog device, take the following steps:

Procedure
1. Log in to the Sentrigo Hedgehog command-line interface (CLI).
2. Open the following file for editing:
   `<Installation directory>/conf/sentrigo-custom.properties`
   Where `<Installation directory>` is the directory that contains your Sentrigo Hedgehog installation.
3. Add the following `log.format` entries to the custom properties file:
   
   ```
   Note: Depending on your Sentrigo Hedgehog configuration or installation, you might need to replace or overwrite the existing `log.format` entry.
   
   sentrigo.comm.ListenAddress=1996
   log.format.body.custom=usrName=$osUser:20$|duser=$execUser:20$|
   severity=$severity$|identHostName=$sourceName:20$|src=$sourceIP:30$|
   dst=$targetIP:30$|devTime=$logonTime$|
   devTimeFormat=EEE MMM dd HH:mm:ss z yyyy|
   cmdType=$cmdType$|externalId=$id$|
   execTime=$executionTime.time$|
   dstServiceName=$database.name:20$|
   srcHost=$sourceHost:30$|execProgram=$execProgram:20$|
   cmdType=$cmdType:15$|oper=$operation:225$|
   accessedObj=$accessedObjects.name:200$
   log.format.header.custom=LEEF:1.0|
   Sentrigo|Hedgehog|$serverVersion|$
   log.format.header.escaping.custom=\|
   log.format.header.seperator.custom=,
   log.format.header.escape.char.custom=\|
   log.format.body.escaping.custom=\|
   log.format.body.escape.char.custom=\|
   log.format.body.seperator.custom=|
   log.format.empty.value.custom=NULL
   log.format.length.value.custom=10000
   log.format.convert.newline.custom=true
   ```

4. Save the custom properties file.
5. Stop and restart your Sentrigo Hedgehog service to implement the `log.format` changes.

You can now configure the log source in QRadar.

6. To configure QRadar to receive events from a Sentrigo Hedgehog device: From the Log Source Type list, select the Sentrigo Hedgehog option.

   For more information about Sentrigo Hedgehog see your vendor documentation.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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 136. Skyhigh Networks Cloud Security Platform


The following table identifies the specifications for the Skyhigh Networks Cloud Security Platform DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Skyhigh Networks</td>
</tr>
<tr>
<td>DSM name</td>
<td>Skyhigh Networks Cloud Security Platform</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-SkyhighNetworksCloudSecurityPlatform-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>2.4 and 3.3</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Privilege Access, Insider Threat, Compromised Account, Access, Admin, Data, Policy, and Audit</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Skyhigh Networks website (<a href="http://www.skyhighnetworks.com/">www.skyhighnetworks.com/</a>)</td>
</tr>
</tbody>
</table>

To integrate Skyhigh Networks Cloud Security Platform 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:
   - Skyhigh Networks Cloud Security Platform DSM RPM
   - DSMCommon RPM

2. Configure your Skyhigh Networks Cloud Security Platform device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a Skyhigh Networks Cloud Security Platform log source on the QRadar Console. The following table describes the parameters that require specific values for Skyhigh Networks Cloud Security Platform event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Skyhigh Networks Cloud Security Platform</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>The IP address or host name of the Skyhigh Networks Cloud Security Platform that sends events to QRadar.</td>
</tr>
</tbody>
</table>

4. To verify that QRadar is configured correctly, go to the following table to review a sample event message.
The following table shows a sample event message from Skyhigh Networks Cloud Security Platform:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| Login Success    | User Login Success        | <14>Mar 16 18:51:10 hostname
LEEF:1.0|Skyhigh|Anomalies|192.0.2.0|LoginSuccess|cat=Alert.Access
devTimeFormat=MMM dd yyyy HH:mm:ss.
SSS zzz    devTime=Jan 30 2017 06:59:11.000 UTC    usrName=username
sev=0    activityName=Login
anomalyValue=51
countries=[XX]    emailDomain=example.com  incidentGroupId=10014
incidentId=733    isPartOfThreat=false
riskSeverity=low
serviceNames=[<Services>]
sourceIps=[<Source_IP_address]
status=OPENED threatCategory=Compromised Accounts
Duration=daily thresholdValue=30
updatedAt=Jan 30 2017 07:08:05.906 UTC |

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 Skyhigh Networks Cloud Security Platform to communicate with QRadar

Procedure
1. Log in to the Skyhigh Enterprise Connector administration interface.
2. Select Enterprise Integration > SIEM Integration.
3. Configure the following SIEM SYSLOG SERVICE parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIEM server</td>
<td>ON</td>
</tr>
<tr>
<td>Format</td>
<td>Log Event Extended Format (LEEF)</td>
</tr>
<tr>
<td>Syslog Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>&lt;QRadar IP or hostname&gt;</td>
</tr>
<tr>
<td>Syslog Port</td>
<td>514</td>
</tr>
<tr>
<td>Send to SIEM</td>
<td>new anomalies only</td>
</tr>
</tbody>
</table>

4. Click Save.
Chapter 137. SolarWinds Orion

The IBM QRadar DSM for SolarWinds Orion collects events from a SolarWinds Orion appliance.

The following table describes the specifications for the SolarWinds Orion DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>SolarWinds</td>
</tr>
<tr>
<td>DSM name</td>
<td>SolarWinds Orion</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-SolarWindsOrion-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>2013.2.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>SNMPv2, SNMPv3</td>
</tr>
<tr>
<td>Event format</td>
<td>name-value pair (NVP)</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>SolarWinds website (<a href="http://www.solarwinds.com/orion">http://www.solarwinds.com/orion</a>)</td>
</tr>
</tbody>
</table>

To integrate SolarWinds Orion with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the SolarWinds Orion DSM RPM on your QRadar Console:
2. Configure your SolarWinds Orion device to send events to QRadar.
3. Add a SolarWinds Orion log source on the QRadar Console.
4. Verify that QRadar is configured correctly.

The following table shows a normalized sample event message from SolarWinds Orion:
Table 548. SolarWinds Orion sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain controller</td>
<td>Warning</td>
<td>1.3.6.1.2.1.1.3.0=0:00:00.00 1.3.6.1.6.3.1.1.4.1.0=1.3.6.1.4.1.11307.10 1.3.6.1.4.1.11307.10.2=hostname 1.3.6.1.4.1.11307.10.3=127.0.0.1 1.3.6.1.4.1.11307.10.4=2466 1.3.6.1.4.1.11307.10.5=hostname 1.3.6.1.4.1.11307.10.6=Node 1.3.6.1.4.1.11307.10.7=2466 1.3.6.1.4.1.11307.10.8=InfoSec - EMAIL ONLY - Domain Controller UnManaged - hostname - Status = Unknown - EMAIL ONLY - Domain Controller UnManaged hostname is Unknown.</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Configuring a SolarWinds Orion log source by using the SNMP protocol” on page 1012

Configure IBM QRadar to access your SolarWinds Orion appliance by using the SNMP protocol.

Configuring SolarWinds Orion to communicate with QRadar

To collect events in IBM QRadar from SolarWinds Orion, you must configure your SolarWinds Orion Alert Manager device to create SNMP traps.

Procedure

1. Log in to your SolarWinds Orion Alert Manager device.
2. Select Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager.
3. In the Alert Manager Quick Start window, click Configure Alerts.
4. In the Manage Alerts window, select an existing alert and then click Edit.
5. Click the Triggered Actions tab.
6. Click Add New Action.
7. In the Select an Action window, select Send an SNMP Trap and then click OK.
8. To configure SNMP Trap Destinations, type the IP address of the QRadar Console or QRadar Event Collector.
9. To configure the Trap Template, select ForwardSyslog.
10. To configure the SNMP Version, select the SNMP version that you want to use to forward the event:

   **SNMPv2c** - Type the SNMP Community String to use for SNMPv2c authentication. The default SNMP Community String value is public.

   **SNMPv3** - Requires a username and password for authentication. The default username is "public" and the default password is "public".

IBM QRadar : QRadar DSM Configuration Guide

1010
Note: To verify that your SNMP trap is configured properly, select an alert that you edited and click Test. This action triggers and forwards the events to QRadar.

SNMPv3 - Type the Username and then select the Authentication Method to use for SNMPv3.
Figure 11. Edit SNMP Trap Action configuration for SNMPv3

**Note:** To verify that your SNMP trap is configured properly, select an alert that you edited and click **Test**. This action triggers and forwards the events to QRadar.

11. Click **OK**.

**What to do next**

Repeat these steps to configure the SolarWinds Orion Alert Manager with all of the SNMP trap alerts that you want to monitor in QRadar.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 a SolarWinds Orion log source by using the SNMP protocol**

Configure IBM QRadar to access your SolarWinds Orion appliance by using the SNMP protocol.

**Procedure**

1. Click the **Admin** tab.
2. Click the **Log Sources** icon, and then click **Add**.
3. In the **Log Source Name** field, type a name for your SolarWinds Orion log source.
4. From the **Log Source Type** list, select **SolarWinds Orion**.
5. From the **Protocol Configuration** list, select either **SNMPv2** or **SNMPv3**.
6. Optional: If you selected **SNMPv2**, configure the following specific log source parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or the host name of your SolarWinds Orion appliance to use as the identifier.</td>
</tr>
<tr>
<td>Community</td>
<td>Type the SNMP community name that was used when SNMP was configured on your SolarWinds Orion appliance.</td>
</tr>
<tr>
<td>Include OIDs in Event Payload</td>
<td>To allow the SolarWinds Orion event payloads to be constructed as name-value pairs instead of the standard event payload format, select the Include OIDs in Event Payload check box. <strong>Important:</strong> You must include OIDs in the event payload for processing SNMPv2 or SNMPv3 events for SolarWinds Orion.</td>
</tr>
</tbody>
</table>

7. Optional: If you selected **SNMPv3**, configure the following specific log source parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or the host name of your SolarWinds Orion appliance to use as the identifier.</td>
</tr>
</tbody>
</table>
| Authentication Protocol    | The algorithm that was used when SNMP was configured on your SolarWinds Orion appliance:  
  • **MD5** uses Message Digest 5 (MD5) as your authentication protocol.  
  • **SHA** uses Secure Hash Algorithm (SHA) as your authentication protocol. |
| Authentication Password    | The password that was used when SNMP was configured on your SolarWinds Orion appliance. Your authentication password must include a minimum of 8 characters. |
| Decryption Protocol        | Select the algorithm that was used when SNMP was configured on your SolarWinds Orion appliance. Your authentication password must include a minimum of 8 characters.  
  • **DES**  
  • **AES128**  
  • **AES192**  
  • **AES256**  
  **Note:** If you select AES192 or AES256 as your decryption algorithm, you must install the Java Cryptography Extension. |
### Table 550. SNMPv3 log source parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Decryption Password</strong></td>
<td>The decryption password that was used when SNMP was configured on your SolarWinds Orion appliance. Your decryption password must include a minimum of 8 characters.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The user name that was used when SNMP was configured on your SolarWinds Orion appliance.</td>
</tr>
<tr>
<td><strong>Include OIDs in Event Payload</strong></td>
<td>To allow the SolarWinds Orion event payloads to be constructed as name-value pairs instead of the standard event payload format, select the <strong>Include OIDs in Event Payload</strong> check box. Important: You must include OIDs in the event payload for processing SNMPv2 or SNMPv3 events for SolarWinds Orion.</td>
</tr>
</tbody>
</table>

8. Click **Save**.

9. Click the **Admin** tab, and then click **Deploy Changes**.

**Related tasks**

“Installing the Java Cryptography Extension on QRadar” on page 746

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

---

### Installing the Java Cryptography Extension on QRadar

The Java Cryptography Extension (JCE) is a Java framework that is required for IBM 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 Java Cryptography Extension from the following website:
   The Java 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 QRadar Event Collector as a root user.

4. Copy the JCE JAR files to the following directory on your QRadar Console or Event Collector:
   /opt/ibm/java-x86_64/jre/lib/security/
   **Note:** The JCE JAR files are only copied to the system that receives the AES192 or AES256 encrypted files.

5. Restart the QRadar services by typing one of the following commands:
   - If you are using QRadar 7.2.x, type `service ecs-ec restart`.
   - If you are using QRadar 7.3.0, type `systemctl restart ecs-ec.service`.

---

1014 IBM QRadar : QRadar DSM Configuration Guide
• If you are using QRadar 7.3.1, type `systemctl restart ecs-ec-ingress.service`. 
Chapter 138. SonicWALL

The SonicWALL SonicOS DSM accepts events by using syslog.

IBM QRadar records all relevant syslog events that are forwarded from SonicWALL appliances by using SonicOS firmware. Before you can integrate with a SonicWALL SonicOS device, you must configure syslog forwarding on your SonicWALL SonicOS appliance.

Configuring SonicWALL to forward syslog events

SonicWALL captures all SonicOS event activity. The events can be forwarded to IBM QRadar by using SonicWALL's default event format.

**Procedure**

1. Log in to your SonicWALL web interface.
2. From the navigation menu, select **Log > Syslog**.
3. From the **Syslog Servers** pane, click **Add**.
4. In the **Name or IP Address** field, type the IP address of your QRadar Console or Event Collector.
5. In the **Port** field, type **514**.
   
   SonicWALL syslog forwarders send events to QRadar by using UDP port 514.
6. Click **OK**.
7. From the **Syslog Format** list, select **Default**.
8. Click **Apply**.

   Syslog events are forwarded to QRadar. SonicWALL events that are forwarded to QRadar are automatically discovered and log sources are created automatically. For more information on configuring your SonicWALL appliance or for information on specific events, see your vendor documentation.

Configuring a log source

QRadar automatically discovers and creates a log source for syslog events from SonicWALL appliances. The following configuration steps are optional.

**About this task**

To manually configure a log source for SonicWALL syslog events:

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. In the **Log Source Name** field, type a name for your log source.
6. In the **Log Source Description** field, type a description for the log source.
7. From the **Log Source Type** list, select **SonicWALL SonicOS**.
8. From the **Protocol Configuration** list, select **Syslog**.
9. Configure the following values:
### Table 551. Syslog parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from SonicWALL appliances. Each log source that you create for your SonicWALL SonicOS appliance ideally includes a unique identifier, such as an IP address or host name.</td>
</tr>
</tbody>
</table>

10. Click **Save**.

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

The log source is added to QRadar. Events that are forwarded to QRadar by SonicWALL SonicOS appliances are displayed on the **Log Activity** tab. For more information, see the *IBM QRadar User Guide*. 
Chapter 139. Sophos

IBM QRadar supports a number of Sophos DSMs.

Sophos Enterprise Console

IBM QRadar has two options for gathering events from a Sophos Enterprise Console by using JDBC. Select the method that best applies to your Sophos Enterprise Console installation:

- “Configuring QRadar using the Sophos Enterprise Console Protocol” on page 1019
- c_DSMSGuide_Sophos_EntConsole_JDBC.dita#c_dsm_guide_sophos_entconsole_jdbc

Note: To use the Sophos Enterprise Console protocol, you must ensure that the Sophos Reporting Interface is installed with your Sophos Enterprise Console. If you do not have the Sophos Reporting Interface, you must configure QRadar by using the JDBC protocol. For information on installing the Sophos Reporting Interface, see your Sophos Enterprise Console documentation.

Related tasks
- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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

Related information
- c_logsource_JDBCprotocol.dita

Configuring QRadar using the Sophos Enterprise Console Protocol

The Sophos Enterprise Console DSM for IBM QRadar accepts events by using Java Database Connectivity (JDBC).

About this task

The Sophos Enterprise Console DSM works in coordination with the Sophos Enterprise Console protocol to combine payload information from anti-virus, application control, device control, data control, tamper protection, and firewall logs in the vEventsCommonData table and provide these events to QRadar. You must install the Sophos Enterprise Console protocol before you configure QRadar.

To configure QRadar to access the Sophos database by using the JDBC protocol:

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
6. From the Log Source Type list, select Sophos Enterprise Console.
7. From the Protocol Configuration list, select Sophos Enterprise Console JDBC.
**Note:** You must refer to the **Configure Database Settings** on your Sophos Enterprise Console to define the parameters that are required to configure the Sophos Enterprise Console JDBC protocol in QRadar.

8. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Log Source Identifier**| Type the identifier for the log source. Type the log source identifier in the following format: <Sophos Database>@<Sophos Database Server IP or Host Name> Where:  
• <Sophos Database> is the database name, as entered in the Database Name parameter.  
• <Sophos Database Server IP or Host Name> is the host name or IP address for this log source, as entered in the IP or Hostname parameter.   
When you define a name for your log source identifier, you must use the values of the Sophos Database and Database Server IP address or host name from the Management Enterprise Console. |
| **Database Type**        | From the list, select **MSDE**.                                                                                                                |
| **Database Name**        | Type the exact name of the Sophos database.                                                                                                  |
| **IP or Hostname**       | Type the IP address or host name of the Sophos SQL Server.                                                                                  |
| **Port**                 | Type the port number that is used by the database server. The default port for **MSDE** in Sophos Enterprise Console is 1168.  
The JDBC configuration port must match the listener port of the Sophos database. The Sophos database must have incoming TCP connections are enabled to communicate with QRadar.  
If you define a **Database Instance** when you use **MSDE** as the database type, you must leave the **Port** parameter blank in your configuration. |
<p>| <strong>Username</strong>             | Type the user name that is required to access the database.                                                                                  |
| <strong>Password</strong>             | Type the password that is required to access the database. The password can be up to 255 characters in length.                               |
| <strong>Confirm Password</strong>     | Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the Password parameter. |
| <strong>Authentication Domain</strong>| If you select <strong>MSDE</strong> as the <strong>Database Type</strong> and the database is configured for Windows, you must define a Window Authentication Domain. Otherwise, leave this field blank. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Instance</td>
<td>Optional. Type 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 block access to port 1434 for SQL database resolution, you must leave the Database Instance parameter blank in your configuration.</td>
</tr>
<tr>
<td>Table Name</td>
<td>Type vEventsCommonData as the name of the table or view that includes the event records.</td>
</tr>
<tr>
<td>Select List</td>
<td>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 this is needed for your configuration. The list must contain the field that is defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.)</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Type InsertedAt as the compare field. The compare field is used to identify new events added between queries to the table.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Type the polling interval, which 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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td>Use Named Pipe Communication</td>
<td>Clear the Use Named Pipe Communications check box. When 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.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>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 to ensure Named Pipe communication functions properly.</td>
</tr>
</tbody>
</table>
Configure IBM QRadar by using the JDBC protocol

The Sophos Enterprise Console DSM for IBM QRadar accepts events by using Java Database Connectivity (JDBC).

QRadar records all relevant anti-virus events. This document provides information on configuring QRadar to access the Sophos Enterprise Console database by using the JDBC protocol.

Configuring the database view

To integrate IBM QRadar with Sophos Enterprise Console:

Procedure

1. Log in to your Sophos Enterprise Console device command-line interface (CLI).
2. Type the following command to create a custom view in your Sophos database to support QRadar:

   ```
   ```

   Where `<Database Name>` is the name of the Sophos database.

   **Note:** The database name must not contain any spaces.

   **What to do next**

   After you create your custom view, you must configure QRadar to receive event information that uses the JDBC protocol. To configure the Sophos Enterprise Console DSM with QRadar, see “Configuring a JDBC log source in QRadar to collect events from Sophos Enterprise Console” on page 1023.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use NTLMv2</td>
<td>If you select MSDE as the Database Type, the Use NTLMv2 check box is displayed. Select the Use NTLMv2 check box to force MSDE connections to use the NTLMv2 protocol when they communicate with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the Use NTLMv2 check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.</td>
</tr>
</tbody>
</table>

**Note:** Selecting a value greater than 5 for the Credibility parameter weights your Sophos log source with a higher importance compared to other log sources in QRadar.
Configuring a JDBC log source in QRadar to collect events from Sophos Enterprise Console

You can configure IBM QRadar to access the Sophos Enterprise Console database by using the JDBC protocol.

Procedure

1. Log in to QRadar
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.

**Note:** You must refer to the Configure Database Settings on your Sophos Enterprise Console to define the parameters that are required to configure the Sophos Enterprise Console DSM in QRadar.

5. Configure the parameters. The following table describes the parameters that require specific values to collect events from Sophos Enterprise Console by using the JDBC protocol:

<table>
<thead>
<tr>
<th>Table 553. Sophos Enterprise Console JDBC parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Description (Optional)</td>
</tr>
<tr>
<td>Log Source Type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Database Type</td>
</tr>
<tr>
<td>Database Name</td>
</tr>
<tr>
<td>IP or Hostname</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>----------------------------</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Confirm Password</td>
</tr>
<tr>
<td>Authentication Domain</td>
</tr>
<tr>
<td>Database Instance</td>
</tr>
<tr>
<td>Predefined Query (Optional)</td>
</tr>
<tr>
<td>Table Name</td>
</tr>
<tr>
<td>Select List</td>
</tr>
<tr>
<td>Compare Field</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
</tr>
<tr>
<td>Start Date and Time</td>
</tr>
</tbody>
</table>
Table 553. Sophos Enterprise Console JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Type the polling interval, which 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.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td><strong>Use Named Pipe Communication</strong></td>
<td>If you did not select Use Microsoft JDBC, Use Named Pipe Communication is displayed. Clear the Use Named Pipe Communication check box. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database</td>
</tr>
<tr>
<td><strong>Database Cluster Name</strong></td>
<td>If you selected Use Named Pipe Communication, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.</td>
</tr>
<tr>
<td><strong>Use NTLMv2</strong></td>
<td>If you did not select Use Microsoft JDBC, Use NTLMv2 is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td><strong>Use Microsoft JDBC</strong></td>
<td>If you want to use the Microsoft JDBC driver, you must enable Use Microsoft JDBC.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>Select this option if your connection supports SSL. This option only appears for MSDE.</td>
</tr>
<tr>
<td><strong>Microsoft SQL Server Hostname</strong></td>
<td>If you selected Use Microsoft JDBC and Use SSL, the Microsoft SQL Server Hostname parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

**Note:** Selecting a value greater than 5 for the Credibility parameter weights your Sophos log source with a higher importance compared to other log sources in QRadar.

For more information about configuring the JDBC protocol, see `c_logsource_JDBCprotocol.dita`

6. Click **Save**.
7. On the **Admin** tab, click **Deploy Changes**.
Sophos PureMessage

The Sophos PureMessage DSM for IBM QRadar accepts events by using Java Database Connectivity (JDBC).

QRadar records all relevant quarantined email events. This document provides information about configuring QRadar to access the Sophos PureMessage database by using the JDBC protocol.

QRadar supports the following Sophos PureMessage versions:

- Sophos PureMessage for Microsoft Exchange - Stores events in a Microsoft SQL Server database that is specified as savexquar.
- Sophos PureMessage for Linux - Stores events in a PostgreSQL database that is specified as pmx_quarantine.

Here’s information on integrating QRadar with Sophos:

- “Integrating QRadar with Sophos PureMessage for Microsoft Exchange” on page 1026
- “Integrating QRadar with Sophos PureMessage for Linux” on page 1029

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4

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

Integrating QRadar with Sophos PureMessage for Microsoft Exchange

You can integrate QRadar with Sophos PureMessage for Microsoft Exchange.

Procedure

1. Log in to the Microsoft SQL Server command-line interface (CLI):

   ```
   osql -E -S localhost\sophos
   ```

2. Type which database you want to integrate with QRadar:

   ```
   use savexquar; go
   ```

3. Type the following command to create a SIEM view in your Sophos database to support QRadar:

   ```
   create view siem_view as select 
   'Windows PureMessage' as application, id, reason, 
   timecreated, emailonly as sender, filesize, subject, 
   messageid, filename from dbo.quaritems, 
   dbo.quaraddresses where ItemID = ID and Field = 76;
   ```

What to do next

After you create your SIEM view, you must configure QRadar to receive event information by using the JDBC protocol. To configure the Sophos PureMessage DSM with QRadar, see “Configuring QRadar to collect events from Sophos PureMessage by using the JDBC protocol” on page 1026.

Configuring QRadar to collect events from Sophos PureMessage by using the JDBC protocol

Configure IBM QRadar to collect events from the Sophos PureMessage for Microsoft Exchange database by using the JDBC protocol.

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. Configure the parameters. The following table describes the parameters that require specific values to collect event from Sophos PureMessage:

   **Note:** You must refer to the database configuration settings on your Sophos PureMessage device to define the parameters that are required to configure the Sophos PureMessage DSM in QRadar.

<table>
<thead>
<tr>
<th>Table 554. Sophos PureMessage JDBC parameters for Microsoft Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Description (Optional)</td>
</tr>
<tr>
<td>Log Source Type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
</tbody>
</table>
| Log Source Identifier | Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol.

   If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.

| Database Type | MSDE |
| Database Name | Type savexquar. |
| IP or Hostname | Type the IP address or host name of the Sophos PureMessage server. |
| Port | Type the port number used by the database server. The default port for MSDE is 1433. Sophos installations typically use 24033. You can confirm port usage by using the SQL Server Configuration Manager utility. For more information, see your vendor documentation.

   The JDBC configuration port must match the listener port of the Sophos database. The Sophos database must have incoming TCP connections enabled to communicate with QRadar.

   If you define a database instance in the **Database Instance** parameter, you must leave the **Port** parameter blank. You can only define a database instance if the database server uses the default port of 1433. This is not the standard Sophos configuration.

<p>| Username | Type the user name required to access the database. |
| Password | Type the password required to access the database. The password can be up to 255 characters in length. |
| Confirm Password | Confirm the password required to access the database. The confirmation password must be identical to the password entered in the <strong>Password</strong> parameter. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Domain</td>
<td>If you did not select Use Microsoft JDBC, Authentication Domain is displayed.</td>
</tr>
<tr>
<td></td>
<td>The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>The database instance, if required. MSDE databases can include multiple SQL server instances on one server.</td>
</tr>
<tr>
<td></td>
<td>When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the Database Instance parameter must be blank in the log source configuration.</td>
</tr>
<tr>
<td>Predefined Query (Optional)</td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the none option.</td>
</tr>
<tr>
<td>Table Name</td>
<td>Type siem_view as the name of the table or view that includes the event records.</td>
</tr>
<tr>
<td>Select List</td>
<td>Type * for all fields from the table or view.</td>
</tr>
<tr>
<td></td>
<td>You can use a comma-separated list to define specific fields from tables or views, if it is needed for your configuration. The list must contain the field that is defined in the Compare Field parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Type ID. The Compare Field parameter is used to identify new events added between queries to the table.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Select this check box to use prepared statements.</td>
</tr>
<tr>
<td></td>
<td>Prepared statements enable the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements.</td>
</tr>
<tr>
<td></td>
<td>Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
<tr>
<td>Start Date and Time (Optional)</td>
<td>Type the start date and time for database polling in the following format: 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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000.</td>
</tr>
</tbody>
</table>
Table 554. Sophos PureMessage JDBC parameters for Microsoft Exchange (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Named Pipe Communication</td>
<td>If you did not select Use Microsoft JDBC, Use Named Pipe Communication is displayed. Clear the Use Named Pipe Communication check box. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>If you selected 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 to ensure Named Pipe communication functions properly.</td>
</tr>
<tr>
<td>Use MTLMv2</td>
<td>If you did not select Use Microsoft JDBC, Use NTLMv2 is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable Use Microsoft JDBC.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option if your connection supports SSL. This option appears only for MSDE.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected Use Microsoft JDBC and Use SSL, the Microsoft SQL Server Hostname parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

Note: Selecting a value greater than 5 for the Credibility parameter weights your Sophos PureMessage log source with a higher importance compared to other log sources in QRadar.

For more information about configuring the JDBC protocol parameters, see c_logsource_JDBCprotocol.dita

6. Click Save.
7. On the Admin tab, click Deploy Changes.

Integrating QRadar with Sophos PureMessage for Linux

You can integrate IBM QRadar with Sophos PureMessage for Linux.

Procedure

1. Navigate to your Sophos PureMessage PostgreSQL database directory:
   ```
   cd /opt/pmx/postgres-8.3.3/bin
   ```
2. Access the pmx_quarantine database SQL prompt:
   ```
   ./psql -d pmx_quarantine
   ```
3. Type the following command to create a SIEM view in your Sophos database to support QRadar:

Chapter 139. Sophos 1029
create view siem_view as select 'Linux PureMessage' as application, id, b.name, m_date, h_from_local, h_from_domain, m_global_id, m_message_size, outbound, h_to, c_subject_utf8 from message a, m_reason b where a.reason_id = b.reason_id;

What to do next
After you create your database view, you must configure QRadar to receive event information by using the JDBC protocol.

Configuring a log source for Sophos PureMessage for Microsoft Exchange
You can configure IBM QRadar to access the Sophos PureMessage database using the JDBC protocol:

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources.
   The Data Sources pane is displayed.
4. Click the Log Sources icon.
   The Log Sources window is displayed.
5. Click Add.
   The Add a log source window is displayed.
6. From the Log Source Type list, select Sophos PureMessage.
7. From the Protocol Configuration list, select JDBC.

   Note: You must refer to the Configure Database Settings on your Sophos PureMessage to define the parameters required to configure the Sophos PureMessage DSM in QRadar.
8. Configure the following values:

<table>
<thead>
<tr>
<th>Sophos PureMessage JDBC parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
</tbody>
</table>
| Log Source Identifier | Type the identifier for the log source. Type the log source identifier in the following format:  
<Sophos PureMessage Database>@<Sophos PureMessage Database Server IP or Host Name>  
Where:  
• <Sophos PureMessage Database> is the database name, as entered in the Database Name parameter.  
• <Sophos PureMessage Database Server IP or Host Name> is the hostname or IP address for this log source, as entered in the IP or Hostname parameter.  
When defining a name for your log source identifier, you must use the values of the Database and Database Server IP address or host name of the Sophos PureMessage device. |
<p>| Database Type | From the list, select Postgres. |
| Database Name | Type pmx_quarantine. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP or Hostname</td>
<td>Type the IP address or host name of the Sophos PureMessage server.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number used by the database server. The default port is 1532. The JDBC configuration port must match the listener port of the Sophos database. The Sophos database must have incoming TCP connections enabled to communicate with QRadar.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name required to access the database.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password required to access the database. The password can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password required to access the database. The confirmation password must be identical to the password entered in the Password parameter.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>Optional. Type the database instance, if you have multiple SQL server instances on your database server.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Table Name</td>
<td>Type <code>siem_view</code> as the name of the table or view that includes the event records.</td>
</tr>
<tr>
<td>Select List</td>
<td>Type <code>*</code> for all fields from the table or view.</td>
</tr>
<tr>
<td></td>
<td>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. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Type <code>ID</code>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Compare Field</strong> parameter is used to identify new events added between queries to the table.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Select this check box to use prepared statements.</td>
</tr>
<tr>
<td></td>
<td>Prepared statements allows the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, we recommend that you use prepared statements.</td>
</tr>
<tr>
<td></td>
<td>Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.</td>
</tr>
</tbody>
</table>
Sophos PureMessage JDBC parameters
(continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start Date and Time</strong></td>
<td>Optional. Type the start date and time for database polling. The <strong>Start Date and Time</strong> parameter must be formatted as yyyy-MM-dd HH: mm with HH specified by using a 24-hour clock. If the <strong>Start Date and Time</strong> parameter is clear, polling begins immediately and repeats at the specified polling interval.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Type the polling interval, which 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 entered without an H or M poll in seconds.</td>
</tr>
</tbody>
</table>

**Note:** Selecting a value greater than 5 for the **Credibility** parameter weights your Sophos PureMessage log source with a higher importance compared to other log sources in QRadar.

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

**Sophos Astaro Security Gateway**

The Sophos Astaro Security Gateway DSM for IBM QRadar accepts events by using syslog, enabling QRadarto record all relevant events.

**About this task**

To configure syslog for Sophos Astaro Security Gateway:

**Procedure**

1. Log in to the Sophos Astaro Security Gateway console.
2. From the navigation menu, select **Logging > Settings**.
3. Click the **Remote Syslog Server** tab.
   The **Remote Syslog Status** window is displayed.
4. From **Syslog Servers** panel, click the + icon.
   The **Add Syslog Server** window is displayed.
5. Configure the following parameters:
   a) **Name** - Type a name for the syslog server.
   b) **Server** - Click the folder icon to add a pre-defined host, or click + and type in new network definition
   c) **Port** - Click the folder icon to add a pre-defined port, or click + and type in a new service definition. By default, QRadar communicates by using the syslog protocol on UDP/TCP port 514.
   d) Click Save.
6. From the **Remote syslog log selection** field, you must select check boxes for the following logs:
   a) **POP3 Proxy** - Select this check box.
   b) **Packet Filter** - Select this check box.
c) Packet Filter - Select this check box.

d) Intrusion Prevention System - Select this check box

e) Content Filter(HTTPS) - Select this check box.

f) High availability - Select this check box

g) FTP Proxy - Select this check box.

h) SSL VPN - Select this check box.

i) PPTP daemon - Select this check box.

j) IPSEC VPN - Select this check box.

k) HTTP daemon - Select this check box

l) User authentication daemon - Select this check box.

m) SMTP proxy - Select this check box.

n) Click Apply.

o) From Remote syslog status section, click Enable

You can now configure the log source in QRadar.

7. To configure QRadar to receive events from your Sophos Astaro Security Gateway device: From the Log Source Type list, select Sophos Astaro Security Gateway.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 4

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

Sophos Web Security Appliance

The Sophos Web Security Appliance (WSA) DSM for IBM QRadar accepts events using syslog.

About this task

QRadar records all relevant events forwarded from the transaction log of the Sophos Web Security Appliance. Before configuring QRadar, you must configure your Sophos WSA appliance to forward syslog events.

To configure your Sophos Web Security Appliance to forward syslog events:

Procedure

1. Log in to your Sophos Web Security Appliance.

2. From the menu, select Configuration > System > Alerts & Monitoring.

3. Select the Syslog tab.

4. Select the Enable syslog transfer of web traffic check box.

5. In the Hostname/IP text box, type the IP address or host name of QRadar.

6. In the Port text box, type 514.

7. From the Protocol list, select a protocol. The options are:

- TCP - The TCP protocol is supported with QRadar on port 514.

- UDP - The UDP protocol is supported with QRadar on port 514.

- TCP - Encrypted - TCP Encrypted is an unsupported protocol for QRadar.

8. Click Apply.

You can now configure the Sophos Web Security Appliance DSM in QRadar.
9. QRadar automatically detects syslog data from a Sophos Web Security Appliance. To manually configure QRadar to receive events from Sophos Web Security Appliance: From the Log Source Type list, select **Sophos Web Security Appliance**.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 140. Sourcefire Intrusion Sensor

The Sourcefire Intrusion Sensor DSM for IBM 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.
11. Click Apply.

What to do next

You are now ready to configure the log source in QRadar.

Configuring a log source for Sourcefire Intrusion Sensor in QRadar

QRadar automatically discovers and creates a log source for syslog events from Sourcefire Intrusion Sensor. However, you can manually create a log source for QRadar to receive syslog events. The following procedure is optional.

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 Snort Open Source IDS.
9. From the Protocol Configuration list, select Syslog.
10. Configure the remaining parameters.
11. Click Save.
12. On the Admin tab, click Deploy Changes.
Chapter 141. Splunk

IBM QRadar accepts and parses multiple event types that are forwarded from Splunk appliances. For Check Point events that are forwarded from Splunk, see Chapter 40, “Check Point,” on page 299.

Collect Windows events that are forwarded from Splunk

To collect events, you can configure your Windows end points to forward events to your QRadar Console and your Splunk indexer.

Forwarding Windows events from aggregation nodes in your Splunk deployment is not recommended. Use the Splunk forwarder to send Windows event data to IBM QRadar. Splunk indexers that forward events from multiple Windows end points to QRadar can obscure the true source of the events with the IP address of the Splunk indexer. To prevent a situation where an incorrect IP address association might occur in the log source, you can update your Windows end-point systems to forward to both the indexer and your QRadar Console.

Splunk events are parsed by using the Microsoft Windows Security Event Log DSM with the TCP multiline syslog protocol. The regular expression that is configured in the protocol defines where a Splunk event starts or ends in the event payload. The event pattern allows QRadar to assemble the raw Windows event payload as a single-line event that is readable by QRadar. The regular expression that is required to collect Windows events is outlined in the log source configuration.

To configure event collection for Splunk syslog events, you must complete the following tasks:

1. On your QRadar appliance, configure a log source to use the Microsoft Windows Security Event Log DSM.
   
   **Note:** You must configure 1 log source for Splunk events. QRadar can use the first log source to autodiscover more Windows end points.

2. On your Splunk appliance, configure each Splunk Forwarder on the Windows instance to send Windows event data to your QRadar Console or Event Collector.
   
   To configure a Splunk Forwarder, you must edit the props.conf, transforms.conf, and output.conf configuration files. For more information on event forwarding, see your Splunk documentation.

3. Ensure that no firewall rules block communication between your Splunk appliance and the QRadar Console or managed host that is responsible for retrieving events.

4. On your QRadar appliance, verify the Log Activity tab to ensure that the Splunk events are forwarded to QRadar.

Configuring a log source for Splunk forwarded events

To collect raw events that are forwarded from Splunk, you must configure a log source in IBM QRadar.

**Before you begin**

On your Splunk forwarder, you must set sendCookedData to false so that the forwarder sends raw data to 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. In the **Log Source Name** field, type a name for your log source.
7. Optional: In the **Log Source Description** field, type a description for your log source.
8. From the **Log Source Type** list, select Microsoft Windows **Security Event Log**.
9. From the **Protocol Configuration** list, select **TCP Multiline Syslog**.
10. Configure the following values:

<p>| Table 555. TCP multiline syslog protocol parameters |
|----------------------------------|----------------------------------|
| <strong>Parameter</strong>                   | <strong>Description</strong>                  |
| <strong>Protocol Configuration</strong>       | <strong>TCP Multiline Syslog</strong>         |
| <strong>Log Source Identifier</strong>        | Type the IP address or host name for the log source as an identifier for events from your Splunk appliance. The log source identifier must be unique value. |
| <strong>Listen Port</strong>                 | Type the port number that is used by QRadar to accept incoming TCP multi-line syslog events from Splunk. The default listen port is 12468. <strong>Important:</strong> Do not use listen port 514. The port number that you configure on QRadar must match the port number that is configured on the Splunk Forwarder. Every listen port in QRadar accepts up to 50 inbound Forwarder connections. If more Forwarder connections are necessary, create multiple Splunk Forwarder log sources on different ports. The connection limit refers to the number of forwarder connections and not the number of log sources that are coming in from each Forwarder connection. |
| <strong>Aggregation Method</strong>           | The default is <strong>Start/End Matching</strong>. If you want to combine multiline events that are joined by a common identifier, use <strong>ID-Linked</strong>. |
| <strong>Event Start Pattern</strong>          | Type the following regular expression (regex) to identify the start of your Splunk windows event: <code>(?:&lt;\d+&gt;|s?\w{3}\s?\d{2}\s?\d{2}:\d{2}:\d{2})\s?(\d{2}/\d{2}/\d{4}\s?\d{2}:\d{2}:\d{2} [AP]M)</code> The regular expression (regex) that is required to identify the start of a TCP multiline event payload. Syslog headers typically begin with a date or time stamp. The protocol can create a single-line event that is based on solely on an event start pattern, such as a time stamp. When only a start pattern is available, the protocol captures all the information between each start value to create a valid event. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Event End Pattern        | This parameter is available when you set the Aggregation Method parameter to **Start/End Matching**.  
This regular expression (regex) that is required to identify the end of a TCP multiline event payload. If the syslog event ends with the same value, you can use a regular expression to determine the end of an event. The protocol can capture events that are based solely on an event end pattern. When only an end pattern is available, the protocol captures all the information between each end value to create a valid event.                                                                                                                                                                                                                                                                                                                                                           |
| Message ID Pattern       | This parameter is available when you set the **Aggregation Method** parameter to **ID-Linked**.  
This regular expression (regex) that is required to filter the event payload messages. The TCP multiline event messages must contain a common identifying value that repeats on each line of the event message.                                                                                                                                                                                                                                                                                                                                                                             |
| Event Formatter           | Use the **Windows Multiline** option for multiline events that are formatted specifically for Windows.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Show Advanced Options    | The default is **No**. If you want to customize the event data, select **Yes**.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Use Custom Source Name   | This parameter is available when you set **Show Advanced Options** to **Yes**.  
Select the check box if you want to customize the source name with regex.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Source Name Regex         | This parameter is available when you check **Use Custom Source Name**.  
The regular expression (regex) that captures one or more values from event payloads that are handled by this protocol. These values are used along with the **Source Name Formatting String** parameter to set a source or origin value for each event. This source value is used to route the event to a log source with a matching Log Source Identifier value.                                                                                                                                                                                                                                                                                                                                                                           |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Source Name Formatting String              | This parameter is available when you check **Use Custom Source Name**. You can use a combination of one or more of the following inputs to form a source value for event payloads that are processed by this protocol:  
• One or more capture groups from the **Source Name Regex**. To refer to a capture group, use \x notation where x is the index of a capture group from the **Source Name Regex**.  
• The IP address where the event data originated from. To refer to the packet IP, use the token $PIP$.  
• Literal text characters. The entire **Source Name Formatting String** can be user-provided text. For example, if the **Source Name Regex** is 'hostname=(.*?)' and you want to append hostname.com to the capture group 1 value, set the **Source Name Formatting String** to \1.hostname.com. If an event is processed that contains hostname=ibm, then the event payload's source value is set to ibm.hostname.com, and QRadar routes the event to a log source with that **Log Source Identifier**. |
| Use as a Gateway Log Source                | This parameter is available when you set **Show Advanced Options** to **Yes**. When selected, events that flow through the log source can be routed to other log sources, based on the source name tagged on the events. When this option is not selected and **Use Custom Source Name** is not checked, incoming events are tagged with a source name that corresponds to the **Log Source Identifier** parameter. |
| Flatten Multiline Events into Single Line  | This parameter is available when you set **Show Advanced Options** to **Yes**. Shows an event in one single line or multiple lines.                                                                                                                                                                                                                       |
| Retain Entire Lines during Event Aggregation | This parameter is available when you set **Show Advanced Options** to **Yes**. If you set the **Aggregation Method** parameter to **ID-Linked**, you can enable **Retain Entire Lines during Event Aggregation** to either discard or keep the part of the events that comes before **Message ID Pattern** when events are concatenated with the same ID pattern together. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
13. Optional: If you have 50 or more Windows sources, you must repeat this process to create another log source.

Events that are provided by the Splunk Forwarder to QRadar are displayed on the **Log Activity** tab.
Chapter 142. Squid Web Proxy

The Squid Web Proxy DSM for IBM QRadar records all cache and access log events by using syslog.

To integrate QRadar with Squid Web Proxy, you must configure your Squid Web Proxy to forward your cache and access logs by using syslog.

Configuring syslog forwarding

You can configure Squid to use syslog to forward your access and cache events.

Procedure

1. Use SSH to log in to the Squid device command line interface.
2. Open the following file:
   `/etc/rc3.d/S99local`
   **Note:** If `/etc/rc3.d/S99local` does not exist, use `/etc/rc.d/rc.local`.
3. Add the following line:
   ```
   tail -f /var/log/squid/access.log | logger -p <facility>.<priority> &
   ```
   • `<facility>` is any valid syslog facility, which is written in lowercase such as authpriv, daemon, local0 to local7, or user.
   • `<priority>` is any valid priority that is written in lowercase such as err, warning, notice, info, debug.
4. Save and close the file.
   Logging begins the next time that the system is restarted.
5. To begin logging immediately, type the following command:
   ```
   nohup tail -f /var/log/squid/access.log | logger -p <facility>.<priority> &
   ```
   The `<facility>` and `<priority>` options are the same values that you entered.
6. Open the following file:
   `/etc/syslog.conf`
   **Note:** When using rsyslog, open `/etc/rsyslog.conf` instead of `/etc/syslog.conf`.
7. Add the following line to send the logs to QRadar:
   ```
   <priority>.<facility> @<QRadar_IP_address>
   ```
   The following example shows a priority and facility for Squid messages and a QRadar IP address:
   ```
   info.local4 @<IP_address>
   ```
8. Confirm that access_log format ends in common.

Example:

<table>
<thead>
<tr>
<th>access_log /path/to/access.log common</th>
</tr>
</thead>
</table>

If the access_log format end value is squid, change squid to common, as displayed in the example.

If the access_log format does not have an ending value, add the following line to the Squid.conf file to turn on httpd log file emulation:

| emulate_httpd_log on |
9. Choose one of the following options:
   • To restart the Squid service, type the following command:

     ```
     service squid restart
     ```
   • To reload the configuration without restarting the service, type the following command:

     ```
     /usr/sbin/squid -k reconfigure
     ```

10. Save and close the file.

11. Type the following command to restart the syslog daemon:

    ```
    /etc/init.d/syslog restart
    ```

    For more information about configuring Squid, see your vendor documentation.

**Results**

After you configure syslog forwarding for your cache and access logs, the configuration is complete. QRadar can automatically discover syslog events that are forwarded from Squid.

---

### Create a log source

IBM QRadar automatically discovers and creates a log source for syslog events forwarded from Squid Web Proxy appliances. These configuration steps for creating a log source are optional.

**About this task**

To manually configure a log source for Squid Web Proxy:

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   
   The **Data Sources** pane is displayed.
4. Click the **Log Sources** icon.
   
   The **Log Sources** window is displayed.
5. Click **Add**.
   
   The Add a log source window is displayed.
6. In the **Log Source Name** field, type a name for the log source.
7. In the **Log Source Description** field, type a description for the log source.
8. From the **Log Source Type** list, select **Squid Web Proxy**.
9. From the **Protocol Configuration** list, select **Syslog**.
   
   The syslog protocol configuration is displayed.
10. Configure the following values:

    | Parameter             | Description                                                                 |
    |-----------------------|-----------------------------------------------------------------------------|
    | **Log Source Identifier** | Type the IP address or host name for the log source as an identifier for events from the Squid Web Proxy. |

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.
Chapter 143. SSH CryptoAuditor

The IBM QRadar DSM for SSH CryptoAuditor collects logs from an SSH CryptoAuditor.

The following table identifies the specifications for the SSH CryptoAuditor DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>SSH Communications Security</td>
</tr>
<tr>
<td>Product</td>
<td>CryptoAuditor</td>
</tr>
<tr>
<td>DSM Name</td>
<td>SSH CryptoAuditor</td>
</tr>
<tr>
<td>RPM filename</td>
<td>DSM-SSHCryptoAuditor-QRadar_release-Build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>1.4.0 or later</td>
</tr>
<tr>
<td>Event format</td>
<td>Syslog</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Audit, Forensics</td>
</tr>
<tr>
<td>Log source type in QRadar UI</td>
<td>SSH CryptoAuditor</td>
</tr>
<tr>
<td>Auto discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>SSH Communications Security website (<a href="http://www.ssh.com/">http://www.ssh.com/</a>)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>SSH CryptoAuditor</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks
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 QRadar.

Adding a DSM
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 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.
The Starent Networks DSM for IBM QRadar accepts Event, Trace, Active, and Monitor events.

**About this task**

Before you configure a Starent Networks device in QRadar, you must configure your Starent Networks device to forward syslog events to QRadar.

To configure the device to send syslog events to QRadar:

**Procedure**

1. Log in to your Starent Networks device.
2. Configure the syslog server:

   ```
   logging syslog <IP address> [facility <facilities>] [<rate value>] [pdu-verbosity <pdu_level>] [pdu-data <format>] [event-verbosity <event_level>]
   ```

   The following table provides the necessary parameters:

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog &lt;IP address&gt;</td>
<td>Type the IP address of your QRadar</td>
</tr>
<tr>
<td>facility &lt;facilities&gt;</td>
<td>Type the local facility for which the logging options are applied. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>• local0</td>
</tr>
<tr>
<td></td>
<td>• local1</td>
</tr>
<tr>
<td></td>
<td>• local2</td>
</tr>
<tr>
<td></td>
<td>• local3</td>
</tr>
<tr>
<td></td>
<td>• local4</td>
</tr>
<tr>
<td></td>
<td>• local5</td>
</tr>
<tr>
<td></td>
<td>• local6</td>
</tr>
<tr>
<td></td>
<td>• local7</td>
</tr>
<tr>
<td></td>
<td>The default is local7.</td>
</tr>
<tr>
<td>rate value</td>
<td>Type the rate that you want log entries to be sent to the system log server.</td>
</tr>
<tr>
<td></td>
<td>This value must be an integer 0 - 100000. The default is 1000 events per second.</td>
</tr>
<tr>
<td>pdu-verbosity &lt;pdu_level&gt;</td>
<td>Type the level of verboseness you want to use in logging the Protocol Data Units (PDUs). The range is 1 - 5 where 5 is the most detailed. This parameter affects only protocol logs.</td>
</tr>
</tbody>
</table>
Table 558. Syslog server parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| pdu-data <format> | Type the output format for the PDU when logged as one of following formats:  
  • none - Displays results in raw or unformatted text.  
  • hex - Displays results in hexadecimal format.  
  • hex-ascii - Displays results in hexadecimal and ASCII format similar to a main frame dump. |
| event-verbosity <event_level> | Type the level of detail you want to use in logging of events, that includes:  
  • min - Provides minimal information about the event, such as, event name, facility, event ID, severity level, data, and time.  
  • concise - Provides detailed information about the event, but does not provide the event source.  
  • full - Provides detailed information about the event and includes the source information that identifies the task or subsystem that generated the event. |

3. From the root prompt for the Exec mode, identify the session for which the trace log is to be generated:

   `logging trace {callid <call_id> | ipaddr <IP address> | msid <ms_id> | name <username>}`

The following table provides the necessary parameters:

Table 559. Trace log parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callid &lt;call_id&gt;</td>
<td>Indicates a trace log is generated for a session that is identified by the call identification number. This value is a 4-byte hexadecimal number.</td>
</tr>
<tr>
<td>ipaddr &lt;IP address&gt;</td>
<td>Indicates a trace log is generated for a session that is identified by the specified IP address.</td>
</tr>
<tr>
<td>msid &lt;ms_id&gt;</td>
<td>Indicates a trace log is generated for a session that is identified by the mobile station identification (MSID) number. This value must be 7 - 16 digits, which are specified as an IMSI, MIN, or RMI.</td>
</tr>
<tr>
<td>name &lt;username&gt;</td>
<td>Indicates a trace log is generated for a session that is identified by the username. This value is the name of the subscriber that was previously configured.</td>
</tr>
</tbody>
</table>

4. To write active logs to the active memory buffer, in the config mode:

   `logging runtime buffer store all-events`

5. Configure a filter for the active logs:

   `logging filter active facility <facility> level <report_level> [critical-info | no-critical-info]`

The following table provides the necessary parameters:
### Table 560. Active log parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| facility <facility> | Type the facility message level. A facility is a protocol or task that is in use by the system. The local facility defines which logging options are applied for processes that run locally. The options are as follows:  
  • local0  
  • local1  
  • local2  
  • local3  
  • local4  
  • local5  
  • local6  
  • local7  
  The default is local7. |
| level <report_level> | Type the log severity level, including:  
  • critical - Logs only those events that indicate a serious error is occurring and that is causing the system or a system component to cease functioning. Critical is the highest level severity.  
  • error - Logs events that indicate an error is occurring that is causing the system or a system component to operate in a degraded state. This level also logs events with a higher severity level.  
  • warning - Logs events that can indicate a potential problem. This level also logs events with a higher severity level.  
  • unusual - Logs events that are unusual and might need to be investigated. This level also logs events with a higher severity level.  
  • info - Logs informational events and events with a higher severity level.  
  • debug - Logs all events regardless of the severity.  
  It is suggested that a level of error or critical can be configured to maximize the value of the logged information and lower the quantity of logs that are generated. |
| critical-info | The critical-info parameter identifies and displays events with a category attribute of critical information. Examples of these types of events can be seen at bootup when system processes or tasks are being initiated. |
| no-critical-info | The no-critical-info parameter specifies that events with a category attribute of critical information are not displayed. |

6. Configure the monitor log targets:  

   logging monitor {msid <ms_id>|username <username>}

   The following table provides the necessary parameters:
Table 561. Monitor log parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msid &lt;md_id&gt;</td>
<td>Type an msid to define that a monitor log is generated for a session that is identified by using the Mobile Station Identification (MDID) number. This value must be 7 - 16 digits that are specified as a IMSI, MIN, or RMI.</td>
</tr>
<tr>
<td>username &lt;username&gt;</td>
<td>Type user name to identify a monitor log generated for a session by the user name. The user name is the name of the subscriber that was previously configured.</td>
</tr>
</tbody>
</table>

7. You are now ready to configure the log source in QRadar.

To configure QRadar to receive events from a Starent device:

a) From the Log Source Type list, select the Starent Networks Home Agent (HA) option.

For more information about the device, see your vendor documentation.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4

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 145. STEALTHbits

IBM QRadar supports a range of STEALTHbits DSMs.

STEALTHbits StealthINTERCEPT

The IBM QRadar DSM for STEALTHbits StealthINTERCEPT can collect event logs from your STEALTHbits StealthINTERCEPT and File Activity Monitor services.

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>STEALTHbits Technologies</td>
</tr>
<tr>
<td>DSM</td>
<td>STEALTHbits StealthINTERCEPT</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-STEALTHbitsStealthINTERCEPT-QRadar_Version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>3.3</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>Active Directory Audit Events, File Activity Monitor Events</td>
</tr>
<tr>
<td>Automatically discovered</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td><a href="http://www.stealthbits.com/resources">http://www.stealthbits.com/resources</a></td>
</tr>
</tbody>
</table>

Configuring a STEALTHbits StealthINTERCEPT log source in IBM QRadar

To collect STEALTHbits StealthINTERCEPT events, configure a log source in QRadar.

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. In the navigation pane, 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**.

**Configuring your STEALTHbits StealthINTERCEPT to communicate with QRadar**

To collect all audit logs and system events from STEALTHbits StealthINTERCEPT, you must specify IBM 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:

<table>
<thead>
<tr>
<th>Table 563. Syslog parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Host Address</td>
</tr>
<tr>
<td>Port</td>
</tr>
</tbody>
</table>

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.
   
   Leave the **Send to Events DB** check box selected. StealthINTERCEPT uses the events database to generate reports.
10. Click **Add**.

**Configuring your STEALTHbits File Activity Monitor to communicate with QRadar**

To collect events from STEALTHbits File Activity Monitor, you must specify IBM QRadar as the Syslog server and configure the message format.

**Procedure**

1. Log in to the server that runs STEALTHbits File Activity Monitor.
2. Select the **Monitored Hosts** tab.
3. Select a monitored host and click **Edit** to open the host's properties window.
4. Select the Syslog tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bulk Syslog server in SERVER[:PORT] format</strong></td>
<td><code>&lt;QRadar event collector IP address&gt;:514</code>&lt;br&gt;Example: <code>192.0.2.1:514</code>&lt;br&gt;<code>&lt;qradarhostname&gt;:514</code></td>
</tr>
<tr>
<td><strong>Syslog message template file path</strong></td>
<td><code>SyslogLeefTemplate.txt</code>&lt;br&gt;The template is stored in the STEALTHbits File Activity Monitor Install Directory</td>
</tr>
</tbody>
</table>

5. Click **OK**.
Configuring a log source for STEALTHbits File Activity Monitor in QRadar

To collect STEALTHbits File Activity Monitor events, configure a STEALTHbits StealthINTERCEPT log source in QRadar.

**Procedure**

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the navigation pane, 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**.

The following table provides a sample event message for the STEALTHbits StealthINTERCEPT DSM:

<table>
<thead>
<tr>
<th>Table 564. STEALTHbits StealthINTERCEPT and STEALTHbits File Activity Monitor sample event message supported by the STEALTHbits StealthINTERCEPT DSM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Event name</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
</tbody>
</table>
| Active Directory Group Created | Group Added | LEEF:1.0|STEALTHbits
| | | [StealthINTERCEPT]
| | | <IP_address>| Active Directory group Object Added|TrueFalse|
| | | cat=Object Added devTimeFormat=yyyy-MM-dd HH:mm:ss.SSS
| | | devTime=2013-10-24 15:41:38.387
| | | SettingName=All AD Changes
| | | domain=<Domain>
| | | usrName=CN=Administrator,
| | | CN=Users,
| | | DC=<Domain_controller>,
| | | DC=com
| | | src=LDAP: [<Source_IPv6_address]:6084
| | | 3
| | | DistinguishedName= cn=asdfsdfasdfsdf,
| | | OU=<City>,
| | | OU=<State>,
| | | DC=<Domain_controller>,
| | | DC=com
| | | className=group
| | | OrigServer=<Server>
| | | Success=True Blocked=False
| | | AttNames=
| | | AttNewValues=
| | | AttOldValues= |
Table 564. STEALTHbits StealthINTERCEPT and STEALTHbits File Activity Monitor sample event message supported by the STEALTHbits StealthINTERCEPT DSM (continued)

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows File System Folder or File Delete</td>
<td>File Deleted</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>

STEALTHbits StealthINTERCEPT Alerts

IBM 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 565. STEALTHbits StealthINTERCEPT Alerts DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>STEALTHbits Technologies</td>
</tr>
<tr>
<td>DSM name</td>
<td>STEALTHbits StealthINTERCEPT Alerts</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-STEALTHbitsStealthINTERCEPTAlerts-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>3.3</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Active Directory Alerts Events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>StealthINTERCEPT (<a href="http://www.stealthbits.com/products/stealthintercept">http://www.stealthbits.com/products/stealthintercept</a>)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>STEALTHbits StealthINTERCEPT Alerts</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Related tasks**
- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>The IP address of the QRadar Console</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
</tbody>
</table>

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**.
STEALTHbits StealthINTERCEPT Analytics

IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>STEALTHbits Technologies</td>
</tr>
<tr>
<td>DSM name</td>
<td>STEALTHbits StealthINTERCEPT Analytics</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-STEALTHbitsStealthINTERCEPTAnalytics-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>3.3</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Active Directory Analytics Events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>StealthINTERCEPT (<a href="http://www.stealthbits.com/products/stealthintercept">http://www.stealthbits.com/products/stealthintercept</a>)</td>
</tr>
</tbody>
</table>

Integrate STEALTHbits StealthINTERCEPT with QRadar by completing 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 in the order that they are listed:
   - 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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>STEALTHbits StealthINTERCEPT Analytics</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks

“Adding a DSM” on page 4
“Collecting analytics logs from STEALTHbits StealthINTERCEPT” on page 1057

To collect all analytics logs from STEALTHbits StealthINTERCEPT, you must specify IBM QRadar as the syslog server and configure the message format.

“Adding a log source” on page 4
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 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>The IP address of the QRadar Console</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
</tbody>
</table>

5. Click Import mapping file.
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 146. Sun

IBM QRadar supports a range of Sun DSMs.

Sun ONE LDAP

The Sun ONE LDAP DSM for QRadar accepts multiline UDP access and LDAP events from Sun ONE Directory Servers.

Sun ONE LDLAP is known as Oracle Directory Server.

QRadar retrieves access and LDAP events from Sun ONE Directory Servers by connecting to each server to download the event log. The event file must be written to a location accessible by the log file protocol of QRadar with FTP, SFTP, or SCP. The event log is written in a multiline event format, which requires a special event generator in the log file protocol to properly parse the event. The ID-Linked Multiline event generator is capable of using regex to assemble multiline events for QRadar when each line of a multiline event shares a common starting value.

The Sun ONE LDAP DSM also can accept events streamed using the UDP Multiline Syslog protocol. However, in most situations your system requires a 3rd party syslog forwarder to forward the event log to QRadar. This can require you to redirect traffic on your QRadar Console to use the port defined by the UDP Multiline protocol.

Related concepts
“UDP multiline syslog protocol configuration options” on page 96
To create a single-line syslog event from a multiline event, configure a log source to use the UDP multiline protocol. The UDP multiline syslog protocol uses a regular expression to identify and reassemble the multiline syslog messages into single event payload.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Enabling the event log for Sun ONE Directory Server

To collect events from your Sun ONE Directory Server, you must enable the event log to write events to a file.

Procedure
1. Log in to your Sun ONE Directory Server console.
2. Click the Configuration tab.
3. From the navigation menu, select Logs.
4. Click the Access Log tab.
5. Select the Enable Logging check box.
6. Type or click Browse to identify the directory path for your Sun ONE Directory Server access logs.
7. Click Save.

What to do next
You are now ready to configure a log source in QRadar.
Configuring a log source for Sun ONE LDAP

To receive events, you must manually create a log source for your Sun ONE Directory Server. QRadar does not automatically discover log file protocol events.

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 Name field, type a name for your log source.
7. In the Log Source Description field, type a description for your log source.
8. From the Log Source Type list box, select Sun ONE LDAP.
9. From the Protocol Configuration list box, select Log File.
10. From the Event Generator list box, select ID-Linked Multiline.
11. In the Message ID Pattern field, type conn=(\d+) as the regular expression that defines your multiline events.
12. Configure the following log file protocol parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type an IP address, host name, or name to identify the event source. IP addresses or host names enable QRadar to identify a log file to a unique event source. For example, if your network contains multiple devices, such as a management console or a file repository, specify the IP address or host name of the device that created the event. This enables events to be identified at the device level in your network, instead of identifying the event for the management console or file repository.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535. The options include: FTP TCP Port 21. SFTP TCP Port 22. SCP TCP Port 22. Important: 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.</td>
</tr>
<tr>
<td>Remote User</td>
<td>Type the user name necessary to log in to the host that contains your event files. The user name can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password necessary to log in to the host.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>If you select SCP or SFTP as the Service Type, this parameter enables you to define an SSH private key file. When you provide an SSH Key File, the Remote Password field is ignored.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Important:</strong></td>
<td>For FTP only. If your log files are 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.</td>
</tr>
<tr>
<td>Recursive</td>
<td>Enable this check box to allow FTP or SFTP connections to recursively search sub folders of the remote directory for event data. Data that is collected from sub folders depends on matches to the regular expression in the FTP File Pattern. The Recursive option is not available for SCP connections.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>If you select SFTP or FTP as the Service Type, this option enables 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. For example, if you want to list all files that start with the word log, followed by one or more digits and ending with tar.gz, use the following entry: log[0-9]+.tar.gz. Use of this parameter requires knowledge of regular expressions (regex). For more information about regular expressions, see the Oracle website (<a href="http://docs.oracle.com/javase/tutorial/essential/regex/">http://docs.oracle.com/javase/tutorial/essential/regex/</a>)</td>
</tr>
<tr>
<td>FTP Transfer Mode</td>
<td>This option only appears if you select FTP as the Service Type. The FTP Transfer Mode parameter enables you to define the file transfer mode when you retrieve log files over FTP. From the list box, select the transfer mode that you want to apply to this log source: <strong>Binary</strong> Select Binary for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files. <strong>ASCII</strong> Select ASCII for log sources that require an ASCII FTP file transfer. Important: You must select NONE for the Processor parameter and LINEBYLINE the Event Generator parameter when you use ASCII as the FTP Transfer Mode.</td>
</tr>
<tr>
<td>SCP Remote File</td>
<td>If you select SCP as the Service Type you must type the file name of the remote file.</td>
</tr>
<tr>
<td>Start Time</td>
<td>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.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>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, 2H if you want the directory to be scanned every 2 hours. The default is 1H.</td>
</tr>
<tr>
<td>Run On Save</td>
<td>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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Processor</strong></td>
<td>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 to be processed.</td>
</tr>
<tr>
<td><strong>Ignore Previously Processed File(s)</strong></td>
<td>Select this check box to track files that were processed and you do not want the files to be processed a second time. This only applies to FTP and SFTP Service Types.</td>
</tr>
<tr>
<td><strong>Change Local Directory?</strong></td>
<td>Select this check box to define the local directory on your QRadar that you want to use for storing downloaded files during processing. Most configurations can leave this check box clear. When you select the check box, the <strong>Local Directory</strong> field is displayed, which enables you to configure a local directory to use for temporarily storing files.</td>
</tr>
<tr>
<td><strong>Event Generator</strong></td>
<td>Select <strong>ID-Linked Multiline</strong> to process to the retrieved event log as multiline events. The ID-Linked Multiline format processes multiline event logs that contain a common value at the start of each line in a multiline event message. This option displays the <strong>Message ID Pattern</strong> field that uses regex to identify and reassemble the multiline event in to single event payload.</td>
</tr>
<tr>
<td><strong>Folder Separator</strong></td>
<td>Type the character that is used to separate folders for your operating system. The default value is <code>/</code>. Most configurations can use the default value in the <strong>Folder Separator</strong> field. This field is only used by operating systems that use an alternate character to define separate folders. For example, periods that separate folders on mainframe systems.</td>
</tr>
</tbody>
</table>

13. Click **Save**.

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

**Configuring a UDP Multiline Syslog log source**

To collect syslog events, you must configure a log source for Sun ONE LDAP to use the UDP Multiline Syslog 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 log source.
5. From the **Log Source Type** list, select **Sun ONE LDAP**.
6. From the **Protocol Configuration** list, select **UDP Multiline Syslog**.
7. Configure the following values:

<table>
<thead>
<tr>
<th>Table 569. Sun ONE LDAP UDP Multiline Syslog log source parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Log Source Identifier</strong></td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td><strong>Listen Port</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Message ID Pattern</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
</tr>
</tbody>
</table>

8. Click **Save**.

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

**Configuring IPtables for UDP Multiline Syslog events**

You might be unable to send events directly to the standard UDP Multiline port 517 or any unused available ports when you collect UDP Multiline Syslog events in IBM QRadar. If this error occurs, then you must redirect events from port 514 to the default port 517 or your chosen alternative port by using IPTables. You must configure IPtables on your QRadar Console or for each QRadar Event Collector that receives UDP Multiline Syslog events from an SunOne LDAP server. Then, you must complete the configuration for each SunOne LDAP server IP address that you want to receive logs from.
Before you begin

Important: Complete this configuration method when you can't send UDP Multiline Syslog events directly to the chosen UDP Multiline port on QRadar from your SunOne LDAP server. Also, you must complete this configuration when you are restricted to send only to the standard syslog port 514.

Procedure

1. Using SSH, log in to QRadar as the root user.
   - Login: root
   - Password: password

2. Type the following command to edit the IPtables file:
   - vi /opt/qradar/conf/iptables-nat.post
   The IPtables NAT configuration file is displayed.

3. Type the following command to instruct QRadar to redirect syslog events from UDP port 514 to UDP port 517:
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port <new-port> -s <IP address>

   Where:
   - IP address is the IP address of your SunOne LDAP server.
   - New port is the port number that is configured in the UDP Multiline protocol for SunOne LDAP.

   You must include a redirect for each SunOne LDAP IP address that sends events to your QRadar Console or Event Collector. Example:
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s <IP_address>

4. Save your IPtables NAT configuration.

   You are now ready to configure IPtables on your QRadar Console or Event Collector to accept events from your SunOne LDAP servers.

5. Type the following command to edit the IPtables file:
   - vi /opt/qradar/conf/iptables.post
   The IPtables configuration file is displayed.

6. Type the following command to instruct QRadar to allow communication from your SunOne LDAP servers:
   -I QChain 1 -m udp -p udp --src <IP_address> --dport <New port> -j ACCEPT

   Where:
   - IP address is the IP address of your SunOne LDAP server.
   - New port is the port number that is configured in the UDP Multiline protocol for SunOne LDAP.

   You must include a redirect for each SunOne LDAP IP address that sends events to your QRadar Console or Event Collector. Example:
   -I QChain 1 -m udp -p udp --src <IP_address> --dport 517 -j ACCEPT

7. Type the following command to update IPtables in QRadar:
   ./opt/qradar/bin/iptables_update.pl
**Example**

If you need to configure another QRadar Console or Event Collector that receives syslog events from an SunOne LDAP server, repeat these steps.

**What to do next**

Configure your SunOne LDAP server to forward events to QRadar.

## Sun Solaris DHCP

IBM QRadar automatically discovers and creates a log source for syslog events from Sun Solaris DHCP installations.

**About this task**

The following configuration steps are optional.

**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 Authentication Messages.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from Sun Solaris installations. Each additional log source that you create when you have multiple installations ideally includes a unique identifier, such as an IP address or host name.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The log source is added to IBM QRadar. Events that are forwarded to QRadar by Solaris Sendmail is displayed on the Log Activity tab.

## Configuring Sun Solaris DHCP

The Sun Solaris DHCP DSM for IBM QRadar records all relevant DHCP events by using syslog.

**About this task**

To collect events from Sun Solaris DHCP, you must configure syslog to forward events to QRadar.

**Procedure**

1. Log in to the Sun Solaris command-line interface.
2. Edit the `/etc/default/dhcp` file.
3. Enable logging of DHCP transactions to syslog by adding the following line:
   ```
   LOGGING_FACILITY=X
   ```
   Where X is the number corresponding to a local syslog facility, for example, a number 0 - 7.
4. Save and exit the file.
5. Edit the `/etc/syslog.conf` file.
6. To forward system authentication logs to QRadar, add the following line to the file:
   ```
   localX.notice @<IP address>
   ```
   Where:
   - X is the logging facility number that you specified in “Configuring Sun Solaris DHCP” on page 1065.
   - `<IP address>` is the IP address of your QRadar. Use tabs instead of spaces to format the line.
7. Save and exit the file.
8. Type the following command:
   ```
   kill -HUP `cat /etc/syslog.pid`
   ```

**What to do next**

You are now ready to configure the log source in QRadar.

### Configuring Sun Solaris

The Sun Solaris DSM for IBM QRadar records all relevant Solaris authentication events by using syslog.

**About this task**

To collect authentication events from Sun Solaris, you must configure syslog to forward events to IBM 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:
   ```
   *.err;authnotice;auth.info@<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 more 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`
   ```

**What to do next**

You are now ready to configure the log source QRadar.

**Note:** If a Linux log source is created for the Solaris system that is sending events, disable the Linux log source, and then adjust the parsing order. Ensure that the Solaris DSM is listed first.
### Sun Solaris Sendmail

The Sun Solaris Sendmail DSM for IBM QRadar accepts Solaris authentication events by 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 more 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 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.

#### 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. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:
Table 571. Syslog parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from Sun Solaris Sendmail installations. Each additional log source that you create when you have multiple installations ideally includes a unique identifier, such as an IP address or host name.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The log source is added to QRadar. Events that are forwarded to QRadar by Solaris Sendmail are displayed on the **Log Activity** tab.

### Sun Solaris Basic Security Mode (BSM)

Sun Solaris Basic Security Mode (BSM) is an audit tracking tool for the system administrator to retrieve detailed auditing events from Sun Solaris systems.

IBM QRadar retrieves Sun Solaris BSM events by using the log file Protocol. For you to configure QRadar to integrate with Solaris Basic Security Mode, take the following steps:

1. Enable Solaris Basic Security Mode.
2. Convert audit logs from binary to a human-readable format.
3. Schedule a cron job to run the conversion script on a schedule.
4. Collect Sun Solaris events in QRadar by using the log file protocol.

### Enabling Basic Security Mode in Solaris 10

To configure Sun Solaris BSM in Solaris 10, you must enable Solaris Basic Security Mode and configure the classes of events the system logs to an audit log file.

#### About this task

Configure Basic Security Mode and enable auditing in Sun Solaris 10.

#### Procedure

1. Log in to your Solaris console as a superuser or root user.
2. Enable single-user mode on your Solaris console.
3. Type the following command to run the bsmconv script and enable auditing:
   ```sh
   /etc/security/bsmconv
   ```
   The bsmconv script enables Solaris Basic Security Mode and starts the auditing service auditd.
4. Type the following command to open the audit control log for editing:
   ```sh
   vi /etc/security/audit_control
   ```
5. Edit the audit control file to contain the following information:
   ```sh
   dir:/var/audit flags:lo,ad,ex,-fw,-fc,-fd,-fr naflags:lo,ad
   ```
6. Save the changes to the audit_control file, and then reboot the Solaris console to start auditd.
7. Type the following command to verify that auditd starts:
   ```sh
   /usr/sbin/auditconfig -getcond
   ```
   If the auditd process is started, the following string is returned:
**What to do next**

You can now convert the binary Solaris Basic Security Mode logs to a human-readable log format.

---

**Enabling Basic Security Mode in Solaris 11**

To configure Sun Solaris BSM in Solaris 11, you must enable Solaris Basic Security Mode and configure the classes of events the system logs to an audit log file.

**Procedure**

1. Log in to Solaris 11 console as a superuser or root.
2. Start the audit service by typing the following command:
   ```
   audit -s
   ```
3. Set up the attributable classes by typing the following command:
   ```
   auditconfig -setflags lo,ps-fw
   ```
4. Set up the non-attributable classes by typing the following command:
   ```
   auditconfig -setnaflags lo,na
   ```
5. To verify that audit service starts, type the following command:
   ```
   /usr/sbin/auditconfig -getcond
   ```
   If the `auditd` process is started, the following string is returned:
   ```
   audit condition = auditing
   ```

---

**Converting Sun Solaris BSM audit logs**

IBM QRadar cannot process binary files directly from Sun Solaris BSM. You must convert the audit log from the existing binary format to a human-readable log format by using `praudit` before the audit log data can be retrieved by QRadar.

**Procedure**

1. Type the following command to create a new script on your Sun Solaris console:
   ```
   vi /etc/security/newauditlog.sh
   ```
2. Add the following information to the `newauditlog.sh` script:
   ```bash
   #!/bin/bash
   # newauditlog.sh - Start a new audit file and expire the old logs
   AUDIT_EXPIRE=30
   AUDIT_DIR="/var/audit"
   LOG_DIR="/var/log/"
   
   /usr/sbin/audit -n cd $AUDIT_DIR # in case it is a link #
   
   FILES=$(ls -lrt | tr -s " " | cut -d " " -f9 | grep -v "not_terminated")
   
   lastFile="" for file in $FILES; do
     lastFile=$file
   done
   
   # Extract a human-readable file from the binary log file
   echo "Beginning praudit of $lastFile"
   ```

---

*Chapter 146. Sun* 1069
```
praudit -l $lastFile > "$LOG_DIR$lastFile.log" echo "Done praudit, creating log file at: $LOG_DIR$lastFile.log"
```

```bash
/usr/bin/find . $AUDIT_DIR -type f -mtime +$AUDIT_EXPIRE \ -exec rm {} > /dev/null 2>&1 \;
```

```
# End script
The script outputs log files in the <starttime>.<endtime>.<hostname>.log format.

For example, the log directory in /var/log would contain a file with the following name:
```
20111026030000.20111027030000.qasparc10.log
```

3. Optional: Edit the script to change the default directory for the log files.
   a) AUDIT_DIR="/var/audit" - The Audit directory must match the location that is specified by the audit control file you configured in “Enabling Basic Security Mode in Solaris 10” on page 1068.

4. LOG_DIR="/var/log/" - The log directory is the location of the human-readable log files of your Sun Solaris system that are ready to be retrieved by QRadar.

5. Save your changes to the newauditlog.sh script.

**What to do next**
You can now automate this script by using CRON to convert the Sun Solaris Basic Security Mode log to human-readable format.

**Creating a cron job**
Cron is a Solaris daemon utility that automates scripts and commands to run system-wide on a scheduled basis.

**About this task**
The following steps provide an example for automating newauditlog.sh to run daily at midnight. If you need to retrieve log files multiple times a day from your Solaris system, you must alter your cron schedule.

**Procedure**
1. Type the following command to create a copy of your cron file:
```
crontab -l > cronfile
```
2. Type the following command to edit the cronfile:
```
vi cronfile
```
3. Add the following information to your cronfile:
```
0 0 * * * /etc/security/newauditlog.sh
```
4. Save the change to the cronfile.
5. Type the following command to add the cronfile to crontab:
```
crontab cronfile
```
6. You can now configure the log source in IBM QRadar to retrieve the Sun Solaris BSM audit log files.

**What to do next**
You are now ready to configure a log source in QRadar.
Configuring a log source for Sun Solaris BSM

A log file protocol source allows IBM QRadar to retrieve archived log files from a remote host. Sun Solaris BSM supports the bulk loading of audit log files by using the log file protocol.

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. From the Log Source Type list, select Solaris BSM.
7. Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source. The log source identifier must be unique for the log source type.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP.</td>
</tr>
<tr>
<td></td>
<td>• SFTP - SSH File Transfer Protocol</td>
</tr>
<tr>
<td></td>
<td>• FTP - File Transfer Protocol</td>
</tr>
<tr>
<td></td>
<td>• SCP - Secure Copy</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>Type the IP address or host name of the Sun Solaris BSM system.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>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.</td>
</tr>
<tr>
<td>Remote User</td>
<td>Type the user name necessary to log in to your Sun Solaris system.</td>
</tr>
<tr>
<td></td>
<td>The user name can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Type the password necessary to log in to your Sun Solaris system.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the Remote Password to log in to your Sun Solaris system.</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>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 gives the option to ignore the Remote Password field.</td>
</tr>
<tr>
<td>Remote Directory</td>
<td>Type the directory location on the remote host from which the files are retrieved. By default, the newauditlog.sh script writes the human-readable logs files to the /var/log/ directory.</td>
</tr>
</tbody>
</table>
### Table 572. Log file parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recursive</td>
<td>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.</td>
</tr>
<tr>
<td>FTP File Pattern</td>
<td>If you select SFTP or FTP as the Service Type, this gives the option to configure the regular expression (regex) that is needed to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing. For example, if you want to retrieve all files in the &lt;starttime&gt;.&lt;endtime&gt;.&lt;hostname&gt;.log format, use the following entry: \d+/.\d+/.\w+.log. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: <a href="http://download.oracle.com/javase/tutorial/essential/regex/">http://download.oracle.com/javase/tutorial/essential/regex/</a></td>
</tr>
<tr>
<td>FTP Transfer Mode</td>
<td>This option appears only if you select FTP as the Service Type. The FTP Transfer Mode parameter gives the option 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:</td>
</tr>
<tr>
<td></td>
<td>- Binary - Select Binary for log sources that require binary data files or compressed .zip, .gzip, .tar, or .tar+gzip archive files.</td>
</tr>
<tr>
<td></td>
<td>- 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 use the ASCII as the transfer mode.</td>
</tr>
<tr>
<td>SCP Remote File</td>
<td>If you select SCP as the Service Type, you must type the file name of the remote file.</td>
</tr>
<tr>
<td>Start Time</td>
<td>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.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>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.</td>
</tr>
<tr>
<td>Run On Save</td>
<td>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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.</td>
</tr>
</tbody>
</table>
Table 572. Log file parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>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 processed.</td>
</tr>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>Select this check box to track files that are processed already, and you do not want the files to be processed a second time. This applies only to FTP and SFTP Service Types.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>Select this check box to define the local directory on your QRadar system that you want to use for storing downloaded files during processing. It is suggested that you leave the check box clear. When the check box is selected, the Local Directory field is displayed, which gives you the option to configure the local directory to use for storing files.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the Event Generator list, select LINEBYLINE.</td>
</tr>
</tbody>
</table>

8. Click Save.

The configuration is complete. Events that are retrieved by using the log file protocol are displayed on the Log Activity tab of QRadar.
You can integrate a Sybase Adaptive Server Enterprise (ASE) device with IBM QRadar SIEM to record all relevant events by using JDBC.

About this task
To configure a Sybase ASE device:

Procedure
1. Configure Sybase auditing.
   For information about configuring Sybase auditing, see your Sybase documentation.
2. Log in to the Sybase database as a sa user:
   \texttt{isql -Usa -P<password>}
   Where <password> is the password necessary to access the database.
3. Switch to the security database:
   \texttt{use sybsecurity}
   \texttt{go}
4. Create a view for IBM QRadar SIEM.
   \texttt{create view audit_view as select audit_event_name(event) as event_name, * from <audit_table_1>}
   \texttt{union}
   \texttt{select audit_event_name(event) as event_name, * from <audit_table_2>}
   \texttt{go}
5. For each additional audit table in the audit configuration, make sure that the \texttt{union select} parameter is repeated for each additional audit table.
   For example, if you want to configure auditing with four audit tables (sysaudits_01, sysaudits_02, sysaudits_03, sysaudits_04), type the following commands:
   \texttt{create view audit_view as select audit_event_name(event) as event_name, * from sysaudits_01}
   \texttt{union select audit_event_name(event) as event_name, * from sysaudits_02,}
   \texttt{union select audit_event_name(event) as event_name, * from sysaudits_03,}
   \texttt{union select audit_event_name(event) as event_name, * from sysaudits_04}

What to do next
You can now configure the log source IBM QRadar SIEM.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 QRadar to receive events from a Sybase ASE device

Configure QRadar to collect events from a Sybase ASE device by using the JDBC protocol.

### Procedure

1. Log in to QRadar SIEM.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**, and then configure the parameters.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>Type a unique name for the log source.</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>Type a description for the log source.</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>Sybase ASE</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>Sybase</td>
</tr>
<tr>
<td>Database Name</td>
<td>The name of the database to which you want to connect.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name of the database server.</td>
</tr>
</tbody>
</table>
### Table 573. Sybase JDBC protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port                 | Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are:  
- MSDE - 1433  
- Postgres - 5432  
- MySQL - 3306  
- Sybase - 1521  
- Oracle - 1521  
- Informix - 9088  
- DB2 - 50000  
If a database instance is used with the MSDE database type, you must leave the **Port** field blank. |
| Username             | A user account for QRadar in the database.                                                                                                                                                           |
| Password             | The password that is required to connect to the database.                                                                                                                                              |
| Confirm Password     | The password that is required to connect to the database.                                                                                                                                              |
| Predefined Query     | Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the **none** option.                                   |
| Table Name           | The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.). |
| Select List          | The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the **Compare Field**. |
| Compare Field        | A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. Enables the protocol to identify events that were previously polled by the protocol to ensure that duplicate events are not created. |
| Use Prepared Statements | Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements. |
| Start Date and Time  | Type the start date and time for database polling in the following format: 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. |
### Table 573. Sybase JDBC protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Polling Interval</strong></td>
<td>Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value. The maximum polling interval is one week.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000.</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>Select this check box to enable the log source. By default, the check box is selected.</td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
<td>From the list, select the Credibility of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
<td>Select the Target Event Collector to use as the target for the log source.</td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
<td>Select the Coalescing Events check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the Coalescing Events list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
<td>Select the Store Event Payload check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Store Event Payload list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

For more information about configuring JDBC parameters, see [c_logsource_JDBCprotocol.dita](#).

6. Click **Save**.
7. On the Admin tab, click **Deploy Changes**.
Chapter 148. Symantec

IBM QRadar supports a number of Symantec DSMs.

Symantec Critical System Protection

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Symantec</td>
</tr>
<tr>
<td>DSM Name</td>
<td>Critical System Protection</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-SymantecCriticalSystemProtection-QRadar_version_build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>5.1.1</td>
</tr>
<tr>
<td>Event format</td>
<td>DB Entries</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>All events from the ‘CSPEVENT_VW’ view</td>
</tr>
<tr>
<td>Log source type in QRadar UI</td>
<td>Symantec Critical System Protection</td>
</tr>
<tr>
<td>Auto discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties</td>
<td>No</td>
</tr>
</tbody>
</table>

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. The following table describes the parameters that require specific values to collect events from Symantec Critical System Protection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Symantec Critical System Protection</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>JDBC</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2.</td>
</tr>
<tr>
<td>Database Type</td>
<td>MSDE</td>
</tr>
<tr>
<td>Database Name</td>
<td>SCSPDB</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>The IP address or host name of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Sybase - 1521 • Oracle - 1521 • Informix - 9088 • DB2 - 50000 If a database instance is used with the MSDE database type, you must leave the Port field blank.</td>
</tr>
<tr>
<td>Username</td>
<td>A user account for QRadar in the database.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is required to connect to the database.</td>
</tr>
<tr>
<td>Authentication Domain</td>
<td>If you did not select Use Microsoft JDBC, Authentication Domain is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>SCSP</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Predefined Query (Optional)</td>
<td>Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the none option.</td>
</tr>
<tr>
<td>Table Name</td>
<td>CSPEVENT_VW</td>
</tr>
<tr>
<td>Select List</td>
<td>The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the Compare Field.</td>
</tr>
<tr>
<td>Compare Field</td>
<td>EVENT_ID</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.</td>
</tr>
<tr>
<td>Start Date and Time (Optional)</td>
<td>Type the start date and time for database polling in the following format: 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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value. The maximum polling interval is one week.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>The number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 20,000.</td>
</tr>
<tr>
<td>Use Named Pipe Communication</td>
<td>If you did not select Use Microsoft JDBC, Use Named Pipe Communication is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
<tr>
<td>Database Cluster Name</td>
<td>If you selected Use Named Pipe Communication, the Database Cluster Name parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select <strong>Use Microsoft JDBC</strong>, <strong>Use NTLMv2</strong> is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable <strong>Use Microsoft JDBC</strong>.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option if your connection supports SSL. This option appears only for MSDE.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected <strong>Use Microsoft JDBC</strong> and <strong>Use SSL</strong>, the <strong>Microsoft SQL Server Hostname</strong> parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

For more information about configuring the JDBC protocol parameters, see [c_logsouce_JDBCprotocol.dita](#).  

**Related tasks**

“Adding a DSM” on page 4  
“Adding a log source” on page 4  
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

---

**Symantec Data Loss Prevention (DLP)**

The Symantec Data Loss Protection (DLP) DSM for IBM QRadar accepts events from a Symantec DLP appliance by using syslog.

Before you configure QRadar, you must configure response rules on your Symantec DLP. The response rule allows the Symantec DLP appliance to forward syslog events to QRadar when a data loss policy violation occurs. Integrating Symantec DLP requires you to create two protocol response rules (SMTP and None of SMTP) for QRadar. These protocol response rules create an action to forward the event information, using syslog, when an incident is triggered.

To configure Symantec DLP with QRadar, take the following steps:

1. Create an SMTP response rule.
2. Create a None of SMTP response rule.
3. Configure a log source in QRadar.
4. Map Symantec DLP events in QRadar.
Creating an SMTP response rule

You can configure an SMTP response rule in Symantec DLP.

**Procedure**

1. Log in to your Symantec DLP user interface.
2. From the menu, select the Manage > Policies > Response Rules.
3. Click Add Response Rule.
4. Select one of the following response rule types:
   - **Automated Response** - Automated response rules are triggered automatically as incidents occur. This is the default value.
   - **Smart Response** - Smart response rules are added to the Incident Command screen and handled by an authorized Symantec DLP user.
5. Click Next.
6. **Rule Name** - Type a name for the rule you are creating. This name ideally is descriptive enough for policy authors to identify the rule. For example, QRadar Syslog SMTP.
7. **Description** - Optional. Type a description for the rule you are creating.
8. Click Add Condition.
9. On the Conditions panel, select the following conditions:
   - From the first list, select Protocol or Endpoint Monitoring.
   - From the second list, select Is Any Of.
   - From the third list, select SMTP.
10. On the Actions pane, click Add Action.
11. From the Actions list, select All: Log to a Syslog Server.
12. Configure the following options:
   a) **Host** - Type the IP address of your IBM QRadar.
   b) **Port** - Type 514 as the syslog port.
   c) **Message** - Type the following string to add a message for SMTP events.

```
LEEF:1.0|Symantec|DLP|2:medium|POLICY$ |usrName=$SENDER$|duser=$RECIPIENTS$|rules=$RULES$ |matchCount=$MATCH_COUNT$|blocked=$BLOCKED$|
incidentID=$INCIDENT_ID$|incidentSnapshot=$INCIDENT_SNAPSHOTS$ |subject=$SUBJECTS$|fileName=$FILE_NAME$|parentPath=$PARENT_PATHS$|
path=$PATHS$|quarantineParentPath=$QUARANTINE_PARENT_PATHS$|scan=$SCAN$|target=$TARGET$
```
13. **Level** - From this list, select 6 - Informational.
14. Click Save.

**What to do next**

You can now configure your None Of SMTP response rule.

Creating a None Of SMTP response rule

You can configure a None Of SMTP response rule in Symantec DLP:

**Procedure**

1. From the menu, select the Manage > Policies > Response Rules.
2. Click Add Response Rule.
3. Select one of the following response rule types:
• **Automated Response** - Automated response rules are triggered automatically as incidents occur. This is the default value.

• **Smart Response** - Smart response rules are added to the Incident Command screen and handled by an authorized Symantec DLP user.

4. Click **Next**.

Configure the following values:

5. **Rule Name** - Type a name for the rule you are creating. This name ideally is descriptive enough for policy authors to identify the rule. For example, **QRadar Syslog None Of SMTP**

6. **Description** - Optional. Type a description for the rule you are creating.

7. Click **Add Condition**.

8. On the **Conditions** pane, select the following conditions:
   
   • From the first list, select **Protocol or Endpoint Monitoring**.
   
   • From the second list, select **Is Any Of**.
   
   • From the third list, select **None Of SMTP**.

9. On the **Actions** pane, click **Add Action**.

10. From the **Actions** list, select **All: Log to a Syslog Server**.

11. Configure the following options:

   a) **Host** - Type the IP address of your QRadar.

12. **Port** - Type 514 as the syslog port.

13. **Message** - Type the following string to add a message for **None Of SMTP** events.

   ```
   LEEF:1.0|Symantec|DLP|2:medium|$POLICY$|src=$SENDER$|dst=$RECIPIENTS$|rules=$RULES$|matchCount=$MATCH_COUNT$|blocked=$BLOCKED$|incidentID=$INCIDENT_ID$|incidentSnapshot=$INCIDENT_SNAPSHOT$|subject=$SUBJECT$|fileName=$FILE_NAME$|parentPath=$PARENT_PATH$|path=$PATH$|quarantineParentPath=$QUARANTINE_PARENT_PATH$|scan=$SCAN$|target=$TARGET$
   ```

14. **Level** - From this list, select **6 - Informational**.

15. Click **Save**.

**What to do next**
You are now ready to configure IBM QRadar.

**Configuring a log source**
You can configure the log source in IBM QRadar to receive events from a Symantec DLP appliance.

**About this task**
QRadar automatically detects syslog events for the SMTP and None of SMTP response rules that you create. However, if you want to manually configure QRadar to receive events from a Symantec DLP appliance:

**Procedure**

From the **Log Source Type** list, select the **Symantec DLP** option.

For more information about Symantec DLP, see your vendor documentation.

**Related tasks**
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

**Event map creation for Symantec DLP events**

Event mapping is required for a number of Symantec DLP events. Due to the customizable nature of policy rules, most events, except the default policy events do not contain a predefined QRadar Identifier (QID) map to categorize security events.

You can individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track reoccurring events from your network devices. Until you map an event, all events that are displayed in the **Log Activity** tab for Symantec DLP are categorized as unknown. *Unknown* events are easily identified as the **Event Name** column and **Low Level Category** columns display *Unknown*.

**Discovering unknown events**

As your device forwards events to IBM QRadar, it can take time to categorize all of the events for a device, as some events might not be generated immediately by the event source appliance or software.

**About this task**

It is helpful to know how to quickly search for *unknown* events. When you know how to search for *unknown* events, it is suggested you repeat this search until you are comfortable that you can identify most of your events.

**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 the log source group or **Other**.
   
   Log sources that are not assigned to a group are categorized as **Other**.
6. From the **Log Source** list, select your Symantec DLP log source.
7. Click **Add Filter**.
   
   The **Log Activity** tab is displayed with a filter for your log source.
8. From the **View** list, select **Last Hour**.
   
   Any events that are generated by the Symantec DLP DSM in the last hour are displayed. Events that are displayed as *unknown* in the **Event Name** column or **Low Level Category** column require event mapping in QRadar.

   **Note:** You can save your existing search filter by clicking **Save Criteria**.

**What to do next**

You can now modify the event map.

**Modifying the event map**

Modifying an event map gives you the option to manually categorize events to a QRadar Identifier (QID) map.

**About this task**

Any event that is categorized to a log source can be remapped to a new QRadar Identifier (QID).

**Note:** Events that do not have a defined log source cannot be mapped to an event. Events without a log source display SIM Generic Log in the **Log Source** column.
Procedure

1. On the Event Name column, double-click an unknown event for Symantec DLP.
   The detailed event information is displayed.
2. Click Map Event.
3. From the Browse for QID pane, select any of the following search options to narrow the event categories for a IBM QRadar Identifier (QID):
   a) From the High-Level Category list, select a high-level event categorization.
      For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the IBM QRadar Administration Guide.
4. From the Low-Level Category list, select a low-level event categorization.
5. From the Log Source Type list, select a log source type.
   The Log Source Type list gives you the option to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, Symantec provides policy and data loss prevention events, you might select another product that likely captures similar events.
6. To search for a QID by name, type a name in the QID/Name field.
   The QID/Name field gives you the option to filter the full list of QIDs for a specific word, for example, policy.
7. Click Search.
   A list of QIDs are displayed.
8. Select the QID you want to associate to your unknown event.
9. Click OK.
   Maps any additional events that are forwarded from your device with the same QID that matches the event payload. The event count increases each time that the event is identified by QRadar.
   If you update an event with a new QRadar Identifier (QID) map, past events that are stored in QRadar are not updated. Only new events are categorized with the new QID.

Symantec Endpoint Protection

The IBM QRadar DSM for Symantec Endpoint Protection collects events from a Symantec Endpoint Protection system.

The following table describes the specifications for the Symantec Endpoint Protection DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Symantec</td>
</tr>
<tr>
<td>DSM name</td>
<td>Symantec Endpoint Protection</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-SymantecEndpointProtection- QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>Endpoint Protection V11, V12, and V14</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All Audit and Security Logs</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
</tbody>
</table>
To integrate Symantec Endpoint Protection 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
   - Symantec Endpoint Protection DSM RPM
2. Configure your Symantec Endpoint Protection device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Symantec Endpoint Protection log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from Symantec Endpoint Protection:
4. Verify that QRadar is configured correctly.

The following table shows a sample normalized event message from Symantec Endpoint Protection:

### Table 576. Symantec Endpoint Protection log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Symantec Endpoint Protection</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>Type a unique identifier for the log source.</td>
</tr>
</tbody>
</table>

### Table 577. Symantec Endpoint Protection sample message

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked</td>
<td>Access Denied</td>
<td>`&lt;51&gt;Mar 3 13:52:13 &lt;Server&gt; SymantecServer: USER,&lt;IP_address&gt;, Blocked,[AC13-1.5] Block from loading other DLLs - Caller MD5=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx,Load DLL Begin: 2017-03-03 13:48:18,End: 2017-03-03 13:48:18,Rule: Corp Endpoint - Browser Restrictions</td>
</tr>
</tbody>
</table>

### Related tasks
- “Adding a DSM” on page 4
- “Adding a log source” on page 4
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 Symantec Endpoint Protection to Communicate with QRadar**

Before you can add the Symantec Endpoint Protection log source in QRadar, you need to configure your Symantec Endpoint Protection device to forward syslog events.

**Procedure**

1. Log in to your Symantec Endpoint Protection Manager system.
2. In the left pane, click the **Admin** icon.
3. In the bottom of the **View Servers** pane, click **Servers**.
4. In the **View Servers** pane, click **Local Site**.
5. In the **Tasks** pane, click **Configure External Logging**.
6. From the **Generals** tab, select the **Enable Transmission of Logs to a Syslog Server** check box.
7. In the **Syslog Server** field, type the IP address of your QRadar that you want to parse the logs.
8. In the **UDP Destination Port** field, type 514.
9. In the **Log Facility** field, type 6.
10. In the **Log Filter** tab, under **Management Server Logs**, select the **Audit Logs** check box.
11. In the **Client Log** pane, select the **Security Logs** check box.
12. In the **Client Log** pane, select the **Risks** check box.
13. Click **OK**.

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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

**Symantec Encryption Management Server**

The Symantec Encryption Management Server DSM for IBM QRadar collects syslog events from Symantec Encryption Management Servers.

Symantec Encryption Management Server is formerly known as Symantec PGP Universal Server.

QRadar collects all relevant events from the following categories:

- Administration
- Software updates
- Clustering
- Backups
- Web Messenger
- Verified Directory
- Postfix
- Client logs
- Mail
- Whole Disk Encryption logs

Before you can integrate Symantec Encryption Management Server events with QRadar, you must configure Symantec Encryption Management Server to communicate with QRadar.
Related tasks
“Configuring Symantec Encryption Management Server to communicate with QRadar” on page 1089
Enable external logging to forward syslog events to IBM QRadar.

“Configuring a log source ” on page 1089
IBM QRadar automatically discovers and creates a log source for syslog events from Symantec Encryption Management Servers.

“Adding a DSM” on page 4

Configuring Symantec Encryption Management Server to communicate with QRadar
Enable external logging to forward syslog events to IBM QRadar.

Procedure
1. In a web browser, log in to your Encryption Management server's administrative interface.
   https://<Encryption Management Server IP address>:9000
2. Click Settings.
3. Select the Enable External Syslog check box.
4. From the Protocol list, select either UDP or TCP.
   By default, QRadar uses port 514 to receive UDP syslog or TCP syslog event messages.
5. In the Hostname field, type the IP address of your QRadar Console or Event Collector.
6. In the Port field, type 514.
7. Click Save.
   The configuration is complete. The log source is added to QRadar as Symantec Encryption Management Server events are automatically discovered. Events that are forwarded to QRadar by the Symantec Encryption Management Servers are displayed on the Log Activity tab of QRadar.

Configuring a log source
IBM QRadar automatically discovers and creates a log source for syslog events from Symantec Encryption Management Servers.

About this task
If QRadar does not automatically detect the syslog log source, add a Symantec Encryption Management Server log source on the QRadar Console.

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 Symantec Encryption Management Server.
10. Configure the parameter values. The following table describes the parameter that requires a specific value for Symantec Encryption Management event collection:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Symantec Encryption Management Server.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

### Symantec SGS

The Symantec Gateway Security (SGS) Appliance DSM for IBM QRadar accepts SGS events by using syslog.

**About this task**

QRadar records all relevant events from SGS. Before you configure QRadar to integrate with an SGS, you must configure syslog within your SGS appliance. For more information on Symantec SGS, see your vendor documentation.

After you configure syslog to forward events to QRadar, the configuration is complete. Events forward from Symantec SGS to QRadar using syslog are automatically discovered. However, if you want to manually create a log source for Symantec SGS:

**Procedure**

From the **Log Source Type** list, select the **Symantec Gateway Security (SGS) Appliance** option.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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

### Symantec System Center

The Symantec System Center (SSC) DSM for IBM QRadar retrieves events from an SSC database by using a custom view that is created for QRadar.

QRadar records all SSC events. You must configure the SSC database with a user that has read and write privileges for the custom QRadar view to be able to poll the view for information. Symantec System Center (SSC) supports only the JDBC protocol.

**Configuring a database view for Symantec System Center**

A database view is required by the JDBC protocol to poll for SSC events.

**Procedure**

In the Microsoft SQL Server database that is used by the SSC device, configure a custom default view to support IBM QRadar:

**Note:** The database name must not contain any spaces.

- CREATE VIEW dbo.vw_qradar AS SELECT
- dbo.alerts.Idx AS idx,
- dbo.inventory.IP_Address AS ip,
What to do next
After you create your custom view, you must configure QRadar to receive event information by using the JDBC protocol.

Configuring a log source in QRadar to collect events from Symantec System Center
Configure IBM QRadar to access the Symantec System Center database by using the JDBC protocol.

Procedure
1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.
5. Configure the parameters. The following table describes the parameters that require specific values to collect events from Symantec System Center:

<table>
<thead>
<tr>
<th>Table 579. Symantec System Center JDBC parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Name</td>
</tr>
<tr>
<td>Log Source Description (Optional)</td>
</tr>
<tr>
<td>Log Source Type</td>
</tr>
<tr>
<td>Protocol Configuration</td>
</tr>
</tbody>
</table>
Table 57. Symantec System Center JDBC parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Log Source Identifier** | Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol.  
If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the Log Source Identifier value; for example, 192.168.1.1 or JDBC192.168.1.1.  
If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the Log Source Identifier value; for example, JDBC1, JDBC2. |
| **Database Type**       | MSDE.                                                                                                                                                                                                     |
| **Database Name**       | Type Reporting as the name of the Symantec System Center database.                                                                                                                                                                                                  |
| **IP or Hostname**      | Type the IP address or host name of the Symantec System Center 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 Symantec System Center database. The Symantec System Center database must have incoming TCP connections that are enabled to communicate with QRadar.  
If you define a Database Instance when you use MSDE as the database type, you must leave the Port field blank in your configuration. |
| **Username**            | Type the user name that is required to access the database.                                                                                                                                                 |
| **Password**            | Type the password that is required to access the database. The password can be up to 255 characters in length.                                                                                              |
| **Confirm Password**    | Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the Password field.                                                    |
| **Authentication Domain** | If you did not select Use Microsoft JDBC, Authentication Domain is displayed.  
The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.                                      |
<p>| <strong>Database Instance</strong>   | The database instance, if required. MSDE databases can include multiple SQL server instances on one server.                                                                                               |
|                         | When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the Database Instance parameter must be blank in the log source configuration.                     |
| <strong>Table Name</strong>          | Type vw_qradar as the name of the table or view that includes the event records.                                                                                                                            |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select List</td>
<td>Type <code>*</code> for all fields from the table or view. You can use a comma-separated list to define specific tables or views, if you need it for your configuration. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).</td>
</tr>
<tr>
<td>Compare Field</td>
<td>Type <code>idx</code> as the compare field. The compare field is used to identify new events that are added between queries to the table.</td>
</tr>
<tr>
<td>Use Prepared Statements</td>
<td>Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>Type the start date and time for database polling in the following format: <code>yyyy-MM-dd HH:mm</code> with <code>HH</code> 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.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Type the polling interval, which 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 <code>H</code> for hours or <code>M</code> for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values that are entered without an <code>H</code> or <code>M</code> poll in seconds.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The default value is 20000 EPS.</td>
</tr>
<tr>
<td>Use Named Pipe</td>
<td>If you did not select <strong>Use Microsoft JDBC, Use Named Pipe Communication</strong> is displayed. Clear the <strong>Use Named Pipe Communication</strong> check box. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.</td>
</tr>
<tr>
<td>Communication</td>
<td></td>
</tr>
<tr>
<td>Database Cluster</td>
<td>If you selected the <strong>Use Named Pipe Communication</strong> check box, the <strong>Database Cluster Name</strong> parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.</td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Use NTLMv2</td>
<td>If you did not select <strong>Use Microsoft JDBC, Use NTLMv2</strong> is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Microsoft JDBC</td>
<td>If you want to use the Microsoft JDBC driver, you must enable <strong>Use Microsoft JDBC</strong>.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option if your connection supports SSL.</td>
</tr>
<tr>
<td>Microsoft SQL Server Hostname</td>
<td>If you selected <strong>Use Microsoft JDBC</strong> and <strong>Use SSL</strong>, the <strong>Microsoft SQL Server Hostname</strong> parameter is displayed. You must type the host name for the Microsoft SQL server.</td>
</tr>
</tbody>
</table>

For more information about configuring the JDBC protocol, see `c_logsource_JDBCprotocol.dita`.

**Note:** Selecting a value greater than 5 for the **Credibility** parameter weights your Symantec System Center log source with a higher importance compared to other log sources in QRadar.

6. Click **Save**.
7. On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.
Chapter 149. ThreatGRID Malware Threat Intelligence Platform

The ThreatGRID Malware Threat Intelligence Platform DSM for IBM QRadar collects malware events by using the log file protocol or syslog.

QRadar supports ThreatGRID Malware Threat Intelligence Platform appliances with v2.0 software that use the QRadar Log Enhanced Event Format (LEEF) Creation script.

Supported event collection protocols for ThreatGRID Malware Threat Intelligence

ThreatGRID Malware Threat Intelligence Platform writes malware events that are readable by IBM QRadar.

The LEEF creation script is configured on the ThreatGRID appliance and queries the ThreatGRID API to write LEEF events that are readable by QRadar. The event collection protocol your log source uses to collect malware events is based on the script you install on your ThreatGRID appliance.

Two script options are available for collecting LEEF formatted events:

- **Syslog** - The syslog version of the LEEF creation script allows your ThreatGRID appliance to forward events directly to QRadar. Events that are forwarded by the syslog script are automatically discovered by QRadar.
- **Log file** - The log file protocol version of the LEEF creation script allows the ThreatGRID appliance to write malware events to a file. QRadar uses the log file protocol to communicate with the event log host to retrieve and parse malware events.

The LEEF creation script is available from ThreatGRID customer support. For more information, see the ThreatGRID website http://www.threatgrid.com or email ThreatGRID support at support@threatgrid.com.

ThreatGRID Malware Threat Intelligence configuration overview

You can integrate ThreatGRID Malware Threat Intelligence events with IBM QRadar.

You must complete the following tasks:

1. Download the QRadar Log Enhanced Event Format Creation script for your collection type from the ThreatGRID support website to your appliance.
2. On your ThreatGRID appliance, install and configure the script to poll the ThreatGRID API for events.
3. On your QRadar appliance, configure a log source to collect events based on the script you installed on your ThreatGRID appliance.
4. Ensure that no firewall rules block communication between your ThreatGRID installation and the QRadar Console or managed host that is responsible for retrieving events.

Configuring a ThreatGRID syslog log source

IBM QRadar automatically discovers and creates a log source for malware events that are forwarded from the ThreatGRID Malware Threat Intelligence Platform.

**About this task**

This procedure is optional.
**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 **ThreatGRID Malware Intelligence Platform**.
9. From the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source Identifier</strong></td>
<td>Type the IP address or host name for the log source as an identifier for events from your ThreatGRID Malware Intelligence Platform. The log source identifier must be unique for the log source type.</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>Select this check box to enable the log source. By default, the check box is selected.</td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
<td>From the list, select the credibility of the log source. The range is 0 - 10. 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. The default is 5.</td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
<td>From the list, select the <strong>Target Event Collector</strong> to use as the target for the log source.</td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
<td>Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the <strong>Coalescing Events</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td><strong>Incoming Event Payload</strong></td>
<td>From the list, select the incoming payload encoder for parsing and storing the logs.</td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
<td>Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the <strong>Store Event Payload</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

Malware events that are forwarded to QRadar are displayed on the **Log Activity** tab of QRadar.
Configuring a ThreatGRID log file protocol log source

To use the log file protocol to collect events, you must configure a log source in IBM QRadar to poll for the event log that contains your malware events.

Procedure

1. Click the Admin tab.
2. On the navigation menu, click Data Sources.
3. Click the Log Sources icon.
4. Click Add.
5. In the Log Source Name field, type a name for the log source.
6. In the Log Source Description field, type a description for the log source.
7. From the Log Source Type list, select ThreatGRID Malware Threat Intelligence Platform.
8. From the Protocol Configuration list, select Log File.
9. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type an IP address, host name, or name to identify the event source. The log source identifier must be unique for the log source type.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the list, select the protocol that you want to use to retrieve log files from a remote server. The default is SFTP.</td>
</tr>
<tr>
<td></td>
<td>• SFTP - SSH File Transfer Protocol</td>
</tr>
<tr>
<td></td>
<td>• FTP - File Transfer Protocol</td>
</tr>
<tr>
<td></td>
<td>• SCP - Secure Copy Protocol</td>
</tr>
<tr>
<td></td>
<td>The SCP and SFTP service type requires that the host server in the Remote IP or Hostname field has the SFTP subsystem enabled.</td>
</tr>
<tr>
<td>Remote IP or Hostname</td>
<td>Type the IP address or host name of the ThreatGRID server that contains your event log files.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Type the port number for the protocol that is selected to retrieve the event logs from your ThreatGRID server. The valid range is 1 - 65535.</td>
</tr>
<tr>
<td></td>
<td>The list of default service type port numbers:</td>
</tr>
<tr>
<td></td>
<td>• FTP - TCP Port 21</td>
</tr>
<tr>
<td></td>
<td>• SFTP - TCP Port 22</td>
</tr>
<tr>
<td></td>
<td>• SCP - TCP Port 22</td>
</tr>
<tr>
<td>Remote User</td>
<td>Type the user name that is required to log in to the ThreatGRID web server that contains your audit event logs. The user name can be up to 255 characters in length.</td>
</tr>
<tr>
<td>Remote Password</td>
<td>Type the password to log in to your ThreatGRID server.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password to log in to your ThreatGRID server.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>SSH Key File</strong></td>
<td>If you select <strong>SCP</strong> or <strong>SFTP</strong> as the <strong>Service Type</strong>, use this parameter to define an SSH private key file. When you provide an <strong>SSH Key File</strong>, the <strong>Remote Password</strong> field is ignored.</td>
</tr>
<tr>
<td><strong>Remote Directory</strong></td>
<td>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 are in the remote user's home directory, you can leave the remote directory blank. Blank values in the <strong>Remote Directory</strong> field support systems that have operating systems where a change in the working directory (CWD) command is restricted.</td>
</tr>
<tr>
<td><strong>Recursive</strong></td>
<td>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 <strong>Recursive</strong> parameter is ignored if you configure SCP as the <strong>Service Type</strong>.</td>
</tr>
<tr>
<td><strong>FTP File Pattern</strong></td>
<td>Type the regular expression (regex) required to filter the list of files that are specified in the <strong>Remote Directory</strong>. All files that match the regular expression are retrieved and processed. The FTP file pattern must match the name that you assigned to your ThreatGRID event log. For example, to collect files that start with <code>leef</code> or <code>LEEF</code> and ends with a text file extension, type the following value: `(leef</td>
</tr>
<tr>
<td><strong>FTP Transfer Mode</strong></td>
<td>If you select <strong>FTP</strong> as the <strong>Service Type</strong>, from the list, select <strong>ASCII</strong>. ASCII is required for text-based event logs.</td>
</tr>
<tr>
<td><strong>SCP Remote File</strong></td>
<td>If you select <strong>SCP</strong> as the <strong>Service Type</strong>, type the file name of the remote file.</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>Type a time value to represent the time of day you want the log file protocol to start. The start time is based on a 24 hour clock and uses the following format: HH:MM. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the <strong>Recurrence</strong> field value to establish when your ThreatGRID server is polled for new event log files.</td>
</tr>
<tr>
<td><strong>Recurrence</strong></td>
<td>Type the frequency that you want to scan the remote directory on your ThreatGRID server for new event log files. Type this value in hours (H), minutes (M), or days (D). For example, type 2H to scan the remote directory every 2 hours from the start time. The default recurrence value is 1H. The minimum time interval is 15M.</td>
</tr>
</tbody>
</table>
Table 581. Log file protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Run On Save</strong></td>
<td>Select this check box if you want the log file protocol to run immediately after you click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>After the save action completes, the log file protocol follows your configured start time and recurrence schedule.</td>
</tr>
<tr>
<td></td>
<td>Selecting <strong>Run On Save</strong> clears the list of previously processed files for the <strong>Ignore Previously Processed File</strong> parameter.</td>
</tr>
<tr>
<td><strong>EPS Throttle</strong></td>
<td>Type the number of events per second (EPS) that you do not want this protocol to exceed. The valid range is 100 - 5000.</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>From the list, select <strong>NONE</strong>.</td>
</tr>
<tr>
<td></td>
<td>Processors allow event file archives to be expanded and processed for their events. Files are processed after they are downloaded. QRadar can process files in zip, gzip, tar, or tar+gzip archive format.</td>
</tr>
<tr>
<td><strong>Ignore Previously Processed File(s)</strong></td>
<td>Select this check box to track and ignore files that are already processed. QRadar examines the log files in the remote directory to determine whether the event log was processed by the log source. If a previously processed file is detected, the log source does not download the file. Only new or unprocessed event log files are downloaded by QRadar. This option applies to FTP and SFTP service types.</td>
</tr>
<tr>
<td><strong>Change Local Directory?</strong></td>
<td>Select this check box to define a local directory on your QRadar appliance to store event log files during processing.</td>
</tr>
<tr>
<td></td>
<td>In most scenarios, you can leave this check box not selected. When this check box is selected, the <strong>Local Directory</strong> field is displayed. You can configure a local directory to temporarily store event log files. After the event log is processed, the events added to QRadar and event logs in the local directory are deleted.</td>
</tr>
<tr>
<td><strong>Event Generator</strong></td>
<td>From the <strong>Event Generator</strong> list, select <strong>LineByLine</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Event Generator</strong> applies extra 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.</td>
</tr>
</tbody>
</table>

10. Click **Save**.  
11. On the **Admin** tab, click **Deploy Changes**.  
   Malware events that are retrieved by the log source are displayed on the **Log Activity** tab of QRadar.
IBM QRadar supports a range of Tipping Point DSMs.

**Tipping Point Intrusion Prevention System**

The Tipping Point Intrusion Prevention System (IPS) DSM for IBM QRadar accepts Tipping Point events by using syslog.

QRadar records all relevant events from either a Local Security Management (LMS) device or multiple devices with a Security Management System (SMS).

Before you configure QRadar to integrate with Tipping Point, you must configure your device based on type:

- If you are using an SMS, see “Configure remote syslog for SMS ” on page 1101.
- If you are using an LSM, see “Configuring notification contacts for LSM” on page 1102.

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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

**Configure remote syslog for SMS**

To configure Tipping Point for SMS, you must enable and configure your appliance to forward events to a remote host using syslog.

**About this task**

To configure your Tipping Point SMS:

**Procedure**

1. Log in to the Tipping Point system.
3. Select the Management tab.
4. Click Add.

   The Edit Syslog Notification window is displayed.
5. Select the Enable check box.
6. Configure the following values:
   a) **Syslog Server** - Type the IP address of the QRadar to receive syslog event messages.
   b) **Port** - Type 514 as the port address.
   c) **Log Type** - Select SMS 2.0 / 2.1 Syslog format from the list.
   d) **Facility** - Select Log Audit from the list.
   e) **Severity** - Select Severity in Event from the list.
   f) **Delimiter** - Select TAB as the delimiter for the generated logs.
   g) **Include Timestamp in Header** - Select Use original event timestamp.
   h) Select the Include SMS Hostname in Header check box.
   i) Click OK.
   j) You are now ready to configure the log source in QRadar.
7. To configure QRadar to receive events from a Tipping Point device: From the Log Source Type list, select the Tipping Point Intrusion Prevention System (IPS) option.

For more information about your Tipping Point device, see your vendor documentation.

**Related tasks**

- “Adding a log source” on page 4
- 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 notification contacts for LSM**

You can configure LSM notification contacts.

**Procedure**

1. Log in to the Tipping Point system.
2. From the LSM menu, select IPS > Action Sets.
   
   The IPS Profile - Action Sets window is displayed.
3. Click the Notification Contacts tab.
   
   The Edit Notification Contact page is displayed.
5. Configure the following values:
   
   a) Syslog Server - Type the IP address of the QRadar to receive syslog event messages.
   
   b) Port - Type 514 as the port address.
   
   c) Alert Facility - Select none or a numeric value 0-31 from the list. Syslog uses these numbers to identify the message source.
   
   d) Block Facility - Select none or a numeric value 0-31 from the list. Syslog uses these numbers to identify the message source.
   
   e) Delimiter - Select TAB from the list.
   
   f) Click Add to table below.
   
   g) Configure a Remote system log aggregation period in minutes.
6. Click Save.

**Note:** If your QRadar is in a different subnet than your Tipping Point device, you might have to add static routes. For more information, see your vendor documentation.

**What to do next**

You are now ready to configure the action set for your LSM, see “Configuring an Action Set for LSM” on page 1102.

**Configuring an Action Set for LSM**

You can configure an action set for your LSM.

**Procedure**

1. Log in to the Tipping Point system.
2. From the LSM menu, select IPS Action Sets.
   
   The IPS Profile - Action Sets window is displayed.
3. Click Create Action Set.
   
   The Create/Edit Action Set window is displayed.
4. Type the Action Set Name.
5. For Actions, select a flow control action setting:
• **Permit** - Allows traffic.
• **Rate Limit** - Limits the speed of traffic. If you select Rate Limit, you must also select the desired rate.
• **Block** - Does not permit traffic.
• **TCP Reset** - When this is used with the *Block action*, it resets the source, destination, or both IP addresses of an attack. This option resets blocked TCP flows.
• **Quarantine** - When this is used with the *Block action*, it blocks an IP address (source or destination) that triggers the filter.

6. Select the **Remote System Log** check box for each action you select.
7. Click **Create**.

You are now ready to configure the log source in QRadar.

8. To configure QRadar to receive events from a Tipping Point device: From the **Log Source Type** list, select the **Tipping Point Intrusion Prevention System (IPS)** option.

For more information about your Tipping Point device, see your vendor documentation.

### Related tasks
- “Adding a log source” on page 4
- If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

---

### Tipping Point X505/X506 Device

The Tipping Point X505/X506 DSM for IBM QRadar accepts events by using syslog.

QRadar records all relevant system, audit, VPN, and firewall session events.

#### Configuring syslog

You can configure your device to forward events to IBM QRadar.

**Procedure**

1. Log in to the Tipping Point X505/X506 device.
2. From the **LSM** menu, select **System > Configuration > Syslog Servers**.
   - The **Syslog Servers** window is displayed.
3. For each log type you want to forward, select a check box and type the IP address of your QRadar.
   - **Note:** If your QRadar is in a different subnet than your Tipping Point device, you might have to add static routes. For more information, see your vendor documentation.

You are now ready to configure the log source in QRadar.

4. To configure QRadar to receive events from a Tipping Point X505/X506 device: From the **Log Source Type** list, select the **Tipping Point X Series Appliances** option.
   - **Note:** If you have a previously configured Tipping Point X505/X506 DSM installed and configured on your QRadar, the Tipping Point X Series Appliances option is still displayed in the **Log Source Type** list. However, for any new Tipping Point X505/X506 DSM that you configure, you must select the **Tipping Point Intrusion Prevention System (IPS)** option.

**Related tasks**
- “Adding a log source” on page 4
- 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 151. Top Layer IPS

The Top Layer IPS DSM for IBM QRadar accepts Top Layer IPS events by using syslog.
QRadar records and processes Top Layer events. Before you configure QRadar to integrate with a Top Layer device, you must configure syslog within your Top Layer IPS device. For more information on configuring Top Layer, see your Top Layer documentation.

The configuration is complete. The log source is added to QRadar as Top Layer IPS events are automatically discovered. Events that are forwarded to QRadar by Top Layer IPS are displayed on the Log Activity tab of QRadar.

To configure QRadar to receive events from a Top Layer IPS device:

From the Log Source Type list, select the Top Layer Intrusion Prevention System (IPS) option.

For more information about your Top Layer device, see your vendor documentation.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 152. Townsend Security LogAgent

IBM QRadar can collect CEF format events from Townsend Security LogAgent installations on IBM i infrastructure.

QRadar supports CEF events from Townsend Security software that is installed on IBM i V5.1 and above.

Supported event types
Townsend Security LogAgent installations on IBM i can write to forward syslog events for security, compliance, and auditing to QRadar.

All syslog events that are forwarded by Raz-Lee iSecurity automatically discover and the events are parsed and categorized with the IBM i DSM.

Configuring Raz-Lee iSecurity

To collect security and audit events, you must configure your Raz-Lee iSecurity installation to forward syslog events to IBM QRadar.

Procedure
1. Log in to the IBM i command-line interface.
2. Type the following command to access the audit menu options:
   STRAUD
3. From the Audit menu, select 81. System Configuration.
4. From the iSecurity/Base System Configuration menu, select 31. SYSLOG Definitions.
5. Configure the following parameters:
   a) Send SYSLOG message - Select Yes.
   b) Destination address - Type the IP address of QRadar.
   c) "Facility" to use - Type a facility level.
   d) "Severity" range to auto send - Type a severity level.
   e) Message structure - Type any additional message structure parameters that are needed for your syslog messages.

What to do next
Syslog events that are forwarded by Raz-Lee iSecurity are automatically discovered by QRadar by the IBM i DSM. In most cases, the log source is automatically created in QRadar after a few events are detected. If the event rate is low, then you might be required to manually create a log source for Raz-Lee iSecurity in QRadar.

Until the log source is automatically discovered and identified, the event type displays as Unknown on the Log Activity tab of QRadar. Automatically discovered log sources can be viewed on the Admin tab of QRadar by clicking the Log Sources icon.
Configuring a log source

IBM QRadar automatically discovers and creates a log source for syslog events forwarded from Raz-Lee iSecurity. This procedure is optional.

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 box, select IBM i.
9. Using the Protocol Configuration list box, select Syslog.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your IBM i system with Raz-Lee iSecurity.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.
IBM QRadar supports several Trend Micro DSMs.

**Trend Micro Control Manager**

You can integrate a Trend Micro Control Manager device with IBM QRadar.

A Trend Micro Control Manager accepts events using SNMPv1 or SNMPv2. Before you configure QRadar to integrate with a Trend Micro Control Manager device, you must configure a log source, then configure SNMP trap settings for your Trend Micro Control Manager.

**Configuring a log source**

IBM QRadar does not automatically discover SNMP events from Trend Micro Control Manager.

**About this task**

You must configure an SNMP log source for your Trend Micro Control Manager to use the SNMPv1 or SNMPv2 protocol. SNMPv3 is not supported by Trend Micro Control Manager.

**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 **Trend Micro Control Manager**.
9. From the **Protocol Configuration** list, select **SNMPv2**.
10. SNMPv3 is not supported by Trend Micro Control Manager.

Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from your Trend Micro Control Manager appliance.</td>
</tr>
<tr>
<td>Community</td>
<td>Type the SNMP community name required to access the system containing SNMP events. The default is Public.</td>
</tr>
<tr>
<td>Include OIDs in Event Payload</td>
<td>Clear the <strong>Include OIDs in Event Payload</strong> check box, if selected. This option allows the SNMP event payload to be constructed using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
The configuration is complete.

**Configuring SNMP traps**
You can configure SNMP traps for Trend Micro Control Manager. Versions v5.5 and v6.0 are supported.

**Procedure**
1. Log in to the Trend Micro Control Manager device.
2. Choose one of the following options based on the Trend Micro Control Manager version you're using:
   a) For v5.5, select **Administration > Settings > Event Center Settings**.
      
      **Note:** Trend Micro Control Manager v5.5 requires hotfix 1697 or hotfix 1713 after Service Pack 1 Patch 1 to provide correctly formatted SNMPv2c events. For more information, see your vendor documentation.
   b) For v6.0 and v7.0, select **Administration > Event Center > General Event Settings**.
3. Set the SNMP trap notifications: In the **SNMP Trap Settings** field, type the Community Name.
4. Type the IBM QRadar server IP address.
5. Click **Save**.
   You are now ready to configure events in the Event Center.
6. Choose one of the following options based on the Trend Micro Control Manager version you're using:
   a) For v5.5, select **Administration > Event Center**.
   b) For v6.0, select **Administration > Event Center > Event Notifications**.
7. From the **Event Category** list, expand **Alert**.
8. Click **Recipients** for an alert.
9. In **Notification methods**, select the **SNMP Trap Notification** check box.
10. Click **Save**.
    The **Edit Recipients Result** window is displayed.
11. Click **OK**.
12. Repeat “Configuring SNMP traps ” on page 1110 for every alert that requires an SNMP Trap Notification.

The configuration is complete. Events from Trend Micro Control Manager are displayed on the **Log Activity** tab of QRadar. For more information about Trend Micro Control Manager, see your vendor documentation.

**Trend Micro Deep Discovery Analyzer**
The IBM QRadar DSM for Trend Micro Deep Discovery Analyzer collects 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Trend Micro</td>
</tr>
<tr>
<td>DSM name</td>
<td>Trend Micro Deep Discovery Analyzer</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-TrendMicroDeepDiscoveryAnalyzer-QRadar_version-<em>build_number</em>.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>5.0, 5.5, 5.8 and 6.0</td>
</tr>
</tbody>
</table>
Table 584. Trend Micro Deep Discovery Analyzer DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

To send Trend Micro Deep Discovery Analyzer events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the following RPMs.
   - DSMCommon RPM
   - Trend Micro Deep Discovery Analyzer DSM
2. Configure your Trend Micro Deep Discovery Analyzer device to communicate with QRadar.
3. If QRadar does not automatically detect Trend Micro Deep Discovery Analyzer as a log source, create a Trend Micro Deep Discovery Analyzer 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 Analyzer event collection:

Table 585. Trend Micro Deep Discovery Analyzer log source parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Trend Micro Deep Discovery Analyzer</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

Related tasks
Adding a DSM
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
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. To configure Deep Discovery Analyzer V5.0, follow these steps:
   a) Click Administration > Log Settings.
   b) Select Forward logs to a syslog server.
   c) Select LEEF as the log format.
d) Select the protocol that you want to use to forward the events.
e) In the **Syslog server** field, type the host name or IP address of your QRadar Console or Event Collector.
f) In the **Port** field, type 514.

3. To configure Deep Discovery Analyzer V5.5, follow these steps:
   a) Click **Administration > Log Settings**.
   b) Select **Send logs to a syslog server**.
   c) In the **Server** field, type the host name or IP address of your QRadar Console or Event Collector.
   d) In the **Port** field, type 514.
   e) Select the protocol that you want to use to forward the events.
   f) Select **LEEF** as the log format.

4. To configure Deep Discovery Analyzer V5.8 or V6.0, follow these steps:
   a) Click **Administration > Integrated Products/Services > Log Settings**.
   b) Select **Send logs to a syslog server**.
   c) In the **Server address** field, type the host name or IP address of your QRadar console or Event Collector.
   d) In the **Port** field, type the port number.
   
   **Note:** Trend Micro suggests that you use the following default syslog ports: UDP: 514; TCP: 601; and SSL: 443.
   e) Select the protocol that you want to use to forward the events; UDP/TCP/SSL.
   f) Select **LEEF** as the log format.
   g) Select the **Scope** of logs to send to the syslog server.
   h) Optional: Select the **Extensions** check box if you want to exclude any logs from sending data to the syslog server.

5. Click **Save**.

**Trend Micro Deep Discovery Director**

The IBM QRadar DSM for Trend Micro Deep Discovery Director collects LEEF formatted events from a Trend Micro Deep Discovery Director device.

To integrate Trend Micro Deep Discovery Director with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Trend Micro Deep Discovery Inspector DSM RPM
   - Trend Micro Deep Discovery Director DSM RPM

2. Configure your Trend Micro Deep Discovery Director device to send events to QRadar.

3. If QRadar does not automatically detect the log source, add a Trend Micro Deep Discovery Director log source on the QRadar Console. The following table describes the parameters that require specific values to collect Syslog events from Trend Micro Deep Discovery Director:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Source type</strong></td>
<td>Trend Micro Deep Discovery Director</td>
</tr>
<tr>
<td><strong>Protocol Configuration</strong></td>
<td>Syslog</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>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, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.</td>
</tr>
</tbody>
</table>

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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

**Trend Micro Deep Discovery Director DSM specifications**

The following table describes the specifications for the Trend Micro Deep Discovery Director DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Trend Micro</td>
</tr>
<tr>
<td>DSM name</td>
<td>Trend Micro Deep Discovery Director</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-TrendMicroDeepDiscoveryDirector-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>3.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Trend Micro Deep Discovery Inspector Events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

**Configuring Trend Micro Deep Discovery Director to communicate with QRadar**

To collect events from Trend Micro Deep Discovery Director, configure your Trend Micro Deep Discovery Director device to forward syslog events to QRadar.

**Procedure**

1. Log in to your Trend Micro Deep Discovery Director device.
2. Click Administration > Integrated Products/Services > Syslog.
3. Click Add, and then select Enabled.
4. Configure the parameters in the following table.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>The name for the Deep Discovery Director syslog server.</td>
</tr>
<tr>
<td>Server address</td>
<td>The IP address of your QRadar Console or Event Collector.</td>
</tr>
<tr>
<td>Port</td>
<td>• SSL/TLS - 6514 (default port)</td>
</tr>
<tr>
<td></td>
<td>• TCP - 601</td>
</tr>
<tr>
<td></td>
<td>• UDP - 514</td>
</tr>
<tr>
<td>Protocol</td>
<td>• SSL/TLS</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td>• UDP</td>
</tr>
<tr>
<td>Log format</td>
<td>LEEF</td>
</tr>
<tr>
<td>Scope</td>
<td>The events that you want to forward to QRadar.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

**Sample event messages**

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides sample event messages when using the Syslog protocol for the Trend Micro Deep Discovery Director DSM:

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>DENYLIST_CHANGE</td>
<td>Successful Configuration Modification</td>
<td>Oct 24 12:37:32 ddd35-1.ddxqa.com LEEF:1.0</td>
</tr>
</tbody>
</table>
Table 588. Trend Micro Deep Discovery Director sample message supported by Trend Micro Deep Discovery Director.
(continued)

<table>
<thead>
<tr>
<th>Event name</th>
<th>Low-level category</th>
<th>Sample log message</th>
</tr>
</thead>
</table>
| SECURITY_RISK_DETECTION | Potential Misc Exploit | `<156>LEEF:1.0|Trend Micro|Deep Discovery Director[2.0.0.1129]|SECURITY_RISK_DETECTION| Origin=Inspector devTimeFormat=MMM dd yyyy HH:mm:ss z ptype=IDS dvc=198.51.10065 device MacAddress=00-00-5E-00-53-00 dvhost=localhost deviceGUID=E77B0BE4474D-4413AF2F-752E-5810-1B11 devTime=May 25 2017 05:59:53 GMT+00:00 sev=8 origin=Inspector protoGroup=SQL proto=UDP vlAN Id=4995 deviceDirection=1 dhost=hit-ndomain.opendns.com dst=198.51.100.9 dstPort=1207 dstMAC =00:00:0c:07:ac:0 shost=198.51.100.22 src=198.51.100.7 srcPort=1060 srcMAC=00:00:0c:07:ac:0 MalName=OPS_HTTP_SASFIS_REQUEST MalType=FRAUD sAttakcPhase=Data Exfiltration fname=controller.php fileType=458757 fileSize=520704 ruleId=328 msg =WEMON - HTTP (Request) deviceRiskConfidenceLevel =1 duser=username@example.com suser=username@example.com mailMsgSubject=Mail Subject botCommand =msblast.exe botUrl=0005 channelName=#Infected chatUserName=fhkvmxya url=http://1.aliliosanguer.a.com/cgi-bin/forms.cgi requestClientApplication=Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) pComp=VSAPI riskType=0 compressedFileName=test_inarc mitigationTaskId=48b3d7f17-f30f-4890-6267-50bbf5f3b6a srcGroup=Default srcZone=1 dstGroup=Default dstZone=1 detect ionType=2 act=not blocked threatType=1 interest edIp=198.51.100.35 peerIp=198.51.100.8 fileHash =F1C9FCF4BF74E8EE53B6C006A4977F798A4D872 suser1 =srcusername1 sUser1LoginTime=Mar 09 2017 12:34: 56 GMT+00:00 suser2=srcusername2 sUser2LoginTime =Mar 09 2017 12:34:56 GMT+00:00 sUser3=srcusername3 sUser3LoginTime=Mar 09 2017 12:34:56 GMT+00:00 dUser1=dstusername1 dUser1LoginTime=Mar 09 20 17 12:34:56 GMT+00:00 dUser2=dUser2LoginTime=Mar 09 2017 12:34:56 GMT+00:00 dUser3=dUser3LoginTime=Mar 09 2017 12:34:56 GMT+00:00 dUser3=dUser3LoginTime=Mar 09 20 17 12:34:56 GMT+00:00 dUser2=dUser2LoginTime=Mar 09 2017 12:34:56 GMT+00:00 dUser3=dUser3LoginTime=Mar 09 2017 12:34:56 GMT+00:00 dUser3=dUser3LoginTime=Mar 09 2017...

Trend Micro Deep Discovery Email Inspector

The IBM QRadar DSM for Trend Micro Deep Discovery Email Inspector collects events from a Trend Micro Deep Discovery Email Inspector device.

The following table describes the specifications for the Trend Micro Deep Discovery Email Inspector DSM:

Table 589. Trend Micro Deep Discovery Email Inspector DSM specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Trend Micro</td>
</tr>
</tbody>
</table>
To integrate Trend Micro Deep Discovery Email Inspector 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:
   - Trend Micro Deep Discovery Email Inspector DSM RPM
   - DSM Common RPM

2. Configure your Trend Micro Deep Discovery Email Inspector device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a Trend Micro Deep Discovery Email Inspector log source on the QRadar Console. The following table describes the parameters that require specific values for Trend Micro Deep Discovery Email Inspector event collection:

```plaintext
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Trend Micro Deep Discovery Email Inspector</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>
```

**Related tasks**

“Adding a DSM” on page 4  
“Adding a log source” on page 4

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 Trend Micro Deep Discovery Email Inspector to communicate with QRadar**

To collect events from Trend Micro Deep Discovery Email Inspector, configure a syslog server profile for the IBM QRadar host.

**Procedure**

1. Log in to the Trend Micro Deep Discovery Email Inspector user interface.
2. Click **Administration > Log Settings**.
3. Click **Add**.
4. Verify that **Enabled** is selected for **Status**. The default is **Enabled**.
5. Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Specify a name for the profile.</td>
</tr>
<tr>
<td>Syslog server</td>
<td>The host name or IP of the QRadar server.</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
<tr>
<td>Log format</td>
<td>LEEF</td>
</tr>
</tbody>
</table>

6. Select **Detections, Virtual Analyzer Analysis logs**, and **System events** for the types of events to send to QRadar.

### Trend Micro Deep Discovery Inspector

The IBM QRadar DSM for Trend Micro Deep Discovery Inspector can receive event logs from your Trend Micro Deep Discovery Inspector console.

The following table identifies the specifications for the Trend Micro Deep Discovery Inspector DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Trend Micro</td>
</tr>
<tr>
<td>DSM name</td>
<td>Trend Micro Deep Discovery Inspector</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-TrendMicroDeepDiscovery-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V3.0 to V3.8, V5.0 and V5.1</td>
</tr>
<tr>
<td>Event format</td>
<td>LEEF</td>
</tr>
<tr>
<td>QRadar recorded event types</td>
<td>Malicious content, Malicious behavior, Suspicious behavior, Exploit, Grayware, Web reputation, Disruptive application, Sandbox, Correlation, System, Update</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Included identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>
To send Trend Micro Deep Discovery Inspector events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the following RPMs:
   - DSMCommon RPM
   - Trend Micro Deep Discovery Inspector DSM

2. Configure your Trend Micro Deep Discovery Inspector device to send events to QRadar.

3. If QRadar does not automatically detect Trend Micro Deep Discovery Inspector as a log source, create a Trend Micro Deep Discovery Inspector log source on the QRadar Console. The following table shows the protocol-specific values for Trend Micro Deep Discovery Inspector event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Trend Micro Deep Discovery Inspector</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

**Related tasks**

- “Adding a DSM” on page 4
- “Adding a log source” on page 4

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 Trend Micro Deep Discovery Inspector V3.0 to send events to QRadar**

To collect Trend Micro Deep Discovery Inspector events, configure the device to send events to IBM QRadar.

**Procedure**

1. Log in to Trend Micro Deep Discovery Inspector.
2. From the navigation menu, select **Logs > Syslog Server Settings**.
3. Select **Enable Syslog Server**.
4. Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The IP address of your QRadar Console or Event Collector.</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
<tr>
<td>Syslog facility</td>
<td>The local facility, for example, <strong>local 3</strong>.</td>
</tr>
<tr>
<td>Syslog severity</td>
<td>The minimum severity level that you want to include.</td>
</tr>
<tr>
<td>Syslog format</td>
<td>LEEF</td>
</tr>
</tbody>
</table>

5. In the **Detections** pane, select the check boxes for the events that you want to forward to QRadar.
6. Click **Save**.
Configuring Trend Micro Deep Discovery Inspector V3.8, V5.0 and V5.1 to send events to QRadar

To collect Trend Micro Deep Discovery Inspector events, configure the device to send events to IBM QRadar.

Procedure

1. Log in to Trend Micro Deep Discovery Inspector.
2. Click Administration > Integrated Products/Services > Syslog.
3. Click Add, and then select Enable Syslog Server.
4. Configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name or IP address</td>
<td>The IP address of your QRadar Console or Event Collector.</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Facility level</td>
<td>Select a facility level that specifies the source of a message.</td>
</tr>
<tr>
<td>Severity level</td>
<td>Select a severity level of the type of messages to be sent to the syslog server.</td>
</tr>
<tr>
<td>Log format</td>
<td>LEEF</td>
</tr>
</tbody>
</table>

5. In the Detections pane, select the check boxes for the events that you want to forward to QRadar.
6. If you need proxy servers for your connections, select Connect through a proxy server. The device uses the settings that are configured in the Administrator > System Settings > Proxy screen.

Note: If you require the use of proxy servers for intranet connections, select this option.
7. Click Save.

Trend Micro Deep Security


The following table identifies the specifications for the Trend Micro Deep Security DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Trend Micro</td>
</tr>
<tr>
<td>DSM name</td>
<td>Trend Micro Deep Security</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-TrendMicroDeepSecurity-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V9.6.1532, V10.0.1962, V10.1</td>
</tr>
<tr>
<td>Event format</td>
<td>Log Event Extended Format</td>
</tr>
</tbody>
</table>
To integrate Trend Micro Deep Security 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:
   - Trend Micro Deep Security DSM RPM
   - DSMCommon RPM

2. Configure your Trend Micro Deep Security device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a Trend Micro Deep Security DSM log source on the QRadar Console. The following table describes the parameters that require specific values for Trend Micro Deep Security DSM event collection:

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Trend Micro Deep Security</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>
```

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 Trend Micro Deep Security to communicate with QRadar**

To collect all events from Trend Micro Deep Security, you must specify IBM QRadar as the Syslog server and configure the Syslog format on your Trend Micro Deep Security device.

**Before you begin**

Ensure that Deep Security Manager is installed and configured on your Trend Micro Deep Security Device.
Procedure
1. Click Administration > System Settings > SIEM.
2. From the System Event Notification pane in the Manager section, enable the Forward System Events to remote computer (via Syslog) option.
3. Type the host name or the IP address of the QRadar system.
4. Type 514 for the UDP port.
5. Select the Syslog Facility that you want to use.

   Note: Trend Micro Deep Security sends events only in LEEF format from the Deep Security Manager. If you select the Direct forward option on the SIEM tab, you can't select Log Event Extended Format 2.0 for the Syslog Format.

Trend Micro InterScan VirusWall

The Trend Micro InterScan VirusWall DSM for IBM QRadar accepts events by using syslog.

To configure QRadar to receive events from an InterScan VirusWall device, select Trend InterScan VirusWall from the Log Source Type List.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Trend InterScan VirusWall</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>IP address or host name for the log source</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

For more information about your Trend Micro InterScan VirusWall device, see your vendor documentation.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Trend Micro Office Scan

A Trend Micro Office Scan DSM for IBM QRadar accepts events by using SNMPv2.

QRadar records events relevant to virus and spyware events. Before you configure a Trend Micro device in QRadar, you must configure your device to forward SNMPv2 events.

QRadar has several options for integrating with a Trend Micro device. The integration option that you choose depends on your device version:

- “Integrating with Trend Micro Office Scan 8.x ” on page 1122
- “Integrating with Trend Micro Office Scan 10.x ” on page 1123
- “Integrating with Trend Micro OfficeScan XG ” on page 1124

Related concepts
“SNMPv2 protocol configuration options” on page 83
You can configure a log source to use the SNMPv2 protocol to receive SNMPv2 events.

**Related tasks**

“Adding a DSM” on page 4

“Adding a log source” on page 4

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

**Integrating with Trend Micro Office Scan 8.x**

You can integrate a Trend Micro Office Scan 8.x device with IBM QRadar.

**Procedure**

1. Log in to the Office Scan Administration interface.
2. Select **Notifications**.
3. Configure the General Settings for SNMP Traps: In the **Server IP Address** field, type the IP address of the QRadar.
   
   **Note:** Do not change the community trap information.
4. Click **Save**.
5. Configure the Standard Alert Notification: Select **Standard Notifications**.
6. Click the **SNMP Trap** tab.
7. Select the **Enable notification via SNMP Trap for Virus/Malware Detections** check box.
8. Type the following message in the field (this should be the default):

   Virus/Malware: %v Computer: %s Domain: %m File: %p Date/Time: %y Result: %a

9. Select the **Enable notification via SNMP Trap for Spyware/Grayware Detections** check box.
10. Type the following message in the field (this should be the default):

    Spyware/Grayware: %v Computer: %s Domain: %m Date/Time: %y Result: %a

11. Click **Save**.
12. Configure Outbreak Alert Notifications: Select **Out Notifications**.
13. Click the **SNMP Trap** tab.
14. Select the **Enable notification via SNMP Trap for Virus/Malware Outbreaks** check box.
15. Type the following message in the field (this should be the default):

    Number of viruses/malware: %CV Number of computers: %CC Log Type Exceeded: %A Number of firewall violation logs: %C Number of shared folder sessions: %S Time Period: %T

16. Select the **Enable notification via SNMP Trap for Spyware/Grayware Outbreaks** check box.
17. Type the following message in the field (this should be the default):

    Number of spyware/grayware: %CV Number of computers: %CC Log Type Exceeded: %A Number of firewall violation logs: %C Number of shared folder sessions: %S Time Period: %T

18. Click **Save**.

You are now ready to configure the log sources in QRadar.

19. To configure the Trend Micro Office Scan device:

   a) From the **Log Source Type** list, select the **Trend Micro Office Scan** option.

   b) From the **Protocol Configuration** list, select the **SNMPv2** option.
Integrating with Trend Micro Office Scan 10.x
Several preparatory steps are necessary before you configure IBM QRadar to integrate with a Trend Micro Office Scan 10.x device.

About this task
You must:
1. Configure the SNMP settings for Trend Micro Office Scan 10.x.
2. Configure standard notifications.
3. Configure outbreak criteria and alert notifications.

Configuring General Settings
You can integrate a Trend Micro Office Scan 10.x device with IBM QRadar.

Procedure
1. Log in to the Office Scan Administration interface.
2. Select Notifications > Administrator Notifications > General Settings.
3. Configure the General Settings for SNMP Traps: In the Server IP Address field, type the IP address of your QRadar.
4. Type a community name for your Trend Micro Office Scan device.
5. Click Save.

What to do next
You must now configure the Standard Notifications for Office Scan.

Configure Standard Notifications
You can configure standard notifications.

Procedure
2. Define the Criteria settings. Click the Criteria tab.
3. Select the option to alert administrators on the detection of virus/malware and spyware/grayware, or when the action on these security risks is unsuccessful.
4. To enable notifications: Configure the SNMP Trap tab.
5. Select the Enable notification via SNMP Trap check box.
6. Type the following message in the field:
   Virus/Malware: %v Spyware/Grayware: %T Computer: %s IP address: %i Domain: %m File: %p Date/Time: %y Result: %a User name: %n
7. Click Save.

What to do next
You must now configure Outbreak Notifications.

Configuring Outbreak Criteria and Alert Notifications
You can configure outbreak criteria and alert notifications for your Trend Micro Office Scan device.

Procedure
1. Select Notifications > Administrator Notifications > Outbreak Notifications.
2. Click the Criteria tab.
3. Type the number of detections and detection period for each security risk.
Notification messages are sent to an administrator when the criteria exceeds the specified detection limit.

**Note:** Trend Micro suggests that you use the default values for the detection number and detection period.

4. Select **Shared Folder Session Link** and enable Office Scan to monitor for firewall violations and shared folder sessions.

**Note:** To view computers on the network with shared folders or computers currently browsing shared folders, you can select the number link in the interface.

5. Click the **SNMP Trap** tab.
   a) Select the **Enable notification via SNMP Trap** check box.

6. Type the following message in the field:
   - Number of virus/malware: %CV
   - Number of computers: %CC
   - Log Type Exceeded: %A
   - Number of firewall violation logs: %C
   - Number of shared folder sessions: %S
   - Time Period: %T

7. Click **Save**.

8. You are now ready to configure the log source in QRadar.

   **Configure the Trend Micro Office Scan device:**
   a) From the **Log Source Type** list, select the **Trend Micro Office Scan** option.
   b) From the **Protocol Configuration** list, select the **SNMPv2** option.

**Integrating with Trend Micro OfficeScan XG**

You can integrate a Trend Micro OfficeScan XG device with the QRadar system.

**About this task**

Before you can integrate a Trend Micro OfficeScan XG device with the QRadar system you must configure the following items:
- SNMP settings for Trend Micro OfficeScan XG
- Administrator notifications
- Outbreak notifications

**Configuring General Settings in OfficeScan XG**

You can integrate a Trend Micro OfficeScan XG device with IBM QRadar.

**Procedure**

1. Log in to the OfficeScan Administration interface.
2. Click **Administration > Notifications > General Settings**.
3. Configure the General Notification Settings for SNMP Traps.
4. In the **Server IP Address** field, type the IP address of the QRadar Console.
5. Type a community name for your Trend Micro OfficeScan device.
6. Click **Save**.

**What to do next**

You must now configure the Administrator Notifications for OfficeScan.
Configuring Administrator Notifications in OfficeScan XG
Administrators can be notified when certain security risks are detected by Trend Micro OfficeScan XG. Configure the device to send notifications through SNMP Trap.

Procedure
1. Click Administration > Notifications > Administrator.
2. Click the Criteria tab.
3. Select the following options for notification:
   - Virus/Malware Detection
   - Spyware/Grayware Detection
   - C&C Callbacks
4. Optional: To enable notifications, configure the SNMP Trap tab.
5. Select the Enable notification via SNMP Trap check box.
6. Type the following message in the field:
   - Virus/Malware: %v Spyware/Grayware: %T Computer: %s IP address: %i Domain: %m File: %p Date/Time: %y Result: %a User name: %n
   - Spyware/Grayware: %v Endpoint: %s Domain: %m Date/Time: %y Result: %a
   - Compromised Host: %CLIENTCOMPUTER% IP Address: %IP% Domain: %DOMAIN% Date/Time: %DATETIME% Callback address: %CALLBACKADDRESS% C&C risk level: %CNCRISKLEVEL% C&C list source: %CNCLISTSOURCE% Action: %ACTION%
7. Click Save.

What to do next
You must now configure Outbreak Notifications.

Configuring Outbreak Notifications in OfficeScan XG
You can configure your Trend Micro OfficeScan XG device to notify you of security risk outbreaks. Define an outbreak by the number of detections and the detection period.

Procedure
1. Click Administration > Notifications > Outbreak.
2. Click the Criteria tab.
3. Type the number of detections and detection period for each security risk.
   - Note: Notification messages are sent to an administrator when the criteria exceeds the specified detection limit.
   - Tip: Trend Micro suggests that you use the default values for the detection number and detection period.
4. To enable notifications, click the SNMP Trap tab, and select the Enable notification via SNMP Trap check box.
5. Type the following message in the field:
   - Number of virus/malware: %CV Number of computers: %CC
   - Number of spyware/grayware: %CV Number of endpoints: %CC
   - C&C callback detected: Accumulated log count: %C in the last %T hour(s)
6. Click Save.

What to do next
You are now ready to configure the log source in QRadar.
The Tripwire DSM accepts resource additions, removal, and modification events by using syslog.

**Procedure**
1. Log in to the Tripwire interface.
2. On the left navigation, click Actions.
3. Click New Action.
4. Configure the new action.
5. Select Rules and click the rule that you want to monitor.
6. Select the Actions tab.
7. Make sure that the new action is selected.
8. Click OK.
   You are now ready to configure the log source in QRadar.
10. To configure QRadar to receive events from a Tripwire device: From the Log Source Type list, select the Tripwire Enterprise option.
    For more information about your Tripwire device, see your vendor documentation.

**Related tasks**
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 155. Tropos Control

The Tropos Control DSM for IBM QRadar accepts events by using syslog.

About this task
QRadar can record all fault management, login and logout events, provisioning events, and device image upload events. Before you configure QRadar, you must configure your Tropos Control to forward syslog events.

You can configure Tropos Control to forward logs by using syslog to QRadar.

Procedure
1. Use an SSH to log in to your Tropos Control device as a root user.
2. Open the following file for editing:
   `/opt/ControlServer/ems/conf/logging.properties`
3. To enable syslog, remove the comment marker (`#`) from the following line:
   `#log4j.category.syslog = INFO, syslog`
4. To configure the IP address for the syslog destination, edit the following line:
   `log4j.appender.syslog.SyslogHost = <IP address>`
   Where `<IP address>` is the IP address or host name of QRadar.
   By default, Tropos Control uses a facility of USER and a default log level of INFO. These default settings are correct for syslog event collection from a Tropos Control device.
5. Save and exit the file.
6. You are now ready to configure the Tropos Control DSM in QRadar.

   To configure QRadar to receive events from Tropos Control:
   a) From the Log Source Type list, select Tropos Control.

Related tasks
“Adding a DSM” on page 4
“Adding a log source” on page 4
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 156. Universal

IBM QRadar can collect and correlates events from any network infrastructure or security device by using the Universal DSM.

After the events are collected and before the correlation can begin. The individual events from your devices must be properly parsed to determine the event name, IP addresses, protocol, and ports. For common network devices, such as Cisco Firewalls, predefined DSMs are engineered for QRadar to properly parse and classify the event messages from the respective devices. After the events from a device are parsed by the DSM, QRadar can continue to correlate events into offenses.

If an enterprise network has one or more network or security devices that are not officially supported, where no specific DSM for the device exists, you can use the Universal DSM. The Universal DSM gives you the option to forward events and messages from unsupported devices and use the Universal DSM to categorize the events for QRadar. QRadar can integrate with virtually any device or any common protocol source 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 by using the log sources window from the Admin tab, you must create an extensions document for the log source.

For more information about writing and testing a Universal DSM, see the support forum at https://www.ibm.com/developerworks/community/forums.

Related concepts
“Log source extensions” on page 107
An extension document can extend or modify how the elements of a particular log source are parsed. You can use the extension document to correct a parsing issue or override the default parsing for an event from an existing DSM.

Related tasks
“Adding a log source” on page 4
If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Universal CEF

The IBM 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>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSM name</td>
<td>Universal CEF</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-UniversalCEF-Qradar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td></td>
<td>Log File</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>CEF-formatted events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 596. Universal CEF DSM specifications (continued)

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>Universal CEF</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog or Log File</td>
</tr>
</tbody>
</table>

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 QRadar User 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 QRadar 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**.

---

**Universal LEEF**

The Universal LEEF DSM for IBM QRadar can accept events from devices that produce events using the Log Event Extended Format (LEEF).

The LEEF event format is a proprietary event format, which allows hardware manufacturers and software product manufacturers to read and map device events specifically designed for QRadar integration.

LEEF formatted events sent to QRadar outside of the partnership program require you to have installed the Universal LEEF DSM and manually identify each event forwarded to QRadar by mapping unknown events. The Universal LEEF DSM can parse events forwarded from syslog or files containing events in the LEEF format polled from a device or directory using the Log File protocol.

To configure events in QRadar using Universal LEEF, you must:

1. Configure a Universal LEEF log source in QRadar.
2. Send LEEF formatted events from your device to QRadar. For more information on forwarding events, see your vendor documentation.
3. Map unknown events to QRadar Identifiers (QIDs).

**Configuring a Universal LEEF log source**

Before you configure your device to send events to IBM QRadar, you must add a log source for the device providing LEEF events.

**About this task**

QRadar can receive events from a real-time source using syslog or files stored on a device or in a repository using the Log File protocol.

To configure a log source for Universal LEEF using syslog:

**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 **Universal LEEF**.
9. Using the **Protocol Configuration** list, select **Syslog**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 597. Syslog protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

The log source is added to QRadar. You are now ready to forward LEEF events to QRadar.

**Configuring the log file protocol to collect Universal LEEF events**
The Log File protocol allows IBM QRadar to retrieve archived event or log files from a remote host or file repository.

**About this task**
The files are transferred, one at a time, to QRadar for processing. QRadar reads the event files and updates the log source with new events. Due to the Log File protocol polling for archive files, the events are not provided in real-time, but added in bulk. The log file protocol can manage plain text, compressed files, or archives.

**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. In the **Log Source Name** field, type a name for the Universal LEEF log source.
6. In the **Log Source Description** field, type a description for the Universal LEEF log source.
7. From the **Log Source Type** list, select **Universal LEEF**.
8. Using the **Protocol Configuration** list, select **Log File**.
9. Configure the following parameters:

<table>
<thead>
<tr>
<th>Table 598. Log file protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
</tbody>
</table>
| **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 host from which you want to receive files. |
| **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 to 65535. |
| **Remote User**                 | Type the username necessary to log in to the host running the selected Service Type. The username can be up to 255 characters in length. |
| **Remote Password**             | Type the password necessary to log in to the host containing the LEEF event files. |
| **Confirm Password**            | Confirm the Remote Password to log in to the host containing the LEEF event files. |
| **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 option is ignored. |
| **Remote Directory**            | Type the directory location on the remote host from which the files are retrieved.  
  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. By default, the check box is clear.  
  The Recursive parameter is not used if you configure SCP as the Service Type. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP File Pattern</td>
<td>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. For example, if you want to list all files starting with the word log, followed by one or more digits and ending with .tar.gz, use the following entry: ( \text{log}[0-9]+\cdot\text{tar}\cdot\text{gz} ). Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: <a href="http://download.oracle.com/javase/tutorial/essential/regex/">http://download.oracle.com/javase/tutorial/essential/regex/</a>.</td>
</tr>
<tr>
<td>FTP Transfer Mode</td>
<td>This option is only displayed if you select FTP as the Service Type. The FTP Transfer Mode parameter allows you to define the file transfer mode when retrieving log files over FTP. 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. You must select NONE as the Processor and LINEBYLINE as the Event Generator when using ASCII as the FTP Transfer Mode.</td>
</tr>
<tr>
<td>SCP Remote File</td>
<td>If you select SCP as the Service Type you must type the file name of the remote file.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Type the time of day you want 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.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>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.</td>
</tr>
<tr>
<td>Run On Save</td>
<td>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.</td>
</tr>
<tr>
<td>EPS Throttle</td>
<td>Type the number of Events Per Second (EPS) that you do not want this protocol to exceed. The valid range is 100 to 5000.</td>
</tr>
<tr>
<td>Processor</td>
<td>If the files located 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 processed.</td>
</tr>
</tbody>
</table>
Table 598. Log file protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore Previously Processed File(s)</td>
<td>Select this check box to track files that have already been processed that you do not want to be processed a second time. This only applies to FTP and SFTP Service Types.</td>
</tr>
<tr>
<td>Change Local Directory?</td>
<td>Select this check box to define the local directory on your QRadar system that you want to use for storing downloaded files during processing.</td>
</tr>
<tr>
<td></td>
<td>We recommend that you leave this check box clear. When the check box is selected, the Local Directory field is displayed, allowing you to configure the local directory to use for storing files.</td>
</tr>
<tr>
<td>Event Generator</td>
<td>From the Event Generator list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. The LineByLine option reads each line of the file as single event. For example, if a file has 10 lines of text, 10 separate events are created.</td>
</tr>
</tbody>
</table>

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

The log source is added to QRadar. You are now ready to write LEEF events that can be retrieved using the Log file protocol.

**Forwarding events to IBM QRadar**

After you create your log source, you can forward or retrieve events for QRadar. Forwarding events by using syslog might require more configuration of your network device.

As events are discovered by QRadar, either using syslog or polling for log files, events are displayed in the Log Activity tab. Events from the devices that forward LEEF events are identified by the name that you type in the Log Source Name field. The events for your log source are not categorized by default in QRadar and they require categorization. For more information on categorizing your Universal LEEF events, see “Universal LEEF event map creation” on page 1137.

**Universal LEEF event map creation**

Event mapping is required for the Universal LEEF DSM, because Universal LEEF events do not contain a predefined QRadar Identifier (QID) map to categorize security events.

Members of the SIPP Partner Program have QID maps designed for their network devices, whereby the configuration is documented, and the QID maps are tested by IBM Corp.

The Universal LEEF DSM requires that you individually map each event for your device to an event category in IBM QRadar. Mapping events allows QRadar to identify, coalesce, and track events that recur from your network devices. Until you map an event, all events that are displayed in the Log Activity tab for the Universal LEEF DSM are categorized as unknown. Unknown events are easily identified as the Event Name column and Low-Level Category columns display Unknown.
Discovering unknown events
As your device forwards events to IBM QRadar, it can take time to categorize all of the events from a
device, because some events might not be generated immediately by the event source appliance or
software.

About this task
It is helpful to know how to quickly search for unknown events. When you know how to search for
unknown events, you can repeat this search until you are happy that most of your Universal LEEF events
are identified.

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 the log source group or Other.
   Log sources that are not assigned to a group are categorized as Other.
6. From the Log Source list, select your Universal LEEF log source.
7. Click Add Filter.
   The Log Activity tab is displayed with a filter for your Universal LEEF DSM.
8. From the View list, select Last Hour.
   Any events that are generated by your Universal LEEF DSM in the last hour are displayed. Events that
   are displayed as unknown in the Event Name column or Low Level Category column require event
   mapping in QRadar.
   Note: You can save your existing search filter by clicking Save Criteria.
   You are now ready to modify the event map for your Universal LEEF DSM.

Modifying an event map
Modifying an event map allows you to manually categorize events to a IBM QRadar Identifier (QID) map.

About this task
Any event categorized to a log source can be remapped to a new QRadar Identifier (QID). By default, the
Universal LEEF DSM categorizes all events as unknown.

Note: Events that do not have a defined log source cannot be mapped to an event. Events without a log
source display SIM Generic Log in the Log Source column.

Procedure
1. On the Event Name column, double-click an unknown event for your Universal LEEF DSM.
   The detailed event information is displayed.
2. Click Map Event.
3. From the Browse for QID pane, select any of the following search options to narrow the event
categories for a QRadar Identifier (QID):
   a) From the High-Level Category list, select a high-level event categorization.
      For a full list of high-level and low-level event categories or category definitions, see the Event
      Categories section of the IBM QRadar Administration Guide.
   4. From the Low-Level Category list, select a low-level event categorization.
   5. From the Log Source Type list, select a log source type.
The **Log Source Type** list allows you to search for QIDs from other individual log sources. Searching for QIDs by log source is useful when the events from your Universal LEEF DSM are similar to another existing network device. For example, if your Universal DSM provides firewall events, you might select Cisco ASA, as another firewall product that likely captures similar events.

6. To search for a QID by name, type a name in the **QID/Name** field.

   The QID/Name field allows you to filter the full list of QIDs for a specific word, for example, MySQL.

7. Click **Search**.

   A list of QIDs is displayed.

8. Select the QID you want to associate to your unknown Universal LEEF DSM event.

9. Click **OK**.

   QRadar maps any additional events forwarded from your device with the same QID that matches the event payload. The event count increases each time the event is identified by QRadar.

**Note:** If you update an event with a new QRadar Identifier (QID) map, past events stored in QRadar are not updated. Only new events are categorized with the new QID.
Chapter 157. Vectra Networks Vectra

The IBM QRadar DSM for Vectra Networks Vectra collects events from the Vectra Networks Vectra X-Series platform.

The following table describes the specifications for the Vectra Networks Vectra DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Vectra Networks</td>
</tr>
<tr>
<td>DSM name</td>
<td>Vectra Networks Vectra</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-VectraNetworksVectra-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V2.2</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event Format</td>
<td>Common Event Format</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>Host scoring, command and control, botnet activity, reconnaissance, lateral movement, exfiltration</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Vectra Networks Website (<a href="http://www.vectranetworks.com">http://www.vectranetworks.com</a>)</td>
</tr>
</tbody>
</table>

To integrate Vectra Networks Vectra 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 in the order that they are listed:
   - DSMCommon RPM
   - Vectra Networks Vectra DSM RPM

2. Configure your Vectra Networks Vectra device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a Vectra Networks Vectra log source on the QRadar Console. The following table describes the parameters that require specific values for Vectra Networks Vectra event collection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source type</td>
<td>Vectra Networks Vectra</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>Syslog</td>
</tr>
<tr>
<td>Log Source Identifier</td>
<td>A unique identifier for the log source.</td>
</tr>
</tbody>
</table>

The following table provides a sample event message for the Vectra Networks Vectra DSM:
### Related tasks

- **“Adding a DSM” on page 4**
- **“Adding a log source” on page 4**

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 Vectra Networks Vectra to communicate with QRadar

To collect Vectra Networks Vectra events, configure the QRadar syslog daemon listener.

### Procedure

1. Log in to the Vectra web console.
2. Click **settings > Notifications**.
3. In the **Syslog** section, click **Edit**.
4. Configure the following QRadar syslog daemon listener parameters:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The QRadar Event Collector IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>514</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
</tr>
<tr>
<td>Format</td>
<td>CEF</td>
</tr>
</tbody>
</table>

---

Table 601. Vectra Networks Vectra sample message.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Low level category</th>
<th>Sample log message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Scoring</td>
<td>Backdoor Detected</td>
<td>`&lt;13&gt;Dec 22 16:38:53 &lt;Server&gt; - -: CEF:0</td>
</tr>
</tbody>
</table>

---

1142 IBM QRadar : QRadar DSM Configuration Guide
Chapter 158. Venustech Venusense

The Venustech Venusense DSM for IBM QRadar can collect events from Venusense appliances by using syslog.

QRadar records all relevant unified threat, firewall, or network intrusion prevention events that are forwarded by using syslog on port 514.

The following Venustech appliances are supported by QRadar:

• Venustech Venusense Security Platform
• Venustense Unified Threat Management (UTM)
• Venusense Firewall
• Venusense Network Intrusion Prevention System (NIPS)

Venusense configuration overview

IBM QRadar can collect events from Venustech appliances that are configured to forward filtered event logs in syslog format to QRadar.

The following process outlines the steps that are required to collect events from a Venusense Venustech appliance:

1. Configure the syslog server on your Venusense appliance.
2. Configure a log filter on your Venusense appliance to forward specific event logs.
3. Configure a log source in QRadar to correspond to the filtered log events.

Configuring a Venusense syslog server

To forward events to IBM QRadar, you must configure and enable a syslog server on your Venusense appliance with the IP address of your QRadar Console or Event Collector.

Procedure

1. Log in to the configuration interface for your Venusense appliance.
2. From the navigation menu, select Logs > Log Configuration > Log Servers.
3. In the IP Address field, type the IP address of your QRadar Console or Event Collector.
4. In the Port field, type 514.
5. Select the Enable check box.
6. Click OK.

What to do next
You are ready to configure your Venusense appliance to filter which events are forwarded to QRadar.

Configuring Venusense event filtering

Event filtering determines which events your Venusense appliance forwards to IBM QRadar.

Procedure

1. From the navigation menu, select Logs > Log Configuration > Log Filtering.
2. In the Syslog Log column, select a check box for each event log you want to forward to QRadar.

© Copyright IBM Corp. 2005, 2019
3. From the list, select a syslog facility for the event log you enabled.
4. Repeat “Configuring Venuse event filtering” on page 1143 and “Configuring Venuse event filtering” on page 1143 to configure any additional syslog event filters.
5. Click OK.

**What to do next**

You can now configure a log source for your Venuse appliance in QRadar. QRadar does not automatically discover or create log sources for syslog events from Venuse appliances.

### Configuring a Venuse log source

To integrate Venuse syslog events, you must manually create a log source in IBM QRadar as Venuse events to not automatically discover.

**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 your Venustech Venuse appliance.
   
   The type of log source that you select is determined by the event filter that is configured on your Venuse appliance. The options include the following types:
   
   - **Venustech Venuse Security Platform** - Select this option if you enabled all event filter options.
   - **Venustech Venuse UTM** - Select this option if you enabled unified filtering events.
   - **Venustech Venuse Firewall** - Select this option if you enabled filtering for firewall events.
   - **Venustech Venuse NIPS** - Select this option if you enabled filtering for firewall events.
9. From the **Protocol Configuration** list, select **Syslog**.
10. In the **Log Source Identifier** field, type the IP address or host name for the log source as an identifier for your Venuse appliance.
11. Click **Save**.
12. On the Admin tab, click **Deploy Changes**.

   The configuration is complete. Events that are forwarded to QRadar by your Venuse appliance are displayed on the **Log Activity** tab.
Chapter 159. Verdasys Digital Guardian

The Verdasys Digital Guardian DSM for IBM QRadar accepts and categorizes all alert events from Verdasys Digital Guardian appliances.

Verdasys Digital Guardian is a comprehensive Enterprise Information Protection (EIP) platform. Digital Guardian serves as a cornerstone of policy driven, data-centric security by enabling organizations to solve the information risk challenges that exist in today's highly collaborative and mobile business environment. Digital Guardian’s endpoint agent architecture makes it possible to implement a data-centric security framework.

Verdasys Digital Guardian allows business and IT managers to:

• Discover and classify sensitive data by context and content.
• Monitor data access and usage by user or process.
• Implement policy driven information protection automatically.
• Alert, block, and record high risk behavior to prevent costly and damaging data loss incidents.

Digital Guardian's integration with QRadar provides context from the endpoint and enables a new level of detection and mitigation for Insider Threat and Cyber Threat (Advanced Persistent Threat).

Digital Guardian provides QRadar with a rich data stream from the end-point that includes: visibility of every data access by users or processes that include the file name, file classification, application that is used to access the data and other contextual variables.

The following table describes the specifications for the Verdasys Digital Guardian DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Verdasys Digital Guardian</td>
</tr>
<tr>
<td>DSM name</td>
<td>Verdasys Digital Guardian</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-VerdasysDigitalGuardian-QRadar_version-Build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V6.1.x and V7.2.1.0248 with the QRadar LEEF format</td>
</tr>
<tr>
<td></td>
<td>V6.0x with the Syslog event format</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog, LEEF</td>
</tr>
<tr>
<td>Event format</td>
<td>Syslog</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Digital Guardian website (<a href="https://digitalguardian.com">https://digitalguardian.com</a>)</td>
</tr>
</tbody>
</table>
Configuring IPtables

Before you configure your Verdasys Digital Guardian to forward events, you must configure IPtables in IBM QRadar to allow ICMP requests from Verdasys Digital Guardian.

Procedure

1. Use an SSH to log in to QRadar as the root user.
   
   Login: root
   
   Password: <password>

2. Type the following command to edit the IPtables file:
   
   vi /opt/qradar/conf/iptables.post

   The IPtables configuration file is displayed.

3. Type the following commands to allow QRadar to accept ICMP requests from Verdasys Digital Guardian:
   
   -I QChain 1 -m icmp -p icmp --icmp-type 8 --src <IP address> -j ACCEPT
   -I QChain 1 -m icmp -p icmp --icmp-type 0 --src <IP address> -j ACCEPT

   Where <IP address> is the IP address of your Verdasys Digital Guardian appliance. For example,
   
   -I QChain 1 -m icmp -p icmp --icmp-type 8 --src <Source_IP_address> -j ACCEPT
   -I QChain 1 -m icmp -p icmp --icmp-type 0 --src <Source_IP_address> -j ACCEPT

   Note: Make sure that you specify "--icmp-type" in the commands to avoid failures when you're upgrading the IPTables.

4. Save your IPtables configuration.

5. Type the following command to update IPtables in QRadar:
   
   /opt/qradar/bin/iptables_update.pl

6. To verify that QRadar accepts ICMP traffic from your Verdasys Digital Guardian, type the following command:
   
   iptables --list --line-numbers

   The following output is displayed:

<table>
<thead>
<tr>
<th>num</th>
<th>target</th>
<th>prot</th>
<th>opt</th>
<th>source</th>
<th>destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ACCEPT</td>
<td>icmp</td>
<td>--</td>
<td>&lt;IP address&gt;</td>
<td>icmp echo-reply</td>
</tr>
<tr>
<td>2</td>
<td>ACCEPT</td>
<td>icmp</td>
<td>--</td>
<td>&lt;IP address&gt;</td>
<td>icmp echo-request</td>
</tr>
<tr>
<td>3</td>
<td>ACCEPT</td>
<td>tcp</td>
<td>--</td>
<td>anywhere</td>
<td>state NEW tcp dpt:https</td>
</tr>
<tr>
<td>4</td>
<td>ACCEPT</td>
<td>tcp</td>
<td>--</td>
<td>anywhere</td>
<td>state NEW tcp dpt:http</td>
</tr>
</tbody>
</table>

   The IPtables configuration for QRadar is complete.
Configuring a data export

Data exports give you the option to configure the events Verdasys Digital Guardian forwards to IBM QRadar.

Procedure

1. Log in to the Digital Guardian Management Console.
2. Select **Workspace > Data Export > Create Export**.
3. From the **Data Sources** list, select **Alerts** or **Events** as the data source.
4. From the **Export type** list, select QRadar LEEF.

   If your Verdasys Digital Guardian is v6.0.x, you can select **Syslog** as the **Export Type**. QRadar LEEF is the preferred export type format for all Verdasys Digital Guardian appliances with v6.1.1 and later.
5. From the **Type** list, select **UDP** or **TCP** as the transport protocol.

   QRadar can accept syslog events from either transport protocol. If the length of your alert events typically exceeds 1024 bytes, then you can select **TCP** to prevent the events from being truncated.
6. In the **Server** field, type the IP address of your QRadar Console or Event Collector.
7. In the **Port** field, type **514**.
8. From the **Severity Level** list, select a severity level.
9. Select the **Is Active** check box.
10. Click **Next**.
11. From the list of available fields, add the following Alert or Event fields for your data export:

   - **Agent Local Time**
   - **Application**
   - **Computer Name**
   - **Detail File Size**
   - **IP Address**
   - **Local Port**
   - **Operation** (required)
   - **Policy**
   - **Remote Port**
   - **Rule**
   - **Severity**
   - **Source IP Address**
   - **User Name**
   - **Was Blocked**
   - **Was Classified**
12. Select a Criteria for the fields in your data export and click **Next**.

   By default, the Criterion is blank.
13. Select a group for the criteria and click **Next**.

   By default, the Group is blank.
14. Click **Test Query**.

   A Test Query ensures that the database runs properly.
15. Click **Next**.
16. Save the data export.
The configuration is complete.

What to do next
The data export from Verdasys Digital Guardian occurs on a 5-minute interval. You can adjust this timing with the job scheduler in Verdasys Digital Guardian, if required. Events that are exported to QRadar by Verdasys Digital Guardian are displayed on the Log Activity tab.

Configuring a log source
IBM QRadar automatically discovers and creates a log source for data exports from Verdasys Digital Guardian appliances.

About this task
The following procedure is optional.

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 Verdasys Digital Guardian.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Identifier</td>
<td>Type the IP address or host name for the log source as an identifier for events from Verdasys Digital Guardian appliance.</td>
</tr>
</tbody>
</table>

11. Click Save.
12. On the Admin tab, click Deploy Changes.

The log source is added to QRadar.
Chapter 160. Vericept Content 360 DSM

The Vericept Content 360 DSM for IBM QRadar accepts Vericept events by using syslog.

**About this task**

QRadar records all relevant and available information from the event. Before you configure a Vericept device in QRadar, you must configure your device to forward syslog. For more information about configuring your Vericept device, consult your vendor documentation.

After you configure syslog to forward events to QRadar, the configuration is complete. The log source is added to QRadar as Vericept Content 360 events are automatically discovered. Events that are forwarded to QRadar by your Vericept Content 360 appliance are displayed on the **Log Activity** tab.

To manually configure a log source for QRadar to receive events from a Vericept device:

**Procedure**

From the **Log Source Type** list, select the **Vericept Content 360** option.

**Related tasks**

“Adding a DSM” on page 4
“Adding a log source” on page 4

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 161. VMWare

IBM QRadar supports a range of VMWare products.

VMware AppDefense

The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system. To integrate VMware AppDefense with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   • Protocol-Common RPM
   • VMWare AppDefense API Protocol RPM
   • DSMCommon RPM
   • VMWare AppDefense DSM RPM
2. Configure your VMware AppDefense device to send events to QRadar.
3. Add a VMWare AppDefense log source that uses the VMWare AppDefense API protocol on the QRadar Console.

Related concepts
VMware AppDefense sample event messages
Use these sample event messages as a way of verifying a successful integration with QRadar.

Related tasks
Configuring VMware AppDefense to communicate with QRadar
To send events to QRadar from your VMware AppDefense system, you must create a new API key on your VMware AppDefense system.

Configuring a VMware AppDefense log source by using the VMWare AppDefense API protocol
If you want to collect VMware AppDefense logs from VMware AppDefense, add a log source on the QRadar Console so that VMware AppDefense can communicate with QRadar by using the VMWare AppDefense API protocol.

Related reference
VMware AppDefense DSM specifications
The following table describes the specifications for the VMWare AppDefense DSM.

VMWare AppDefense DSM specifications

The following table describes the specifications for the VMWare AppDefense DSM.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>VMware</td>
</tr>
<tr>
<td>DSM name</td>
<td>VMWare AppDefense</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-VMWareAppDefense-QRadar_version-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>V1.0</td>
</tr>
<tr>
<td>Protocol</td>
<td>VMWare AppDefense API</td>
</tr>
<tr>
<td>Specification</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Event format</td>
<td>JSON</td>
</tr>
<tr>
<td>Recorded event types</td>
<td>All</td>
</tr>
<tr>
<td>Automatically discovered?</td>
<td>No</td>
</tr>
<tr>
<td>Includes identity?</td>
<td>No</td>
</tr>
<tr>
<td>Includes custom properties?</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td><a href="https://cloud.vmware.com/appdefense">VMware website</a></td>
</tr>
</tbody>
</table>

**Related concepts**
VMware AppDefense

The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system.

**Configuring VMware AppDefense to communicate with QRadar**

To send events to QRadar from your VMware AppDefense system, you must create a new API key on your VMware AppDefense system.

**Before you begin**

Ensure that you have access to the Integrations settings in the VMware AppDefense user interface so that you can generate the Endpoint URL and API Key that are required to configure a log source in QRadar. You must have the correct user permissions for the VMware AppDefense user interface to complete the following procedure:

**Procedure**

1. Log in to your VMware AppDefense user interface.
2. From the navigation menu, click the icon to the right of your user name, and then select **Integrations**.
3. Click **PROVISION NEW API KEY**.
4. In the **Integration Name** field, type a name for your integration.
5. Select an integration from the **Integration Type** list.
6. Click **PROVISION**, and then record and save the following information from the message in the window that opens. You need this information when you configure a log source in QRadar:
   - **EndPoint URL**
   - **API Key** - This is the **Authentication Token** parameter value when you configure a log source in QRadar.

**Note:** If you click **OK** or close the window, the information in the message can't be recovered.

**Related concepts**
VMware AppDefense
The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system.

Configuring a VMware AppDefense log source by using the VMWare AppDefense API protocol

If you want to collect VMware AppDefense logs from VMware AppDefense, add a log source on the QRadar Console so that VMware AppDefense can communicate with QRadar by using the VMWare AppDefense API protocol.

Procedure

1. Log in to QRadar.
2. Click the Admin tab.
3. Click the Log Sources icon.
4. Click Add.
5. From the Log Source Type list, select VMWare AppDefense.
6. From the Protocol Configuration list, select VMWare AppDefense API.
7. Configure the parameters.

The following table describes the parameters that require specific values to collect JSON events from VMware AppDefense by using the VMWare AppDefense API protocol:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Type</td>
<td>VMWare AppDefense</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>VMWare AppDefense API</td>
</tr>
<tr>
<td>Endpoint URL</td>
<td>The endpoint URL for accessing VMware AppDefense. Example revision: <a href="https://server_name.vmwaredrx.com/partnerapi/v1/orgs/">https://server_name.vmwaredrx.com/partnerapi/v1/orgs/</a>&lt;organization ID&gt;</td>
</tr>
<tr>
<td>Authentication Token</td>
<td>A single authentication token that is generated by the AppDefense console and must be used for all API transactions.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>If QRadar accesses the VMWare AppDefense API by using a proxy, enable Use Proxy.</td>
</tr>
<tr>
<td></td>
<td>If the proxy requires authentication, configure the Hostname, Proxy Port, Proxy Username, and Proxy fields.</td>
</tr>
<tr>
<td></td>
<td>If the proxy does not require authentication, configure the Hostname and Proxy Port fields.</td>
</tr>
<tr>
<td>Automatically Acquire Server Certificates</td>
<td>If you choose Yes from the drop down list, QRadar automatically downloads the certificate and begins trusting the target server. If No is selected QRadar does not attempt to retrieve any server certificates.</td>
</tr>
</tbody>
</table>
Table 604. VMWare AppDefense API protocol log source parameters (continued)
Parameter

Description

Recurrence

Beginning at the Start Time, type the frequency
for how often you want the remote directory to be
scanned. Type this value in hours(H), minutes(M),
or days(D). For example, 2H if you want the
directory to be scanned every 2 hours. The
default is 5M.

Throttle

The maximum number of events per second.
The default is 5000.

8. Click Save.
Related concepts
VMware AppDefense
The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system.

VMware AppDefense sample event messages
Use these sample event messages as a way of verifying a successful integration with QRadar.
The following table provides a sample event message when using the VMWare AppDefense API protocol
for theVMWare AppDefense DSM:
Table 605. VMware AppDefense sample message supported by VMware AppDefense.
Event name

Low-level
category

Inbound
Connection Rule
Violation

Firewall Deny

Sample log message

{"id":1111111,"createdAt":1512009263.471000000,
"remediation":{"id":1111111},"severity":"CRITICAL",
"lastReceivedAt":1516170726.957000000,"count":2,
"status":"UNRESOLVED","violationDetails":{"processHa
shSHA256":"10000000000000000000000000000000000000000
00000000000000000000000","processHash":"100000000000
00000000000000000000","cli":"<cli>","localPort":"<24
","processPath":"","alert":"INBOUND_CONNECTION_RULES
_VIOLATION","localAddress":"192.0.2.0","ipProtocol":
"tcp","preEstablishedConnection":"FALSE"},"violating
VirtualMachine":{"id":1111111,"vmToolsStatus":"TOOLS
_NOT_RUNNING","vcenterUuid":"11111111-1111-1111-1111
-111111111111","vmUuid":"11111111-1111-1111-1111-111
111111111","ipAddress":"192.0.2.0”,"osType":"WINDOWS
","vmManageabilityStatus":"HOST_MODULE_ENABLED_AND_
GUEST_MODULE_MISSING","guestAgentVersion":"1.0.1.0"
,"macAddress":"<MacAddress>","guestId":"windows8","
healthStatus":"CRITICAL","service":{"id":00000},"vm
Id":"1","guestAgentStatus":"Disconnected","guest
Name":"Microsoft Windows","guestStatus":"POWERED_
OFF","name":"<name>","hostName":"<Hostname>"},"viol
atingProcess":{"processReputationProfile":null,
"fullPathName":"System","<System>":"<System>","pro
cess256Hash":"100000000000000000000000000000000000
0000000000000000000000000000","processMd5Hash":"10
000000000000000000000000000000"},"subRuleViolated"
:null,"ruleViolated":"INBOUND_CONNECTION"}

1154 IBM QRadar : QRadar DSM Configuration Guide


Table 605. VMware AppDefense sample message supported by VMware AppDefense. (continued)
Event name

Low-level
category

Outbound
Connection Rule
Violation

Firewall Deny

Sample log message

{"id":10101001,"createdAt":1512009263.495000000,
"remediation":{"id":1551519},"severity":"CRITICAL",
"lastReceivedAt":1516224258.818000000,"count":0000
1,"status":"UNRESOLVED","violationDetails":{"proce
ssHashSHA256":"00000000000000000000000000000000000
00000000000000000000000000","processHash":"0000000
000000000000000000000000","cli":"C:\\<path>,"alert"
:"OUTBOUND_CONNECTION_RULES_VIOLATION","localAddre
ss":"192.0.2.0","remotePort":"24","ipProtocol":
"udp","preEstablishedConnection":"FALSE","remote
Address":"0000::0:0"},"violatingVirtualMachine":
{"id":101010,"vmToolsStatus":"TOOLS_NOT_RUNNING",
"vcenterUuid":"11111111-1111-1111-1111-1111111111
11","vmUuid":"11111111-1111-1111-1111-11111111111
1","ipAddress":"192.0.2.0","osType":"WINDOWS","vm
ManageabilityStatus":"HOST_MODULE_ENABLED_AND_GUE
ST_MODULE_MISSING","guestAgentVersion":"1.0.1.0"
,"macAddress":"<MacAddress>","guestId":"windows8",
"healthStatus":"CRITICAL","service":{"id":28486},
"vmId":"1","guestAgentStatus":"Disconnected","guest
Name":"Microsoft Windows","guestStatus":"POWERED_
OFF","name":"<name>","hostName":"<host>"},"violat
ingProcess":{"processReputationProfile":{"process
FileInfo":{"md5":"000000000000000000000000000000",
"sha256":"000000000000000000000000000000000000000
00000000000000000000","container":false,"executab
le":true,"ssdeep":"100:THGFJFJFHJY7y86gHK7GHk7ghj
gkghjk","fileSizeBytes":1,"peFormat":true,"first
SeenName":"<fileName>","sha1":"00000000000000000
0000000000000000000","crc32":null},"peHeaderMeta
data":{"companyName":"Microsoft Corporation",
"productName":"Microsoft Windows,"version":null,
"originalName":"<host>","description":"<descript
ion>","fileVersion":"192.0.2.0,"codePage":null,
"productVersion":"6.3.9600.17415","language":
"English (U.S.)"},"certificate":{"commonName":
"Windows","certificateexinfo":{"thumbprint":"0000
00000000000000000000000000000000000000000","issue
rThumbprint":"000000000000000000000000000000000"
,"serialNumber":null,"validToDate":1437604140.00
0000000,"validFromDate":1398205740.000000000,"pu
blisher":null,"name":null}},"trust":10,"threat":
0},"fullPathName":"C:\\<path>","process256Hash":
"00000000000000000000000000000000000000000000000
0000000000000","processMd5Hash":"000000000000000
000000000000000000"},"subRuleViolated":null,"rul
eViolated":"OUTBOUND_CONNECTION"}

Related concepts
VMware AppDefense
The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system.

VMware ESX and ESXi
The EMC VMware DSM for IBM QRadar collects ESX and ESXi server events by using the VMware protocol
or syslog. The EMC VMware DSM supports events from VMware ESX or ESXi 3.x, 4.x, 5.x and 6.x servers.
To collect VMware ESX or ESXi events, you can select one of the following event collection methods:
• “Configuring syslog on VMware ESX and ESXi servers” on page 1156
• “Configuring the EMC VMWare protocol for ESX or ESXi servers” on page 1158
Chapter 161. VMWare 1155


Configuring syslog on VMware ESX and ESXi servers

To collect syslog events for VMware, you must configure the server to forward events by using syslogd from your ESXi server to IBM QRadar.

Procedure
1. Log in to your VMware vSphere Client.
2. Select the host that manages your VMware inventory.
3. Click the Configuration tab.
4. From the Software pane, click Advanced Settings.
5. In the navigation menu, click Syslog.
6. Configure values for the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>ESX version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog.Local.DatastorePath</td>
<td>ESX or ESXi 3.5.x or 4.x</td>
<td>Type the directory path for the local syslog messages on your ESXi server. The default directory path is /scratch/log/messages.</td>
</tr>
<tr>
<td>Syslog.Remote.Hostname</td>
<td>ESX or ESXi 3.5.x or 4.x</td>
<td>Type the IP address or host name of QRadar.</td>
</tr>
<tr>
<td>Syslog.Remote.Port</td>
<td>ESX or ESXi 3.5.x or 4.x</td>
<td>Type the port number the ESXi server uses to forward syslog data. The default is port 514.</td>
</tr>
<tr>
<td>Syslog.global.logHost</td>
<td>ESXi v5.x or ESXi v6.x</td>
<td>Type the URL and port number that the ESXi server uses to forward syslog data. Examples: udp://&lt;QRadar IP address&gt;:514 tcp://&lt;QRadar IP address&gt;:514</td>
</tr>
</tbody>
</table>

7. Click OK to save the configuration.

The default firewall configuration on VMware ESXi v5.x and VMware ESXi v6.x servers disable outgoing connections by default. Outgoing syslog connections that are disabled restrict the internal syslog forwarder from sending security and access events to QRadar.

By default, the syslog firewall configuration for VMware products allow only outgoing syslog communications. To prevent security risks, do not edit the default syslog firewall rule to enable incoming syslog connections.

Enabling syslog firewall settings on vSphere Clients

To forward syslog events from ESXi v5.x or ESXi v6.x servers, you must edit your security policy to enable outgoing syslog connections for events.

Procedure
1. Log in to your ESXi v5.x or ESXi v6.x server from a vSphere client.
2. From the Inventory list, select your ESXi Server.
3. Click the Manage tab and select Security Profile.
4. In the **Firewall** section, click **Properties**.
5. In the **Firewall Properties** window, select the **syslog** check box.
6. Click **OK**.

**Enabling syslog firewall settings on vSphere Clients by using the esxcli command**

To forward syslog events from ESXi v5.x or ESXi v6.x servers, as an alternative, you can configure ESXi Firewall Exception by using the esxcli command.

**Note:** To forward syslog logs, you might need to manually open the Firewall rule set. This firewall rule does not effect ESXi 5.0 build 456551. The UDP port 514 traffic flows.

To open outbound traffic through the ESXi Firewall on UDP port 514 and on TCP ports 514 and 1514, run the following commands:

```bash
esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true
esxcli network firewall refresh
```

**Configuring a syslog log source for VMware ESX or ESXi**

IBM QRadar automatically discovers and creates a log source for syslog events from VMware. The following configuration steps are optional.

**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 **EMC VMWare**.
6. Using the **Protocol Configuration** list, select **Syslog**.
7. Configure the following values:

<table>
<thead>
<tr>
<th>Table 607. Syslog protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>Enabled</td>
</tr>
<tr>
<td>Credibility</td>
</tr>
<tr>
<td>Target Event Collector</td>
</tr>
<tr>
<td>Coalescing Events</td>
</tr>
</tbody>
</table>
### Table 607. Syslog protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming Event Payload</strong></td>
<td>From the list, select the incoming payload encoder for parsing and storing the logs.</td>
</tr>
</tbody>
</table>
| **Store Event Payload**          | Select this check box to enable the log source to store event payload information.  
By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the **System Settings** in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source. |

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

### Configuring the EMC VMWare protocol for ESX or ESXi servers

You can configure the EMC VMWare protocol to read events from your VMware ESXi server. The EMC VMWare protocol uses HTTPS to poll for ESX and ESXi servers for events.

**About this task**

Before you configure your log source to use the EMC VMWare protocol, it is suggested that you create a unique user to poll for events. This user can be created as a member of the root or administrative group, but you must provide the user with an assigned role of read-only permission. This ensures that IBM QRadar can collect the maximum number of events and retain a level of security for your virtual servers. For more information about user roles, see your VMware documentation.

To integrate EMC VMWare with QRadar, you must complete the following tasks:

1. Create an ESX account for QRadar.
2. Configure account permissions for the QRadar user.
3. Configure the EMC VMWare protocol in QRadar.

Creating a user who is not part of the root or an administrative group might lead to some events not being collected by QRadar. It is suggested that you create your QRadar user to include administrative privileges, but assign this custom user a read-only role.

### Creating an account for QRadar in ESX

You can create a IBM QRadar user account for EMC VMWare to allow the protocol to properly poll for events.

**Procedure**

1. Log in to your ESX host by using the vSphere Client.
2. Click the **Local Users & Groups** tab.
3. Click **Users**.
4. Right-click and select **Add**.
5. Configure the following parameters:
   a) **Login** - Type a login name for the new user.
   b) **UID** - Optional. Type a user ID.
   c) **User Name** - Type a user name for the account.
   d) **Password** - Type a password for the account.
   e) **Confirm Password** - Type the password again as confirmation.
f) **Group** - From the **Group** list, select **root**

6. Click **Add**.
7. Click **OK**.

**Configuring read-only account permissions**

For security reasons, configure your IBM QRadar user account as a member of your root or admin group, but select an assigned role of read-only permissions.

**About this task**

Read-only permission allows the QRadar user account to view and collect events by using the EMC VMWare protocol.

**Procedure**

1. Click the **Permissions** tab.
2. Right-click and select **Add Permissions**.
3. On the **Users and Groups** window, click **Add**.
4. Select your QRadar user and click **Add**.
5. Click **OK**.
6. From the **Assigned Role** list, select **Read-only**.
7. Click **OK**.

**Configuring a log source for the EMC VMWare protocol**

You can configure a log source with the EMC VMWare protocol to poll for EMC VMWare events.

**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 **EMC VMWare**.
6. Using the **Protocol Configuration** list, select **EMC VMWare**.
7. Configure the following values:

<table>
<thead>
<tr>
<th><strong>Table 608. VMWare protocol parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Log Source Identifier</strong></td>
</tr>
<tr>
<td><strong>ESX IP</strong></td>
</tr>
<tr>
<td><strong>User Name</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
</tbody>
</table>

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

The VMware vCenter DSM for IBM QRadar collects vCenter server events by using the EMC VMWare protocol.

The EMC VMware protocol uses HTTPS to poll for vCenter appliances for events. You must configure a log source in QRadar to collect VMware vCenter events.

Before you configure your log source to use the EMC VMWare protocol, it is suggested that you create a unique user to poll for events. This user can be created as a member of the root or administrative group, but you must provide the user with an assigned role of read-only permission. This ensures that QRadar can collect the maximum number of events and retain a level of security for your virtual servers. For more information about user roles, see your VMware documentation.

Configuring a log source for the VMware vCenter

To collect vCenter events with the EMC VMWare protocol, you must configure a log source in IBM QRadar.

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 VMware vCenter.
6. Using the Protocol Configuration list, select EMC VMWare.
7. Configure the following values:

<table>
<thead>
<tr>
<th>Table 609. EMC VMWare protocol parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>ESX IP</td>
</tr>
<tr>
<td>User Name</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

8. Click Save.

VMware vCloud Director

You can use the VMware vCloud Director DSM and the vCloud protocol for IBM QRadar to poll the vCloud REST API for events.

QRadar supports polling for VMware vCloud Director events from vCloud Directory 5.1 appliances. Events that are collected by using the vCloud REST API are assembled as Log Extended Event Format (LEEF) events.

To integrate vCloud events with QRadar, you must complete the following tasks:
1. On your vCloud appliance, configure a public address for the vCloud REST API.
2. On your QRadar appliance, configure a log source to poll for vCloud events.
3. Ensure that no firewall rules block communication between your vCloud appliance and the QRadar Console or the managed host that is responsible for polling the vCloud REST API.

**Configuring the vCloud REST API public address**

IBM QRadar collects security data from the vCloud API by polling the REST API of the vCloud appliance for events. Before QRadar can collect any data, you must configure the public REST API base URL.

**Procedure**

1. Log in to your vCloud appliance as an administrator.
2. Click the **Administration** tab.
3. From the **Administration** menu, select **System Settings > Public Addresses**.
4. In the **VCD public REST API base URL** field, type an IP address or host name.
   
   The address that you specify becomes a publicly available address outside of the firewall or NAT on your vCloud appliance.
5. Click **Apply**.
   
   The public API URL is created on the vCloud appliance.

**What to do next**

You can now configure a log source in QRadar.

**Supported VMware vCloud Director event types logged by IBM QRadar**

The VMware vCloud Director DSM for QRadar can collect events from several categories.

Each event category contains low-level events that describe the action that is taken within the event category. For example, user events can have **user created** or **user deleted** as a low-level event.

The following list is the default event categories that are collected by QRadar from vCloud Director:

- User events
- Group events
- User role events
- Session events
- Organization events
- Network events
- Catalog events
- Virtual data center (VDC) events
- Virtual application (vApp) events
- Virtual machine (VM) events
- Media events
- Task operation events

**Configuring a VMware vCloud Director log source in IBM QRadar**

To collect VMware vCloud Director events, you must configure a log source in QRadar with the location and credentials that are required to poll the vCloud API.

**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 Name** field, type a name for your log source.
7. Optional: In the **Log Source Description** field, type a description for your log source.
8. From the **Log Source Type** list, select **VMware vCloud Director**.
9. From the **Protocol Configuration** list, select **VMware vCloud Director**.
10. Configure the following values:

<table>
<thead>
<tr>
<th>Table 6.10. VMware vCloud Director log source parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Log Source Identifier</td>
</tr>
<tr>
<td>vCloud URL</td>
</tr>
<tr>
<td>User Name</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Confirm Password</td>
</tr>
<tr>
<td>Polling Interval</td>
</tr>
<tr>
<td>Enabled</td>
</tr>
<tr>
<td>Credibility</td>
</tr>
<tr>
<td>Target Event Collector</td>
</tr>
<tr>
<td>Coalescing Events</td>
</tr>
</tbody>
</table>
**Table 610. VMware vCloud Director log source parameters (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming Event Payload</strong></td>
<td>From the list, select the incoming payload encoder for parsing and storing the logs.</td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
<td>Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the Store Event Payload list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
</tbody>
</table>

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.

vCloud events that are forwarded to QRadar are displayed on the **Log Activity** tab of QRadar.

---

**VMware vShield**

The IBM QRadar DSM for VMware vShield can collect event logs from your VMware vShield servers. The following table identifies the specifications for the VMware vShield Server DSM:

**Table 611. VMware vShield DSM specifications**

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>VMware</td>
</tr>
<tr>
<td>DSM</td>
<td>vShield</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-VMwarevShield-build_number.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>All events</td>
</tr>
<tr>
<td>Automatically discovered</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td><a href="http://www.vmware.com/">http://www.vmware.com/</a></td>
</tr>
</tbody>
</table>

**VMware vShield DSM integration process**

You can integrate VMware vShield DSM with IBM QRadar.

Use the following procedures:

1. If automatic updates are not enabled, download and install the most recent version of the VMware vShield RPM on your QRadar Console.
2. For each instance of VMware vShield, configure your VMware vShield system to enable communication with QRadar. This procedure must be completed for each instance of VMware vShield.
3. If QRadar does not automatically discover the log source, for each VMware vShield server that you want to integrate, create a log source on the QRadar Console.

**Related tasks**

“Configuring your VMware vShield system for communication with IBM QRadar” on page 1164

“Configuring a VMware vShield log source in IBM QRadar” on page 1164

### Configuring your VMware vShield system for communication with IBM QRadar

To collect all audit logs and system events from VMware vShield, you must configure the vShield Manager. When you configure VMware vShield, you must specify IBM QRadar as the syslog server.

**Procedure**

1. Access your vShield Manager inventory pane.
2. Click Settings & Reports.
3. Click Configuration > General.
4. Click Edit next to the Syslog Server option.
5. Type the IP address of your QRadar Console.
6. Optional: Type the port for your QRadar Console. If you do not specify a port, the default UDP port for the IP address/host name of your QRadar Console is used.
7. Click OK.

### Configuring a VMware vShield log source in IBM QRadar

To collect VMware vShield 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 VMware vShield.
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 162. Vormetric Data Security

The Vormetric Data Security DSM for IBM QRadar can collect event logs from your Vormetric Data Security servers.

The following table identifies the specifications for the Vormetric Data Security DSM:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Vormetric, Inc.</td>
</tr>
<tr>
<td>DSM</td>
<td>Vormetric Data Security</td>
</tr>
<tr>
<td>RPM file name</td>
<td>DSM-VormetricDataSecurity-7.1-804377.noarch.rpm</td>
</tr>
<tr>
<td></td>
<td>DSM-VormetricDataSecurity-7.2-804381.noarch.rpm</td>
</tr>
<tr>
<td>Supported versions</td>
<td>Vormetric Data Security Manager v5.1.3 and later</td>
</tr>
<tr>
<td></td>
<td>Vormetric Data Firewall FS Agent v5.2 and later</td>
</tr>
<tr>
<td>Protocol</td>
<td>Syslog (LEEF)</td>
</tr>
<tr>
<td>QRadar recorded events</td>
<td>Audit, Alarm, Warn, Learn Mode, System</td>
</tr>
<tr>
<td>Auto discovered</td>
<td>Yes</td>
</tr>
<tr>
<td>Includes identity</td>
<td>No</td>
</tr>
<tr>
<td>More information</td>
<td>Vormetric website (<a href="http://www.vormetric.com">http://www.vormetric.com</a>)</td>
</tr>
</tbody>
</table>

Vormetric Data Security DSM integration process

You can integrate Vormetric Data Security DSM with IBM QRadar.

Use the following procedures:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console:
   • Syslog protocol RPM
   • DSMCommon RPM

   The minimum version of the DSMCommon RPM that you can use is the DSM-DSMCommon-7.1-530016.noarch.rpm or DSM-DSMCommon-7.2-572972.noarch.rpm
   • Vormetric Data Security RPM

2. For each instance of Vormetric Data Security, configure your Vormetric Data Security system to enable communication with QRadar.

3. If QRadar does not automatically discover the DSM, for each Vormetric Data Security server you want to integrate, create a log source on the QRadar Console.
Related tasks
“Configuring your Vormetric Data Security systems for communication with IBM QRadar” on page 1166
“Configuring a Vormetric Data Security log source in IBM QRadar” on page 1167

Configuring your Vormetric Data Security systems for communication with IBM QRadar

To collect all audit logs and system events from Vormetric Data Security, you must configure your Vormetric Data Security Manager to enable communication with QRadar.

About this task
Your Vormetric Data Security Manager user account must have System Administrator permissions.

Procedure
1. Log in to your Vormetric Data Security Manager as an administrator that is assigned System Administrator permissions.
2. On the navigation menu, click Log > Syslog.
3. Click Add.
4. In the Server Name field, type the IP address or host name of your QRadar system.
5. From the Transport Protocol list, select TCP or a value that matches the log source protocol configuration on your QRadar system.
6. In the Port Number field, type 514 or a value that matches the log source protocol configuration on your QRadar system.
7. From the Message Format list, select LEEF.
8. Click OK.
9. On the Syslog Server summary screen, verify the details that you have entered for your QRadar system. If the Logging to SysLog value is OFF, complete the following steps. On the navigation menu, click System > General Preferences
10. Click the System tab.
11. In the Syslog Settings pane, select the Syslog Enabled check box.

What to do next
“Configuring Vormetric Data Firewall FS Agents to bypass Vormetric Data Security Manager” on page 1166

Configuring Vormetric Data Firewall FS Agents to bypass Vormetric Data Security Manager

When the Vormetric Data Security Manager is enabled to communicate with IBM QRadar, all events from the Vormetric Data Firewall FS Agents are also forwarded to the QRadar system through the Vormetric Data Security Manager.

About this task
To bypass the Vormetric Data Security Manager, you can configure Vormetric Data Firewall FS Agents to send LEEF events directly to the QRadar system.

Your Vormetric Data Security Manager user account must have System Administrator permissions.
**Procedure**

1. Log in to your Vormetric Data Security Manager.
2. On the navigation menu, click **System > Log Preferences**.
3. Click the **FS Agent Log** tab.
4. In the **Policy Evaluation** row, configure the following parameters:
   a) Select the **Log to Syslog/Event Log** check box.
5. Clear the **Upload to Server** check box.
6. From the **Level** list, select **INFO**.
   
   This set up enables a full audit trail from the policy evaluation module to be sent directly to a syslog server, and not to the Security Manager. Leaving both destinations enabled might result in duplication of events to the QRadar system.
7. Under the Syslog Settings section, configure the following parameters. In the **Server** field, use the following syntax to type the IP address or host name and port number of your QRadar system.
   
   \[
   \text{qradar\_IP address_or_host:port}
   \]
8. From the **Protocol** list, select **TCP** or a value that matches the log source configuration on your QRadar system.
9. From the **Message Format** list, select **LEEF**.

**What to do next**

This configuration is applied to all hosts or host groups later added to the Vormetric Data Security Manager. For each existing host or host group, select the required host or host group from the **Hosts** list and repeat the procedure.

---

**Configuring a Vormetric Data Security log source in IBM QRadar**

To collect Vormetric Data Security events, configure a log source in IBM 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 **Vormetric Data Security**.
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 163. WatchGuard Fireware OS

The IBM 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:

| 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 of the following procedures:
   - “Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar” on page 1170
   - “Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar” on page 1170

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 DSM” on page 4
“Adding a log source” on page 4
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 164. Websense

Websense is now known as Forcepoint.

**Related concepts**

Forcepoint

IBM QRadar supports a range of Forcepoint DSMs.
Chapter 165. Zscaler Nanolog Streaming Service

IBM QRadar can collect and categorize events from Zscaler Nanolog Streaming Service (NSS) log feeds that forward syslog event to QRadar.

To collect syslog events, you must configure your Zscaler NSS with an NSS feed to forward TCP syslog events to QRadar. QRadar automatically discovers and creates log sources for syslog events that are forwarded from Zscaler NSS log feeds. QRadar supports syslog events from Zscaler NSS V4.1 and Zscaler NSS V5.3.

To configure Zscaler NSS, complete the following tasks:

1. On your Zscaler NSS appliance, create a log feed for QRadar.
2. On your QRadar system, verify that the forwarded events are automatically discovered.

Supported event types for Zscaler NSS

The Zscaler NSS DSM for QRadar collects information about web browsing events from Zscaler NSS installations.

Each Zscaler NSS event contains information on the action that is taken on the web browsing in the event category. For example, web browsing events can have a category that is allowed or blocked website traffic. Each event defines the website that was allowed or blocked and includes all of the event details in the event payload.

Configuring a syslog feed in Zscaler NSS

To collect events, you must configure a syslog feed on your Zscaler NSS to forward syslog events to IBM QRadar.

Procedure

1. Log in to the administration portal for Zscaler NSS.
2. Select Administration > Settings > Nanolog Streaming Service.
3. On the NSSFeeds tab, click Add.
4. Enter a name for the feed.
5. On the NSSServer menu, select an NSS.
6. Set the SIEM IP Address to the IP address of the QRadar Event Collector.
7. Set the SIEM TCP Port to port 514.
8. Set the Feed Output Type to QRadar LEEF. The Feed Output Format is automatically populated with the appropriate string:

```
%s{mon} %02d{dd} %02d{hh}: %02d{mm}: %02d{ss} zscaler-nss
LEEF:1.0|Zscaler|NSS|4.1|\%{reason}|cat=\%{action}
\%{tdevTime}=\%{mon} \%02d{dd} \%02d{hh}
\%02d{mm}: \%02d{ss} \%s{tz}\%{tdevTimeFormat}=MMM dd yyyy HH:mm:ss
z\%{sip}\tsrscPostNAT=\%{cintip}
\%{realm}=\%{location}\tsrscName=\%{login}\tsrscBytes=\%d{reqsize}
\%{dstBytes}=\%d{respsize}
\%{trole}=\%{dept}\tpolicy=\%{reason}\turl=\%{eurl}
\%{recordingid}=\%{recordid}
\%{bthrottle}=\%{bwthrottle}\tsuseragent=\%{ua}
\%{referer}=\%{referrer}\thostname=\%{ehost}
\%{tappproto}=\%{proto}\turlcategory=\%{urlcat}
\%{tsrcsuperclass}=\%{urlsupercat}
\%{tsrcclass}=\%{urlclass}\tappclass=\%{appclass}\tappname=\%{appname}
\%{tmalwareclass}=\%{malwareclass}\tthreatname=\%{threatname}
\%{triskscore}=\%{riskscore}\tdlpdict=\%{dlpdict}\tdlpeng=\%{dlpeng}\tfileclass=\%{fileclass}
```
9. Click **Save**.

QRadar automatically discovers and creates a log source for Zscaler NSS appliances. Events that are forwarded to QRadar are viewable on the **Log Activity** tab.

## Configuring a Zscaler NSS log source

IBM QRadar automatically discovers and creates a log source for syslog events that are forwarded from Zscaler NSS.

### About this task

These configuration steps are optional.

### Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. In the **Log Source Name** field, type a name for your log source.
6. Optional: In the **Log Source Description** field, type a description for your log source.
7. From the **Log Source Type** list, select **Zscaler NSS**.
8. From the **Protocol Configuration** list, select **Syslog**.
9. Configure the following values:

<table>
<thead>
<tr>
<th><strong>Table 613. Syslog protocol parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>Log Source Identifier</strong></td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
</tr>
<tr>
<td><strong>Credibility</strong></td>
</tr>
<tr>
<td><strong>Target Event Collector</strong></td>
</tr>
<tr>
<td><strong>Coalescing Events</strong></td>
</tr>
</tbody>
</table>
Table 613. Syslog protocol parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming Event Payload</strong></td>
<td>From the list, select the <strong>Incoming Payload Encoder</strong> for parsing and storing the logs.</td>
</tr>
<tr>
<td><strong>Store Event Payload</strong></td>
<td>Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the <strong>Store Event Payload</strong> list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.</td>
</tr>
<tr>
<td><strong>Log Source Language</strong></td>
<td>Select the language of the events that are generated by zScaler NSS.</td>
</tr>
</tbody>
</table>

10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.
IBM QRadar can collect events from your security products by using a plug-in file that is called a Device Support Module (DSM).

QRadar can receive logs from systems and devices by using the Syslog protocol, which is a standard protocol. Supported DSMs can use other protocols, as mentioned in the Supported DSM table. You can try to configure third-party applications to send logs to QRadar through the Syslog protocol. For more information, see “Adding a log source” on page 4.

If you want to send logs by using a supported DSM that is not supported by the auto discovery feature in QRadar, you need to manually add a log source. For more information about adding a log source in QRadar, see “Adding a log source” on page 4.

**What do you do if the product version or device you have is not listed in the DSM Configuration Guide?**

Sometimes a version of a vendor product or a device is not listed as supported. If the product or device is not listed, follow these guidelines:

**Version not listed**

If the DSM is for a product that is officially supported by QRadar, but the version listed in the IBM QRadar DSM Configuration Guide appears to be out-of-date, try the DSM to see whether it works. The product versions that are listed in the guide are those specifically tested by IBM, but newer untested versions may also work. In most cases no changes are necessary, or at most a minor update to the IBM QRadar Identifier (QID) Map may be all that is required. Software updates by vendors might on rare occasions add or change event formats that break the DSM, requiring an RFE for the development of a new integration. This would be the only scenario where an RFE is required. In either event, open a support ticket for a review of the log source to troubleshoot and rule out any potential issues not related to the software version.

**Device not listed**

When a device is not officially supported, you have the following options:

- Open a request for enhancement (RFE) to have your device become officially supported.
  1. Go to the QRadar SIEM RFE page (https://ibm.biz/BdRPx5).
  2. Log in to the support portal page.
  3. Click the Submit tab and type the necessary information.

  **Note:** If you have event logs from a device, attach the event information and include the product version of the device that generated the event log.

- Write a log source extension to parse events for your device. For more information, see Chapter 11, “Log source extensions,” on page 107 and the DSM Editor.

The following table lists supported DSMs for third-party and IBM QRadar solutions.

<table>
<thead>
<tr>
<th>Table 614. QRadar Supported DSMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>3Com</td>
</tr>
<tr>
<td>AhnLab</td>
</tr>
<tr>
<td>Akamai</td>
</tr>
<tr>
<td>Amazon</td>
</tr>
<tr>
<td>Amazon</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>Ambiron</td>
</tr>
<tr>
<td>Apache</td>
</tr>
<tr>
<td>APC</td>
</tr>
<tr>
<td>Apple</td>
</tr>
<tr>
<td>Application Security, Inc.</td>
</tr>
<tr>
<td>Arbor Networks</td>
</tr>
<tr>
<td>Arbor Networks</td>
</tr>
<tr>
<td>Arpeggio Software</td>
</tr>
<tr>
<td>Array Networks</td>
</tr>
<tr>
<td>Aruba Networks</td>
</tr>
<tr>
<td>Aruba Networks</td>
</tr>
<tr>
<td>Avaya Inc.</td>
</tr>
<tr>
<td>Balabit IT Security</td>
</tr>
<tr>
<td>Balabit IT Security</td>
</tr>
<tr>
<td>Barracuda Networks</td>
</tr>
<tr>
<td>Barracuda Networks</td>
</tr>
<tr>
<td>Barracuda Networks</td>
</tr>
<tr>
<td>Blue Cat</td>
</tr>
<tr>
<td>Blue Coat</td>
</tr>
<tr>
<td>Blue Coat</td>
</tr>
<tr>
<td>Box</td>
</tr>
<tr>
<td>Bridgewater Systems</td>
</tr>
<tr>
<td>Brocade</td>
</tr>
<tr>
<td>CA</td>
</tr>
<tr>
<td>CA</td>
</tr>
<tr>
<td>CA</td>
</tr>
<tr>
<td>Centrify</td>
</tr>
<tr>
<td>Carbon Black</td>
</tr>
<tr>
<td>Carbon Black</td>
</tr>
<tr>
<td>Carbon Black</td>
</tr>
<tr>
<td>Carbon Black</td>
</tr>
<tr>
<td>Centrify</td>
</tr>
<tr>
<td>Centrify</td>
</tr>
<tr>
<td>Check Point</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>Check Point</td>
</tr>
<tr>
<td>Check Point</td>
</tr>
<tr>
<td>Ciscom</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>Citrix</td>
</tr>
<tr>
<td>Citrix</td>
</tr>
<tr>
<td>Cloudera</td>
</tr>
<tr>
<td>CloudPassage</td>
</tr>
<tr>
<td>CrowdStrike</td>
</tr>
<tr>
<td>CorreLog</td>
</tr>
<tr>
<td>CRYPTOCard</td>
</tr>
<tr>
<td>CyberArk</td>
</tr>
<tr>
<td>CyberArk</td>
</tr>
<tr>
<td>CyberGuard</td>
</tr>
<tr>
<td>Damballa</td>
</tr>
<tr>
<td>Digital China Networks</td>
</tr>
<tr>
<td>DG Technology</td>
</tr>
<tr>
<td>ESET</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>------------------------------</td>
</tr>
<tr>
<td>Exabeam</td>
</tr>
<tr>
<td>Extreme Networks</td>
</tr>
<tr>
<td>F5 Networks</td>
</tr>
<tr>
<td>F5 Networks</td>
</tr>
<tr>
<td>F5 Networks</td>
</tr>
<tr>
<td>F5 Networks</td>
</tr>
<tr>
<td>F5 Networks</td>
</tr>
<tr>
<td>Fair Warning</td>
</tr>
<tr>
<td>Fasoo</td>
</tr>
<tr>
<td>Fidelis Security Systems</td>
</tr>
<tr>
<td>FireEye</td>
</tr>
<tr>
<td>F5RADIUS</td>
</tr>
<tr>
<td>Forcepoint</td>
</tr>
<tr>
<td>Forcepoint</td>
</tr>
<tr>
<td>Forcepoint</td>
</tr>
<tr>
<td>Forcepoint</td>
</tr>
<tr>
<td>Forcepoint</td>
</tr>
<tr>
<td>ForeScout</td>
</tr>
<tr>
<td>Fortinet</td>
</tr>
<tr>
<td>Foundry</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>genua</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>H3C</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>HP</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>HP</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>HP</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>HP</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Honeycomb</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Huawei</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Huawei</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Imperva</td>
</tr>
<tr>
<td>Imperva</td>
</tr>
<tr>
<td>Infoblox NIOS</td>
</tr>
<tr>
<td>Internet Systems</td>
</tr>
<tr>
<td>Intersect Alliance</td>
</tr>
<tr>
<td>IT-CUBE</td>
</tr>
<tr>
<td>Itron</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks*</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Kaspersky</td>
</tr>
<tr>
<td>Kaspersky</td>
</tr>
<tr>
<td>Kisco</td>
</tr>
<tr>
<td>Lastline</td>
</tr>
<tr>
<td>Lieberman</td>
</tr>
<tr>
<td>LightCyber</td>
</tr>
<tr>
<td>Linux</td>
</tr>
<tr>
<td>Linux</td>
</tr>
<tr>
<td>Linux</td>
</tr>
<tr>
<td>McAfee</td>
</tr>
<tr>
<td>McAfee</td>
</tr>
<tr>
<td>McAfee</td>
</tr>
<tr>
<td>McAfee</td>
</tr>
<tr>
<td>McAfee</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>MetaInfo</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>Motorola</td>
</tr>
<tr>
<td>NCC Group</td>
</tr>
<tr>
<td>Nira</td>
</tr>
<tr>
<td>NetApp</td>
</tr>
<tr>
<td>Netskope</td>
</tr>
<tr>
<td>NSGIX</td>
</tr>
<tr>
<td>NSKun</td>
</tr>
<tr>
<td>Nokia</td>
</tr>
<tr>
<td>Nokia</td>
</tr>
<tr>
<td>Nominum</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel*</td>
</tr>
<tr>
<td>Nortel*</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Novell</td>
</tr>
<tr>
<td>ObserveIT</td>
</tr>
<tr>
<td>Okta</td>
</tr>
<tr>
<td>Onapsis</td>
</tr>
<tr>
<td>OpenBSD Project</td>
</tr>
<tr>
<td>Open LDAP Foundation</td>
</tr>
<tr>
<td>Open Source</td>
</tr>
<tr>
<td>OpenStack</td>
</tr>
<tr>
<td>Oracle</td>
</tr>
<tr>
<td>Oracle</td>
</tr>
<tr>
<td>Oracle</td>
</tr>
<tr>
<td>Oracle</td>
</tr>
<tr>
<td>Oracle</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>Oracle</td>
</tr>
<tr>
<td>Oracle</td>
</tr>
<tr>
<td>OSSEC</td>
</tr>
<tr>
<td>Palo Alto Networks</td>
</tr>
<tr>
<td>Palo Alto Networks</td>
</tr>
<tr>
<td>Pirean</td>
</tr>
<tr>
<td>Postfix</td>
</tr>
<tr>
<td>ProFTpd</td>
</tr>
<tr>
<td>Proofpoint</td>
</tr>
<tr>
<td>Pulse Secure</td>
</tr>
<tr>
<td>Radware</td>
</tr>
<tr>
<td>Radware</td>
</tr>
<tr>
<td>Raz-Lee/Security</td>
</tr>
<tr>
<td>Redback Networks</td>
</tr>
<tr>
<td>Resolution1</td>
</tr>
<tr>
<td>Riverbed</td>
</tr>
<tr>
<td>Riverbed</td>
</tr>
<tr>
<td>RSA</td>
</tr>
<tr>
<td>SafeNet</td>
</tr>
<tr>
<td>Salesforce</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>Samhain Labs</td>
</tr>
<tr>
<td>SAP</td>
</tr>
<tr>
<td>Seculert</td>
</tr>
<tr>
<td>Seculert</td>
</tr>
<tr>
<td>Sentorigo</td>
</tr>
<tr>
<td>Skyhigh Networks</td>
</tr>
<tr>
<td>SolarWinds</td>
</tr>
<tr>
<td>SonicWALL</td>
</tr>
<tr>
<td>Sophos</td>
</tr>
<tr>
<td>Sophos</td>
</tr>
<tr>
<td>Sophos</td>
</tr>
<tr>
<td>Sophos</td>
</tr>
<tr>
<td>Sourcefire</td>
</tr>
<tr>
<td>Sourcefire</td>
</tr>
<tr>
<td>Splunk</td>
</tr>
<tr>
<td>Squid</td>
</tr>
<tr>
<td>Startent Networks</td>
</tr>
<tr>
<td>STEALTHbits Technologies</td>
</tr>
<tr>
<td>STEALTHbits Technologies</td>
</tr>
<tr>
<td>STEALTHbits Technologies</td>
</tr>
<tr>
<td>STEALTHbits Technologies</td>
</tr>
<tr>
<td>Sun</td>
</tr>
<tr>
<td>Sun</td>
</tr>
<tr>
<td>Sun</td>
</tr>
<tr>
<td>Sun</td>
</tr>
<tr>
<td>Sun</td>
</tr>
<tr>
<td>Sybase</td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
</tr>
<tr>
<td><strong>TippingPoint</strong></td>
</tr>
<tr>
<td><strong>TippingPoint</strong></td>
</tr>
<tr>
<td><strong>Top Layer</strong></td>
</tr>
<tr>
<td><strong>Trend Micro</strong></td>
</tr>
<tr>
<td><strong>Trend Micro</strong></td>
</tr>
<tr>
<td><strong>Trend Micro</strong></td>
</tr>
<tr>
<td><strong>Trend Micro</strong></td>
</tr>
<tr>
<td><strong>Trend Micro</strong></td>
</tr>
<tr>
<td><strong>Trend Micro</strong></td>
</tr>
<tr>
<td><strong>Tripwire</strong></td>
</tr>
<tr>
<td><strong>Tropos Networks</strong></td>
</tr>
<tr>
<td><strong>Trusteer</strong></td>
</tr>
<tr>
<td><strong>Universal</strong></td>
</tr>
<tr>
<td><strong>Universal</strong></td>
</tr>
<tr>
<td><strong>Universal</strong></td>
</tr>
<tr>
<td>Manufacturer</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>Universal</td>
</tr>
<tr>
<td>Vectra Networks</td>
</tr>
<tr>
<td>Verdasys</td>
</tr>
<tr>
<td>Vectra Networks</td>
</tr>
<tr>
<td>Veriocept</td>
</tr>
<tr>
<td>VMware</td>
</tr>
<tr>
<td>VMware</td>
</tr>
<tr>
<td>VMware</td>
</tr>
<tr>
<td>VMware</td>
</tr>
<tr>
<td>VMware</td>
</tr>
<tr>
<td>Verheuristic, Inc.</td>
</tr>
<tr>
<td>Watchguard</td>
</tr>
<tr>
<td>Zscaler</td>
</tr>
</tbody>
</table>
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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

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.

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 actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

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

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

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

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.
Commercial use
You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights
Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement
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.


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.

This glossary provides terms and definitions for the IBM QRadar SIEM software and products. The following cross-references are used in this glossary:

- **See** refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- **See also** refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

### A

**accumulator**
A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

**active system**
In a high-availability (HA) cluster, the system that has all of its services running.

**Address Resolution Protocol (ARP)**
A protocol that dynamically maps an IP address to a network adapter address in a local area network.

**administrative share**
A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

**anomaly**
A deviation from the expected behavior of the network.

**application signature**
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

**ARP**
See Address Resolution Protocol.

**ARP Redirect**
An ARP method for notifying the host if a problem exists on a network.

**ASN**
See autonomous system number.

**asset**
A manageable object that is either deployed or intended to be deployed in an operational environment.

**autonomous system number (ASN)**
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

### B

**behavior**
The observable effects of an operation or event, including its results.

**bonded interface**
See link aggregation.
burst
A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

CIDR
See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client
A software program or computer that requests services from a server.

cluster virtual IP address
An IP address that is shared between the primary or secondary host and the HA cluster.

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

credential
A set of information that grants a user or process certain access rights.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

CVSS
See Common Vulnerability Scoring System.

database leaf object
A terminal object or node in a database hierarchy.

datapoint
A calculated value of a metric at a point in time.

Device Support Module (DSM)
A configuration file that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as output.

DHCP
See Dynamic Host Configuration Protocol.

DNS
See Domain Name System.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.
DSM
See Device Support Module.

duplicate flow
Multiple instances of the same data transmission received from different flow sources.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

endpoint
The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

external scanning appliance
A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive
An event or flow that the user can decide should not create an offense, or an offense that the user decides is not a security incident.

flow
A single transmission of data passing over a link during a conversation.

flow log
A collection of flow records.

flow sources
The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination
One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN
See fully qualified domain name.

FQNN
See fully qualified network name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway
A device or program used to connect networks or systems with different network architectures.
HA
See high availability.

HA cluster
A high-availability configuration consisting of a primary server and one secondary server.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

ICMP
See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

IDS
See intrusion detection system.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

Internet service provider (ISP)
An organization that provides access to the Internet.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP
See Internet Protocol.

IP multicast
Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

IPS
See intrusion prevention system.

ISP
See Internet service provider.
key file
In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L
L2L
See Local To Local.
L2R
See Local To Remote.
LAN
See local area network.
LDAP
leaf
In a tree, an entry or node that has no children.
Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.
link aggregation
The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.
live scan
A vulnerability scan that generates report data from the scan results based on the session name.
local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.
Local To Local (L2L)
Pertaining to the internal traffic from one local network to another local network.
Local To Remote (L2R)
Pertaining to the internal traffic from one local network to another remote network.
log source
Either the security equipment or the network equipment from which an event log originates.
log source extension
An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M
Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.
magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.
N

NAT
See network address translation.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network hierarchy
A type of container that is a hierarchical collection of network objects.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network object
A component of a network hierarchy.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

offsite source
A device that is away from the primary site that forwards normalized data to an event collector.

offsite target
A device that is away from the primary site that receives event or data flow from an event collector.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI
See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

P

parsing order
A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

payload data
Application data contained in an IP flow, excluding header and administrative information.

primary HA host
The main computer that is connected to the HA cluster.
**protocol**
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

**Q**

**QID Map**
A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

**R**

**R2L**
See Remote To Local.

**R2R**
See Remote To Remote.

**recon**
See reconnaissance.

**reconnaissance (recon)**
A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

**reference map**
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

**reference map of maps**
A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

**reference map of sets**
A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

**reference set**
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

**reference table**
A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

**refresh timer**
An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

**relevance**
A measure of relative impact of an event, category, or offense on the network.

**Remote To Local (R2L)**
The external traffic from a remote network to a local network.

**Remote To Remote (R2R)**
The external traffic from a remote network to another remote network.

**report**
In query management, the formatted data that results from running a query and applying a form to it.

**report interval**
A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.
routing rule
A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule
A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

scanner
An automated security program that searches for software vulnerabilities within web applications.

secondary HA host
The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity
A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP

SOAP
A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system
A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet
See subnetwork.

subnet mask
For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

subnetwork (subnet)
A network that is divided into smaller independent subgroups, which still are interconnected.

sub-search
A function that allows a search query to be performed within a set of completed search results.

superflow
A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

system view
A visual representation of both primary and managed hosts that compose a system.

TCP

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-
host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

**truststore file**
A key database file that contains the public keys for a trusted entity.

**violation**
An act that bypasses or contravenes corporate policy.

**vulnerability**
A security exposure in an operating system, system software, or application software component.

**whois server**
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.
Index

Numerics

3Com Switch 8800 Series 137

A

About this guide xxvii
Access Manager for Mobile 599
Action Set for LSM 1102
Advanced Firewall Manager
  Logging profile 453
agile 667
agileSI 667
agileSI log source 668
AhnLab Policy Center 139
Akamai Kona 141
Amazon AWS CloudTrail 155–158, 167, 178
Ambiron TrustWave ipAngel 181
Apache HTTP Server
  syslog 191
  syslog-ng 193
APC UPS 189
Apple Mac OS
  Apple Mac OS X 195
Apple Mac OS X
  syslog 195
Application Security DbProtect 199
Arbor 203
Arbor Networks Peakflow
  Supported event types 204
Arbor Networks Peakflow SP
  Configure a log source 206
  Configuring global notifications settings 204
  Configuring remote syslog 204
Arbor Networks PeakFlow SP
  Configuring alert notification rules 205
Arbor Networks Pravail 207, 208
Arpeggio SIFT-IT
  Additional information 211
Array Networks
  SSL VPN 213
Aruba 215
Aruba Mobility Controller 219
Aruba Mobility Controllers 219, 220
  automatic updates 3
Avaya VPN Gateway
  DSM integration 221

B

Balabit
  Filtering log file 227
BalaBit
  Configuring a log source 229
  PE Relay 228
  Syslog 224
  Syslog-ng Agent 226, 227
  IT Security 223
  Microsoft ISA and TMG Events 226
BalaBit Syslog-ng 226
Barracuda
  Log source 231
  Syslog 231
Barracuda Web Filter
  Log source 235
  Syslog 235
Basic Security Mode 1068
BIG-IP
  Log publisher 452
BIG-IP AFM
  High-speed logging destination 452
BIG-IP LTM 458
Bit9 Parity 285
Blue Coat 243, 246, 249
Blue Coat SG 243, 246
BlueCat
  Adonis 241
  Event type 241
  Log source 242
BlueCat Adonis 242
Bluemix 547
Bridgewater 257
Bridgewater Systems
  Log source 257
Brocade Fabric OS
  Syslog 259
  bulk add 6, 101
  bulk edit 103

C

CA ACF2 261
CA SiteMinder
  Log source 269
  Syslog-ng 271
Carbon Black 281
Cascade Profiler 967, 969
Check Point
  Add a host 300
  Log source 308
  Log Source SIC 301
  OPSEC 299, 303, 304
  OPSEC Application Object 300
  OPSEC LEA 304
  OPSEC log source 315
  OPSEC/LEA 301
Check Point Firewall
  Syslog forwarders 308
Check Point Multi-Domain Management (Provider-1)
  OPSEC 314
  Syslog 313
  Syslog events 313

1207
Check Point SmartCenter Server 860
Check Point Syslog 306
Cilasoft QJRN/400
   Log source 320
   Syslog 319
Cisco ACE
   Log source 323
Cisco ACE Firewall 323
Cisco ACS
   Global logging categories 325
   Remote log 325
   v5.x 324
Cisco ACS v4.x
   Log source 327
   Syslog 326
Cisco ACS v5.x
   Log source 325
Cisco Aironet
   Log Source 330
Cisco ASA
   Log source 332
   Log Source 334
   Syslog 330
Cisco ASASyslog 331
Cisco CallManager
   Log Source 341
Cisco CatOS
   Catalyst switches 341
   Log source 342
   Syslog 341
Cisco CSA
   Log Source 347
   Syslog 346
Cisco FWSM
   Log source 354
   Syslog 354
Cisco IDS/IPS 359
Cisco IOS
   Log source 362
Cisco IOSForwarding events 361
Cisco ISE
   Logging categories 358
   Syslog events 358
Cisco NAC
   Syslog events 372
Cisco Nexus
   Log source 374
   NX-OS 373
   Syslog 373
Cisco NSEL 52
Cisco Pix
   Forwarding events 375
Cisco PixSyslog 375
Cisco VPN 3000
   Log source 383
Cisco VPN 3000 Concentrator 383
Cisco Wireless LAN Controller
   Log source 385
   SNMPv2 386, 387
   Syslog 384
   Trap receiver 387
Cisco Wireless LAN Controllers 384
Cisco Wireless Services Module (continued)
   WISM 388
Cisco WISM
   Log source 390
   Syslog 389
Citrix 393
Citrix Access Gateway 395
Citrix NetScaler
   Log source 394
Configuring a log source 225
Configuring syslog forwarding 695
Content Gateway Manager 486
Content Management Console 488
Cron 1070
CRYPTOCard CRYPTO-Shield
   Log source 411
CRYPTOCard CRYPTO-ShieldSyslog 411
CyberArk 413
CyberArk Vault
   Log source 415
   Syslog 415
CyberGuard
   Firewall/VPN Appliance 417
   Log source 417
   Syslog 417
D
Damballa Failsafe
   Log source 419
   Syslog 419
DbProtect alerts 201
DbProtect LEEF Relay 200
DbProtect LEEF Relay Module 200
Digital China Networks
   DCN DCS/DCRS 424
   DCS/DCRS Series Switch 423
   Log source 423
Domino
   SNMP 577
Domino Server
   Add-in Tasks 577
Dragon Enterprise Management Server (EMS) v7.4.0 440
E
EMC VMWare 1158
EMC VMWare protocol 53
extension documents
   troubleshooting 129
Extreme 437
Extreme 800-Series Switch 437
Extreme 800-Series Switches
   Log source 437
Extreme Dragon
   Log source 440
Extreme Dragon EMS
   Alarm tool policy
   Syslog 438
Extreme Dragon EMS v7.4.0
   Syslog 440
Extreme HiGuard Wireless IPS 441
Extreme HiPath Wireless Controller 443
Extreme Matrix K/N/S Series Switch 445
Extreme Matrix Router
version 3.5 444
Extreme NAC
Log source 447
Extreme NetSight Automatic Security Manager 446
Extreme Networks ExtremeWare 449
Extreme stackable and stand-alone switches 448

F
F5 BIG-IP APM 10.x
Remote syslog 455
F5 BIG-IP LTM
9.4.2 to 9.4.8 459
Log source 457
F5 BIG-IP LTM 10.x
Remote syslog 459
F5 BIG-IP LTM 11.x
Remote syslog 458
F5 FirePass
Syslog 460
F5 Networks BIG-IP AFM
Log source 454
F5 Networks BIG-IP APM
Log source 455
Remote syslog 454
F5 Networks BIG-IP ASM
Log source 457
F5 Networks BIG-IP LTM 457
F5 Networks FirePass
Log source 460
Fair Warning
Log source 463
Fidelis XPS
Log source 472
Syslog 471
Forcepoint 1173
Forcepoint Technical Support 486
Forcepoint TRITON 482, 483
Forcepoint TRITON and V-Series 483
Forcepoint V-Series 488
Forcepoint V-Series Content Gateway 485
Forcepoint V-Series Data Security Suite 484, 485
Forcepoint V-Series DSS 484
ForeScout CounterACT
Log source 489
Plug-in 490
Policies 490
Fortinet FortiAnalyzer 494
Fortinet FortiGate 494
Fortinet FortiGate Security Gateway 493
forwarded protocol 53
forwarding events 1137
Foundry FastIron 497
FreeRADIUS 499
FW 5100 858

G
Generic 501

H
H3C Technologies 513
HBGary Active Defense
Log source 511
Syslog 511
Hewlett Packard UniX
Logsourse 523
Hewlett Packard UNIX (HP-UX)
Syslog 523
Honeycomb FIM
Events 515
Honeycomb Lexicon File Integrity Monitor 515
Honeycomb Lexicon FIM
Log source 516
HP 519
HP ProCurve
Log source 521
Syslog 521
HP Tandem 522
HTTP Receiver protocol 54
Huawei 525
Huawei AR Series
Log source 578
Huawei AR Series Router 525
Huawei AR Series Routers 525
Huawei S Series
Log source 527
Huawei S Series Switch
Syslog 528
HyTrust CloudControl 529

I
IBM 531
IBM AIX Audit, configuring for syslog 534
IBM AS/400 538
IBM AS/400 iSeries 540
IBM BigFix 541
IBM BigFix protocol 54
IBM CICS 548
IBM Guardium
event map 145, 569
Event maps 569
Policy 568
Syslog events 567
IBM i 539
IBM IMS
Log source 573
IBM Informix
audit 575
IBM iSeries 538
IBM ISS Proventia 584
IBM Lotus Domino
SNMP Services 576
IBM Network Security (XGS)
Log source 616
IBM Proventia Management SiteProtector 581
IBM Proventia Management SiteProtector® 59
IBM Security Access Manager for Enterprise Single Sign-On version 8.1 or 8.2 597
IBM Security Access Manager for Mobile 599
IBM Security Directory Server
Log source 605
IBM Security Identity Manager 609
IBM Security Network Protection (XGS)
Alerts 615
LEEF 614
IBM Security Trusteer Apex Advanced Malware Protection 621
IBM SiteProtector
Log source 581
IBM Tivoli Access Manager
e-business 632, 634
IBM Tivoli Endpoint Manager 634
IBM WebSphere 634
IBM WebSphere Application Server
Log source 636
IBM zSecure Alert 644
Infoblox NIOS 665
Internet System Consortium (ISC) Bind 647
IPtables 722, 841
IPtables syslog
Log source 723
ISC Bind 647
ISC BIND 648
Itron Smart Meter
Array Networks SSL VPN 671

J

JDBC
Samhain events 986
JDBC protocol 55
JDBC SiteProtector protocol 59
Juniper DX Application Acceleration Platform 676
Juniper EX Series Ethernet Switch 676, 678
Juniper IDP
syslog 678
Juniper Infranet Controller 679
Juniper Junos OS 680
Juniper Junos OS Platform device 682
Juniper Junos WebApp Secure event logging 695
Juniper Networks
Juniper Secure Services Gateway (SSG) 684
Juniper Networks AVT 673
Juniper Networks AVT device 673
Juniper Networks Binary Log Format 686
Juniper Networks Firewall and VPN 679
Juniper Networks Firewall and VPN device events 680
Juniper Networks NSM
export to syslog 684
Juniper Networks NSM protocol 61

Juniper Networks SRX
log source 683
Juniper Networks vGW Virtual Gateway 693
Juniper Networks WLC Series 697
Juniper NSM 679
Juniper Security Binary Log Collector 685, 687
Juniper Security Binary Log Collector protocol 61
Juniper Steel-Belted Radius
syslog 690
Juniper WLC
syslog 698
Juniper WLC user interface
syslog 698

K

Kaspersky 699
Kaspersky Security Center
database view 709
Kisco Information Systems SafeNet/i 711

L

Lastline Enterprise 715
Lexicon mesh service 516
Lieberman Random Password Manager 717
Linux 721
Linux DHCP 721
Linux DHCP Servers
log source 721
Linux IPtables 721
Linux OS
syslog 724
log source
status 4, 27
log source extension
disable extension 133
enable extension 133
log source extensions 133
log sources 25
LOGbinder 727
Logging pool 451
LSM notification contacts 1102

M

Mac OS X log source 195
manage 133
McAfee 733
McAfee Application / Change Control 733
McAfee Intrushield 747
McAfee Intrushield V2.x - V5.x 747
McAfee Intrushield V6.x and V7.x fault notification events 750
McAfee Network Security Platform 747
McAfee Network Security Platform V6.x and V7.x fault notification events 750
McAfee Web Gateway
DSM integration 752
event map 755, 756
log file protocol 754, 755
unknown events 755
media-manager object 893
MetaInfo MetaIP 757
Microsoft 759
Microsoft DHCP protocol 65
Microsoft DHCP Server 766
Microsoft Endpoint Protection
    log source 769
Microsoft Exchange protocol 67
Microsoft Hyper-V
    log source 779
Microsoft IAS
    LOGbinder EX event collection 780
Microsoft IIS
    IIS Protocol 780
    log source 782, 783
Microsoft IIS protocol 69
Microsoft IIS Server
    IIS Protocol 780
Microsoft Internet and Acceleration (ISA) 783
Microsoft Operations Manager
    log source 788
Microsoft Security Event Log protocol 71
Microsoft SharePoint
    audit events 792
database view 792
events 792
    log source 794, 797
Microsoft System Center Operations Manager 805
Motorola Symbol AP xviii, 823
Motorola SymbolAP 823
MSGTRK logs 775, 776

N
Name Value Pair 825
NCC Group DDoS Secure 830
Niksun NetVCR 2005 839
Nokia Firewall
    custom script 842
    log source 842
    OPSEC 843
    OPSEC/LEA 843
    syslog 841
Nominum Vantio 847
None Of SMTP response rule 1083
Nortel Application Switch 851
Nortel Contivity 852
Nortel Ethernet Routing Switch 2500/4500/5500 853
Nortel Ethernet Routing Switch 8300/8600 854
Nortel Multiprotocol Router 849
Nortel Networks 849
Nortel Secure Network Access Switch 856
Nortel Secure Router 855
Nortel Switched Firewall
    OPSEC 858
    syslog 857
Nortel Switched Firewall 5100 857
Nortel Switched Firewall 6000 858
Nortel Switched Firewalls
    OPSEC 859
    syslog 858
Nortel Threat Protection System 860
Nortel VPN Gateway 861
Novell eDirectory 863

O
Observe IT JDBC 867
ObserveIT 867
Open LDAP
    event forwarding 884
    log source 881
    syslog 882
Open Source SNORT
    syslog 886
OpenBSD
    log source 879
    syslog 880
ophos Astaro Security Gateway 1032
OPSEC log source 844
OPSEC/LEA protocol 76
Oracle 891
Oracle Acme
    event types 891
Oracle Acme Packet SBC
    log source 891
    SNMP to syslog conversion 892
Oracle Acme Packet Session Border Controller 891
Oracle audit logs 906
Oracle BEA WebLogic
    application logging 898
    audit provider 898
domain logging 898
    event logs 897
    log source 899
Oracle database
    Perl 910
Oracle Database Listener 912
Oracle Database Listener protocol 78
Oracle DB Listener 908
Oracle Enterprise Manager 912
Oracle Fine Grained Auditing 914
Oracle OS Audit 917, 919
OSSEC
    syslog 921
Outbreak Criteria and Alert Notifications 1123
    overview 25

P
parsing order 6, 105
PCAP Protocol 682
PCAP Syslog Combination protocol 79
Pirean Access: One
    log source 935
PostFix Mail Transfer Agent 939
PostFix MTA
    log source 939
    multiline UDP syslog events 941
ProFTPD 943
Proventia 581

R
Radware DefensePro 955, 957
Raz-Lee i Security
    log source 961
Raz-Lee iSecurity 959, 1107
Red Hat Enterprise Linux v6 operating systems 725
Redback ASE 963
Riverbed 967
Riverbed SteelCentral NetProfiler 967, 969
RSA Authentication Manager
  Linux 973
  log file protocol 974
  syslog 973
  Windows 974
RSA Authentication Manager 6.x 975

S
S3 bucket 155–158, 167, 178
Samhain HIDS 985
Samhain Labs 985
SDEE protocol 81
Sentrigo Hedgehog 1005
SIFT-IT 209
SMB Tail protocol 82
SNMPv2 protocol 83
SonicWAL
  log source 1017
SonicWALL 1017
Sophos 1019
Sophos database 1023
Sophos Enterprise Console
  JDBC 1022
Sophos Enterprise Console JDBC protocol 85
Sophos Enterprise Console Protocol 1019
Sophos PureMessage
  Microsoft Exchange 1030
Sophos PureMessage for Linux 1029
Sophos Web Security Appliance 1033
Spam and Virus Firewall 231
Splunk 1037
Splunk appliances 1037
Splunk forwarded events 1037
Squid Web Proxy 1041, 1042
Standard Notifications 1123, 1125
Starent Networks 1047
STEALTHbits 979, 1051
STEALTHbits StealthINTERCEPT
  log source 1051, 1053
Stonesoft Management Center 477–479
Sun 1059
Sun ONE LDAP
  log source 1062
Sun Solaris 1066
Sun Solaris Basic Security Mode (BSM) 1068
Sun Solaris BSM 1071
Sun Solaris BSM audit logs 1069
Sun Solaris DHCP 1065
Sun Solaris Sendmail 1067
SunOne LDAP
  syslog 1063
Sybase ASE 1075
Sybase ASE device 1076
Symantec 1079
Symantec Data Loss Prevention (DLP) 1082
Symantec Encryption Management Server 1089
Symantec Encryption Management Servers 1089
Symantec Endpoint Protection 1088
Symantec SGS 1090
Symantec System Center 1090
Symantec System Center 1090
Symark PowerBroker 238
syslog firewall settings on vSphere Clients 1156
Syslog Redirect protocol 87
Syslog-ng Agent 223, 225

T
TCP multiline syslog protocol 88
third-party event collection overview 3
ThreatGRID log file protocol 1097
ThreatGRID Malware Threat Intelligence 1095
ThreatGRID syslog 1095
Tipping Point for SMS 1101
Tipping Point Intrusion Prevention System 1101
Tipping Point x505
  Tipping Point x506 1103
  Tipping Point X505/X506 Device 1103
  TippingPoint 1101
Tivoli Access Manager
  Configure e-business 633
TLS syslog protocol 93
Top Layer IPS 1105
Townsend Security LogAgent 1107
Trend Micro 1109
Trend Micro Control Manager 1109, 1110
Trend Micro InterScan VirusWall 1121
Trend Micro Office Scan 1121
Trend Micro Office Scan 10.x 1123
Trend Micro Office Scan 8.x 1122
Trend Micro OfficeScan XG 1124
Tripwire 1127
Tropos Control 1129
Trusteer Apex Local Event Aggregator 629

U
UDP multiline syslog protocol 96
Universal
  LEEF 1133
Universal DSM 1131
unknown events 1085, 1138

V
vCloud Director protocol 100
vCloud event types 1161
vCloud log source 1161
vCloud REST API 1161
Venusense configuration 1143
Venusense event filtering 1143
Venusense log source 1144
Venusense syslog server 1143
Venustech Venusense 1143
Verdasys Digital Guardian
  IPtables 1146
Vericept Content 360 DSM 1149
VMWare 1151
VMware ESX and ESXi servers 1156
VMware ESX or ESXi 1157
VMWare protocol
  read-only account permissions 1159
VMWare Protocol 1159
VMware protocol for ESX or ESXi servers 1158
VMware vCenter 1160
VMWare vCenter 1160
VMware vCloud Director 1160
VMware vShield 1163, 1164
VMware vShield log source 1164
Vormetric Data Firewall 1166
Vormetric Data Security 1165, 1167
Vormetric Data Security systems 1166

W
WebSphere
    JVM logs 635

X
XML examples 129

Z
Zscaler Nanolog Streaming Service 1175
Zscaler NSS 1175, 1176